SOLVED PAPERS

OF

COMPUTER NETWORKS – 1

(JUNE-2013 DEC-2013 JUNE-2014

DEC-2014 & JUNE-2015)

USN | | | | | | | | | | |

10CS55

Fifth Semester B.E. Degree Examination, June/July 2013
Computer Networks – I

Time: 3 hrs. Max. Marks:100

Note: ***Answer FIVE full questions, selecting at least TWO questions from each part.***

PART – A

1 a. Explain OSI reference model. **(10 Marks)**
b. Explain categories of network and differentiate between them. **(10 Marks)**

2 a. Represent the given sequence 01001110 in unipolar, NRZ-L, Manchesters, AMI, Pseudoternary? **(06 Marks)**
b. The loss in a cable defined in debels/km (dB/km). If the signal at beginning of a cable with -3 dB/km has a power of 3 mW. What is the power of the signal at 5 km? **(06 Marks)**
c. Explain the PCM encoder. **(08 Marks)**

3 a. Explain frequency hopping spread spectrum (FHSS). **(10 Marks)**
b. Four 1 Kbps connections are multiplexed together. A unit is 1 bit. Find
i) The duration of 1 bit before multiplexing.
ii) The transmission rate of the link.
iii) The duration of a time slot.
iv) The duration of a frame. **(05 Marks)**
c. Differentiate between circuit switched, datagram networks and virtual circuit networks. **(05 Marks)**

4 a. Explain structure of encoder and decoder for hamming code. **(08 Marks)**
b. Find the codeword, using CRC given dataword 1001 and generator 1011. **(06 Marks)**
c. What is internet checksum? With an example, list the steps undertaken by the sender and receiver for error detection. **(06 Marks)**

PART – B

5 a. Explain stop-and-wait ARQ protocol with neat diagram. **(08 Marks)**
b. What is framing? Explain bit and character stuffing with an example. **(04 Marks)**
c. Write short notes on HDLC. **(08 Marks)**

6 a. Explain CDMA. **(06 Marks)**
b. A slotted ALOHA network transmits 200 bit frames using a shared channel with 200 Kbits/sec bandwidth. Find throughput if system produces i) 1000 frames/sec ii) 500 frames/sec iii) Frames/sec. **(06 Marks)**
c. Explain 802.3 MAC frame format. **(08 Marks)**

7 a. Explain the architecture of IEEE 802.11. **(10 Marks)**
b. Explain connecting devices. **(10 Marks)**

8 a. Draw IPV4 header format and explain. **(08 Marks)**
b. A ISP is granted a block of address starting with 190.100.0.0/16 (655, 536 address). The ISP needs to distribute these addressing to 3 groups of customers.
i) First group has 64 customers each needs 256 address.
ii) Second group has 128 customers each needs 128 address.
iii) The third group has 128 customers each needs 64 address.
Design the subblock and findout. How many addresses are still available after their allocations? **(07 Marks)**
c. Compare between IPV4 and IPV6. **(05 Marks)**

* * * * *

1a. Explain OSI reference model. (10 Marks)

Ans:

LAYERS IN THE OSI MODEL

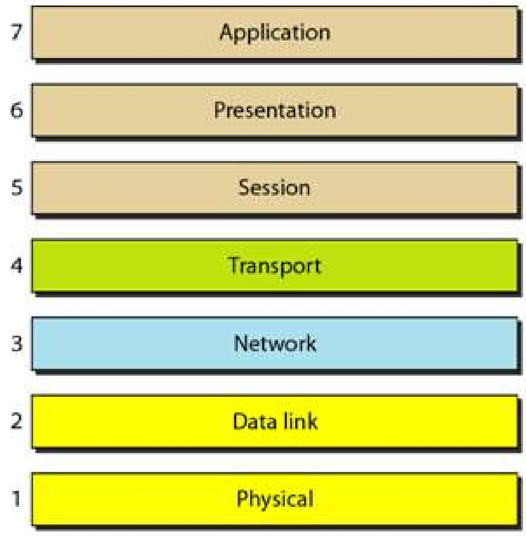


Figure 2.2 *Seven layers of the OSI model*

Physical Layer

• Main Responsibility:

Physical-layer (PL) is responsible for movements of individual bits from one node to another node.

• Other responsibilities:

1) PL defines mechanical/electrical characteristics of the interface & transmission-medium
2) PL defines the type of transmission-medium: Wired or wireless.
3) PL defines the type of encoding i.e. how 0s and 1s are changed to signals.
4) PL defines the transmission-rate.
5) PL deals with the synchronization of the transmitter and receiver.
6) PL defines the nature of the connection ie point-to-point or multipoint configuration
7) PL defines the type of topology: mesh, star, ring or bus.
8) PL defines direction of data-transfer b/w 2 devices: Simplex, Half-duplex or Full-duplex

Data Link Layer

• Main Responsibility:

Data-link-layer (DLL) is responsible for moving frames from one node to another node.

• Other responsibilities:

1) DLL receives & divides the stream of bits from network-layer into frames.
2) DLL provides Physical-addressing
3) DLL provides flow-control.
4) DLL provides error-control.
5) DLL provides access-control.

Network Layer

• Main Responsibility:

Network-layer (NL) is responsible for source-to-destination delivery of a packet, possibly across multiple-networks.

• Other responsibilities:

1) NL provides Logical-addressing
2) NL provides routing of packets.

Transport Layer

• Main Responsibility:

Transport-layer (TL) is responsible for process-to-process delivery of the entire message.

• Other responsibilities:

1) TL provides Service-point Addressing
2) TL is responsible for Segmentation & Reassembly
3) TL provides 2 services: i) connectionless or ii) connection-oriented.
4) TL is responsible for flow-control & error-control.

Session Layer

• Main Responsibility:

Session-layer (SL) establishes, maintains, and synchronizes the interaction between 2 systems.

• Other responsibilities:

1) SL allows 2 systems to start communication with each other in half- or full-duplex.
2) SL provides synchronization

Presentation Layer

• Main Responsibility:

Presentation-layer (PL) is concerned with syntax & semantics of the info. exchanged b/w 2 systems.

• Other responsibilities:

1) PL is responsible for interoperability b/w encoding methods for different computers.
2) PL is responsible for encryption & decryption.
3) PL carries out data compression to reduce the size of the data to be transmitted.

Application Layer

• Main Responsibility:

The application-layer (AL)

→ provides services to the user
→ enables the user to access the network.

• Other responsibilities:

1) Mail Services
2) Directory Services
3) File Transfer, Access, and Management

1b. Explain categories of network and differentiate between them. (10 Marks)

Ans:

Network Types

• Two categories of networks: 1) LAN (Local Area Network) & 2) WAN (Wide Area Network)

LAN

• LAN is used to connect computers in a single office, building or campus (Figure 1.8).
• LAN is usually privately owned network.
• Each host in a LAN has an address that uniquely defines the host in the LAN.
• A packet sent by a host to another host carries both source- & destination-host's addresses.
• LANs use a smart connecting switch.
• The switch is able to
  → recognize the destination address of the packet &
  → guide the packet to its destination.
• The switch
  → reduces the traffic in the LAN &
  → allows more than one pair to communicate with each other at the same time.

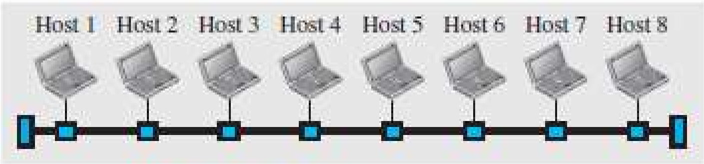


Figure 1.8 . LAN with a common cable

WAN

• WAN is used to connect computers anywhere in the world.
• WAN can cover larger geographical area. It can cover cities, countries and even continents.
• WAN interconnects connecting devices such as switches, routers, or modems.
• Normally, WAN is
  → created & run by communication companies (Ex: BSNL, Airtel)
  → leased by an organization that uses it.
• A WAN can be of 2 types:

1) Point-to-point WAN

➢ A point-to-point WAN is a network that connects 2 communicating devices through a transmission media (Figure 1.9).

Figure 1.9 *A point-to-point WAN*

2) Switched WAN

➢ A switched WAN is a network with more than two ends.
➢ The switched WAN can be the backbones that connect the Internet.
➢ A switched WAN is a combination of several point-to-point WANs that are connected by switches (Figure 1.10).

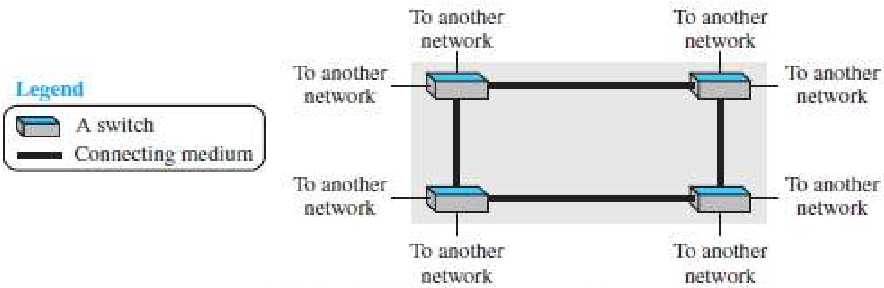
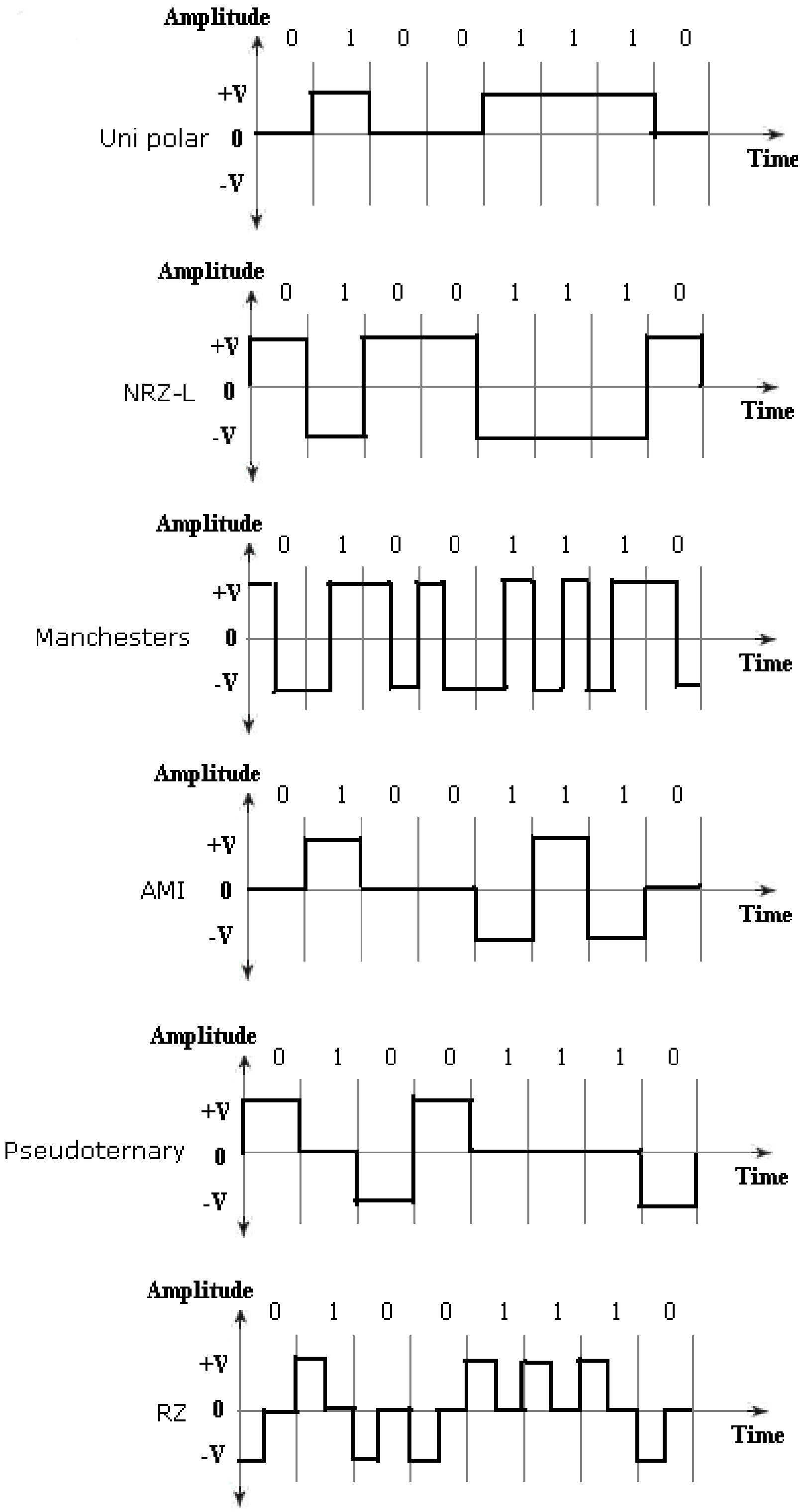


Figure 1.10 *A switched WAN*

Parameters	LAN	WAN
Expands to	Local Area Network	Wide Area Network
Meaning	LAN is used to connect computers in a single office, building or campus	WAN is used to connect computers in a large geographical area such as countries
Ownership of network	Private	Private or public
Range	Small: up to 10 km	Large: Beyond 100 km
Speed	High: Typically 10, 100 and 1000 Mbps	Low: Typically 1.5 Mbps
Propagation Delay	Short	Long
Cost	Low	High
Congestion	Less	More
Design & maintenance	Easy	Difficult
Fault Tolerance	More Tolerant	Less Tolerant
Media used	Twisted pair	Optical fiber or radio waves
Used for	College, Hospital	Internet
Interconnects	LAN interconnects hosts	WAN interconnects connecting devices such as switches, routers, or modems

2a. Represent the given sequence 01001110 in unipolar. Manchesters, AMI, Pseudoternary? (06 Marks)

Ans:



2b. The loss in a cable defined in debels/km (dB/km). If signal at beginning of a cable with -3 dB/km has a power of 3 mW. What is power of the signal at 5 km? (06 Marks)

Ans:

Solution

The loss in the cable in decibels is $5 \times (-0.3) = -1.5$ dB. We can calculate the power as

$$\text{dB} = 10 \log_{10} (P_2 / P_1) = -1.5 \quad \longrightarrow \quad (P_2 / P_1) = 10^{-0.15} = 0.71$$

$$P_2 = 0.71 P_1 = 0.7 \times 2 \text{ mW} = 1.4 \text{ mW}$$

2c. Explain the PCM encoder. (08 Marks)

Ans:

PCM

• PCM is a technique used to change an analog signal to digital data (digitization).

• PCM encoder has 3 processes (Figure 4.21): 1) Sampling 2) Quantization & 3) Encoding.

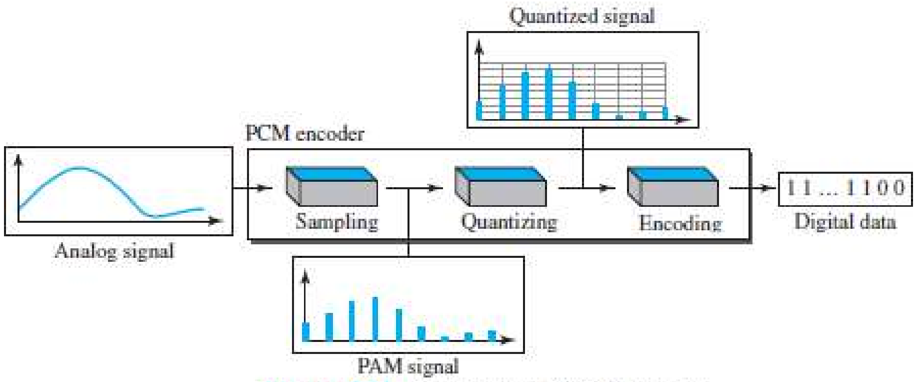


Figure 4.21 Components of PCM encoder

1) Sampling

• We convert the continuous time signal (analog) into the discrete time signal (digital).

• Pulses from the analog-signal are sampled every T_s sec
where T_s is the sample-interval or period.

• The inverse of the sampling-interval is called the sampling-frequency (or sampling-rate).

• Sampling-frequency is given by

$$f_s = 1/T_s.$$

• According to Nyquist theorem,
"The sampling-rate must be at least 2 times the highest frequency, not the bandwidth".
i) If the analog-signal is **low-pass**, the bandwidth and the highest frequency are the same value (Figure 4.23a).
ii) If the analog-signal is **bandpass**, the bandwidth value is lower than the value of the maximum frequency (Figure 4.23b).

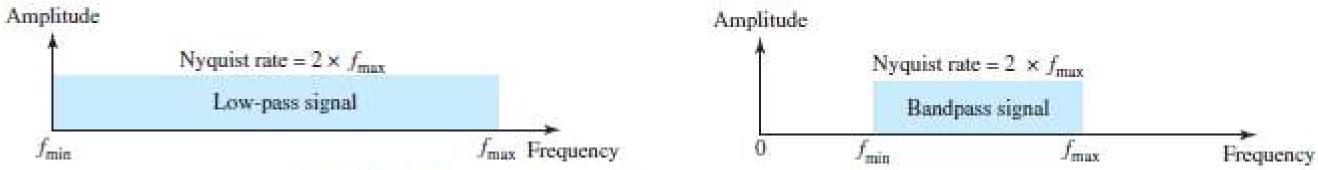


Figure 4.23 Nyquist sampling rate for low-pass and bandpass signals

2) Quantization

• The sampled-signal is quantized.

• Result of sampling is a set of pulses with amplitude-values b/w max & min amplitudes of the signal.

Quantization Level

➢ Let L = number of levels.

➢ The choice of L depends on
→ range of the amplitudes of the analog-signal and
→ how accurately we need to recover the signal.

➢ If the signal has only 2 amplitude values, we need only 2 quantization-levels.
If signal (like voice) has many amplitude values, we need more quantization-levels.

➢ In audio digitizing, L is normally chosen to be 256.
In video digitizing, L is normally thousands.

➢ Choosing lower values of L increases the quantization-error.

➢ Quantization-error is the difference b/w normalized PAM value & quantized values

3) Encoding

• The quantized values are encoded as n-bit code word.

• Relationship between number of quantization-levels (L) & number of bits (n) is given by
$n=\log_2 L$ or $2^n=L$

• The bit-rate is given by:

$$\text{Bit rate} = \text{sampling rate} \times \text{number of bits per sample} = f_s \times n$$

3a. Explain frequency hopping spread spectrum (FHSS). (10 Marks)

Ans:

Frequency Hopping Spread-Spectrum (FHSS)

- This technique uses 'M' different carrier-frequencies that are modulated by the source-signal.
- At one moment, the signal modulates one carrier-frequency.
  At the next moment, the signal modulates another carrier-frequency.
- Although the modulation is done using one carrier-frequency at a time, 'M' frequencies are used in the long run.
- The bandwidth occupied by a source is given by

$$B_{FHSS} >> B$$

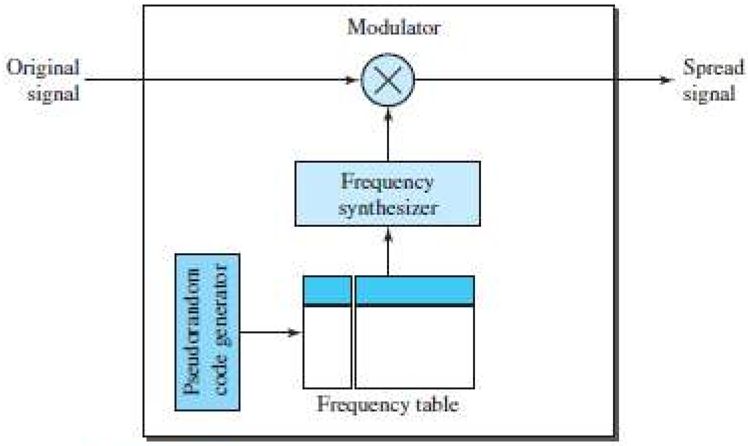


Figure 6.28 *Frequency hopping spread spectrum (FHSS)*

- As shown in Figure 6.28.
  - A pseudorandom code generator (PN) creates a k-bit pattern for every hopping period T_h
  - The frequency-table
    → uses the pattern to find the frequency to be used for this hopping period and
    → passes the frequency to the frequency-synthesizer.
  - The frequency-synthesizer creates a carrier-signal of that frequency.
  - The source-signal modulates the carrier-signal.

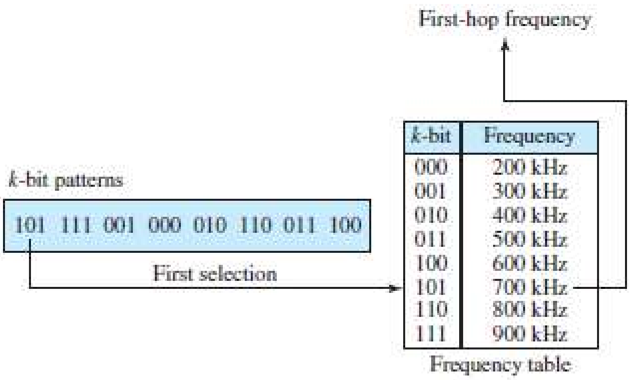


Figure 6.29 *Frequency selection in FHSS*

- As shown in Figure 6.29, assume we have 8 hopping frequencies.
  - Here, M = 8 and k = 3.
  - The pseudorandom code generator will create 8 different 3-bit patterns.
  - These are mapped to 8 different frequencies in the frequency table.
  - The pattern for this station is 101, 111, 001, 000, 010, 111 & 100.
    1) At hopping-period 1, the pattern is 101.
    The frequency selected is 700 kHz; the source-signal modulates this carrier-frequency.
    2) At hopping-period 2, the pattern is 111.
    The frequency selected is 900 kHz; the source-signal modulates this carrier-frequency.

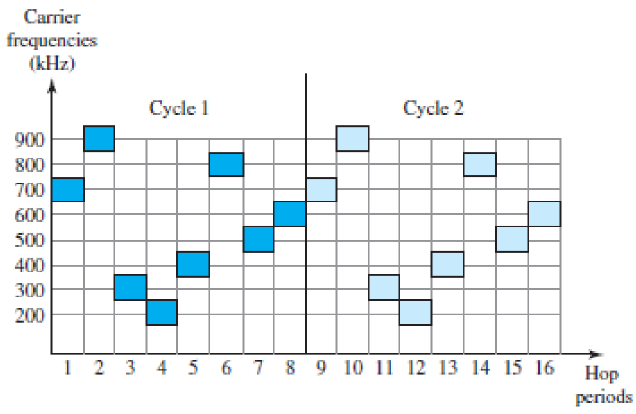


Figure 6.30 *FHSS cycles*

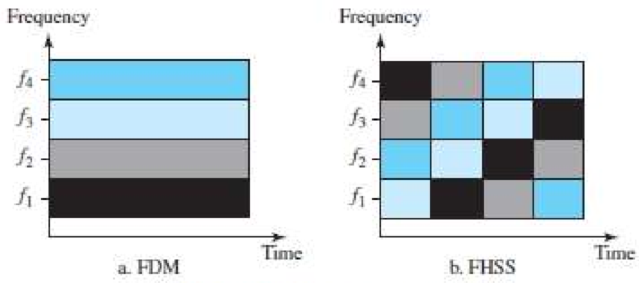


Figure 6.31 *Bandwidth sharing*

- If there are many k-bit patterns & the hopping period is short, a sender & receiver can have privacy.
  If an attacker tries to intercept the transmitted signal, he can only access a small piece of data because he does not know the spreading sequence to quickly adapt himself to the next hop.
- The scheme has also an anti-jamming effect.
  A malicious sender may be able to send noise to jam the signal for one hopping period (randomly), but not for the whole period.

3b. Four 1 Kbps connections are multiplexed together. A unit is 1 bit. Find
i) The duration of 1 bit before multiplexing.
ii) The transmission rate the link
iii) The duration of a time slot.
iv) The duration of a frame. (05 Marks)

Ans:

Solution

We can answer the questions as follows:

1. The duration of 1 bit before multiplexing is 1/1 kbps, or 0.001 s (1 ms).
2. The rate of the link is 4 times the rate of a connection, or 4 kbps.
3. The duration of each time slot is one-fourth of the duration of each bit before multiplexing, or 1/4 ms or 250 μs. Note that we can also calculate this from the data rate of the link, 4 kbps. The bit duration is the inverse of the data rate, or 1/4 kbps or 250 μs.
4. The duration of a frame is always the same as the duration of a unit before multiplexing, or 1 ms. We can also calculate this in another way. Each frame in this case has four time slots. So the duration of a frame is 4 times 250 μs, or 1 ms.

3c. Differentiate between circuit switched, datagram networks and virtual circuit networks. (05 Marks)

Ans:

Circuit Switching	Datagram Packet Switching	Virtual circuit Packet switching
Dedicate transmission path	No dedicate path	No dedicate path
Continuous transmission of data	Transmission of packets	Transmission of packets
Fast enough for interactive	Fast enough for interactive	Fast enough for interactive
Message are not stored	Packets may be stored until delivered	Packets stored until delivered
The path is established for entire conversation	Route established for each packet	Route established for entire conversation
Call setup delay; negligible transmission delay	Packet transmission delay	Call setup delay; Packet transmission delay
Busy signal if called party busy	Sender may be notified if packet not delivered	Sender notified of connection denial
Overload may block call setup; no delay for established calls	Overload increases packet delay	Overload may block call setup; increases packet delay
Electromechanical or computerized switching nodes	Small switching nodes	Small switching nodes
User responsible for message loss protection	Network may be responsible for individual packets	Network may be responsible for packet sequences
Usually no speed or code conversion	Speed and code conversion	Speed and code conversion
Fixed bandwidth	Dynamic use of bandwidth	Dynamic use of bandwidth
No overhead bits after call setup	Overhead bits in each packet	Overhead bits in each packet

4a. Explain structure of encoder and decoder for hamming code. (08 Marks)

Ans:

Hamming Distance

• Hamming distance b/w 2 words is the number of differences between the corresponding bits.
• For example: The Hamming distance d(000, 011) is 2 because 000⊕011= 011 (two 1s).

Parity Check Code C(5, 4)

• This code is a linear block code. This code can detect an odd number of errors.
• A 4-bit data-word is changed to an 5-bit code-word. One extra bit is called the parity-bit.
• The parity-bit is selected to make the total number of 1s in the code-word even.
• Minimum hamming distance d_{min} = 2. This means the code is a single-bit error-detecting code.

Table 10.2 *Simple parity-check code C(5, 4)*

Dataword	Codeword	Dataword	Codeword
0000	00000	1000	10001
0001	00011	1001	10010
0010	00101	1010	10100

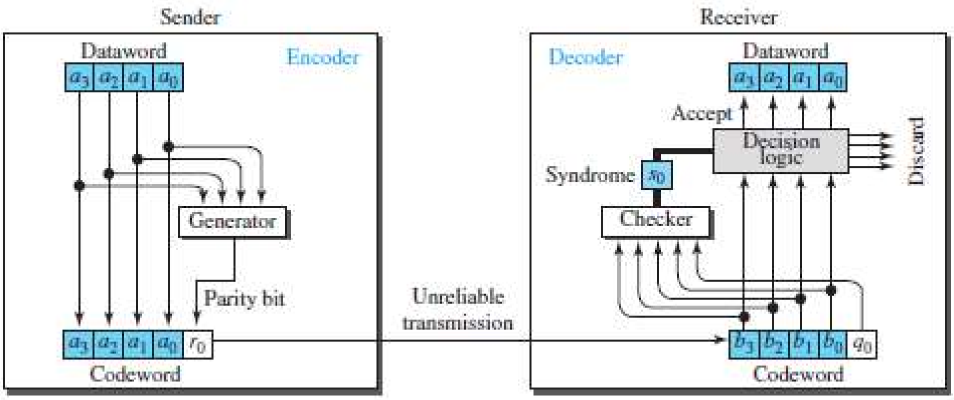


Figure 10.4 *Encoder and decoder for simple parity-check code*

• Here is how it works (Figure 10.4):

1) At Sender

➢ The encoder uses a generator that takes a copy of a 4-bit data-word (a_0, a_1, a_2, and a_3) and generates a parity-bit r_0.
➢ The encoder
→ accepts a copy of a 4-bit data-word (a_0, a_1, a_2, and a_3) and
→ generates a parity-bit r_0 using a generator
→ generates a 5-bit code-word
➢ The parity-bit & 4-bit data-word are added to make the no. of 1s in code-word even.
➢ The addition is done by using the following:

$$r_0 = a_3 + a_2 + a_1 + a_0 \quad \text{(modulo-2)}$$

➢ The result of addition is the parity-bit.
1) If the no. of 1s in data-word = even, result = 0. (r_0=0)
2) If the no. of 1s in data-word = odd, result = 1. (r_0=1)
3) In both cases, the total number of 1s in the code-word is even.
➢ The sender sends the code-word, which may be corrupted during transmission.

2) At Receiver

➢ The receiver receives a 5-bit word.
➢ The checker performs the same operation as the generator with one exception:
The addition is done over all 5 bits.

$$s_0 = b_3 + b_2 + b_1 + b_0 + q_0 \quad \text{(modulo-2)}$$

➢ The result is called the syndrome bit (s_o).
➢ Syndrome bit = 0 when the no. of 1s in received code-word is even; otherwise, it is 1.
➢ The syndrome is passed to the decision logic analyzer.
1) If s_0=0, there is no error in the received code-word. The data portion of the received code-word is accepted as the data-word.
2) If s_0=1, there is error in the received code-word. The data portion of the received code-word is discarded. The data-word is not created.

4b. Find the codeword using CRC given dataword 1001 and generator 1011 (06 Marks)

Ans:

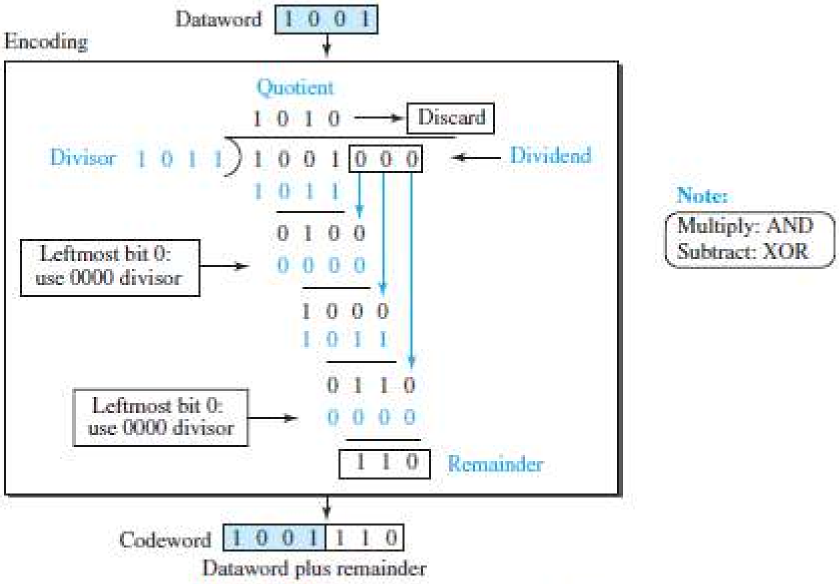


Figure 10.6 *Division in CRC encoder*

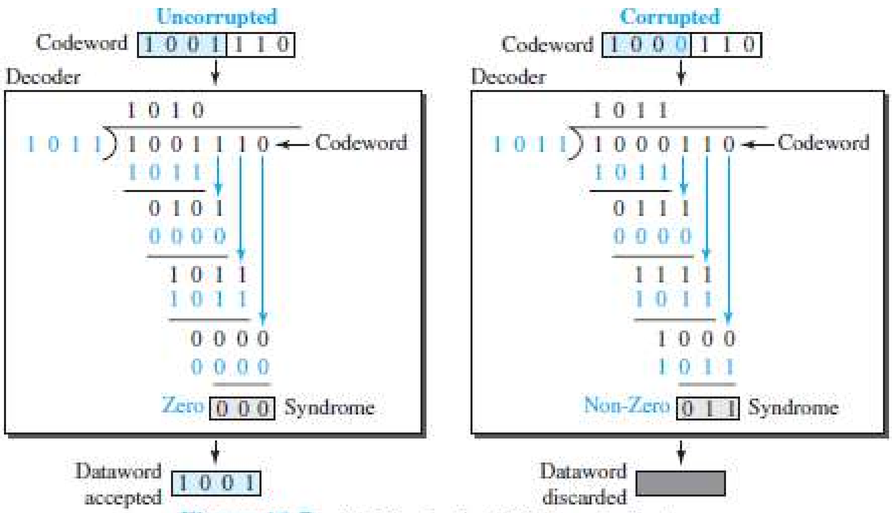


Figure 10.7 *Division in the CRC decoder for two cases*

4c. What is Internet checksum? With an example, list the steps undertaken by the sender and receiver for error detection. (06 Marks)

Ans:

Internet Checksum

- Internet Checksum is an error-detecting technique.
- This is based on the concept of redundancy.
- Traditionally, the Internet has been using a 16-bit checksum.
- The sender or the receiver uses five steps.

Table 10.5 *Procedure to calculate the traditional checksum*

Sender	*Receiver*
1. The message is divided into 16-bit words.	1. The message and the checksum are received.
2. The value of the checksum word is initially set to zero.	2. The message is divided into 16-bit words.
3. All words including the checksum are added using one's complement addition.	3. All words are added using one's complement addition.
4. The sum is complemented and becomes the checksum.	4. The sum is complemented and becomes the new checksum.
5. The checksum is sent with the data.	5. If the value of the checksum is 0, the message is accepted; otherwise, it is rejected.

Algorithm

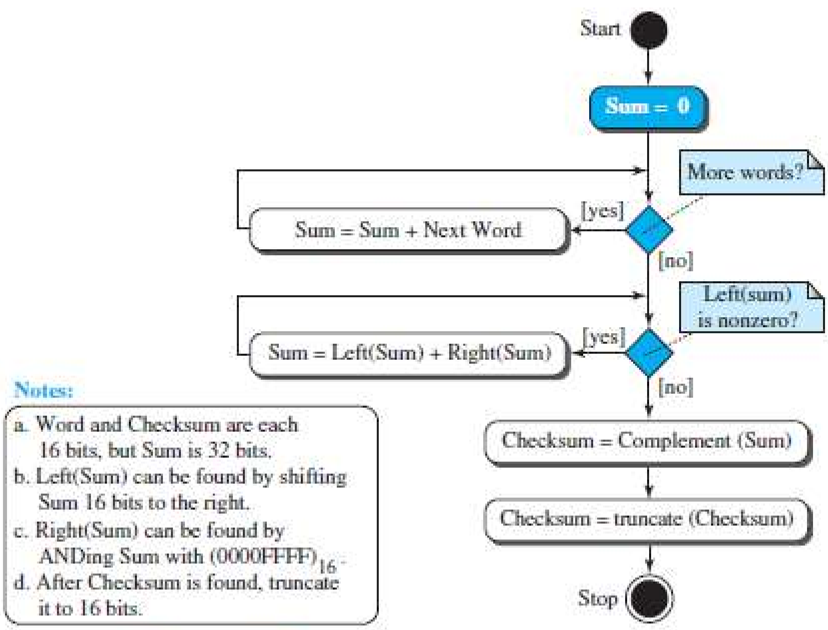


Figure 10.17 *Algorithm to calculate a traditional checksum*

Example

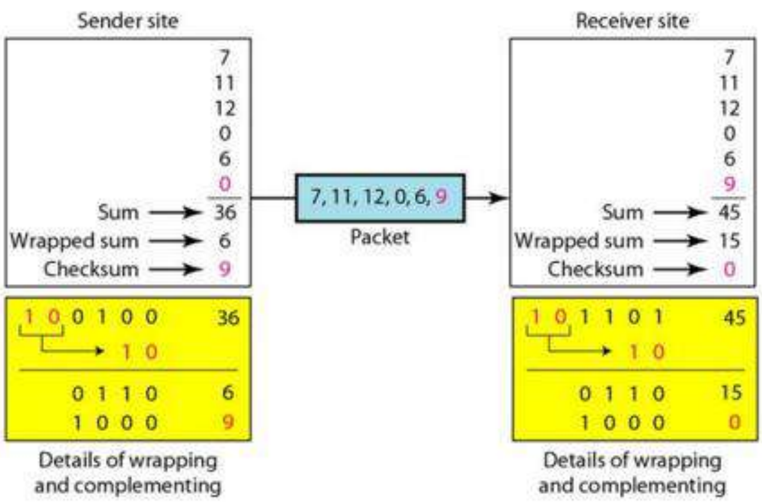


Figure 10.16

5a. Explain stop-and-wait ARQ protocol with neat diagram. (08 Marks)

Ans:

Stop & Wait Protocol

• This uses both flow and error control.
• Normally, the receiver has limited storage-space.
• If the receiver is receiving data from many sources, the receiver may
  → be overloaded with frames &
  → discard the frames.
• To prevent the receiver from being overloaded with frames, we need to tell the sender to slow down.

Design

1) At Sender

➢ The sender
  → sends one frame & starts a timer
  → keeps a copy of the sent-frame and
  → waits for ACK-frame from the receiver (okay to go ahead).

➢ Then,
  1) If an ACK-frame arrives before the timer expires, the timer is stopped and the sender sends the next frame.
  Also, the sender discards the copy of the previous frame.
  2) If the timer expires before ACK-frame arrives, the sender resends the previous frame and restarts the timer

2) At Receiver

➢ To detect corrupted frames, a CRC is added to each data frame.
➢ When a frame arrives at the receiver-site, the frame is checked.
➢ If frame’s CRC is incorrect, the frame is corrupted and discarded.
➢ The silence of the receiver is a signal for the sender that a frame was either corrupted or lost.

FSMs

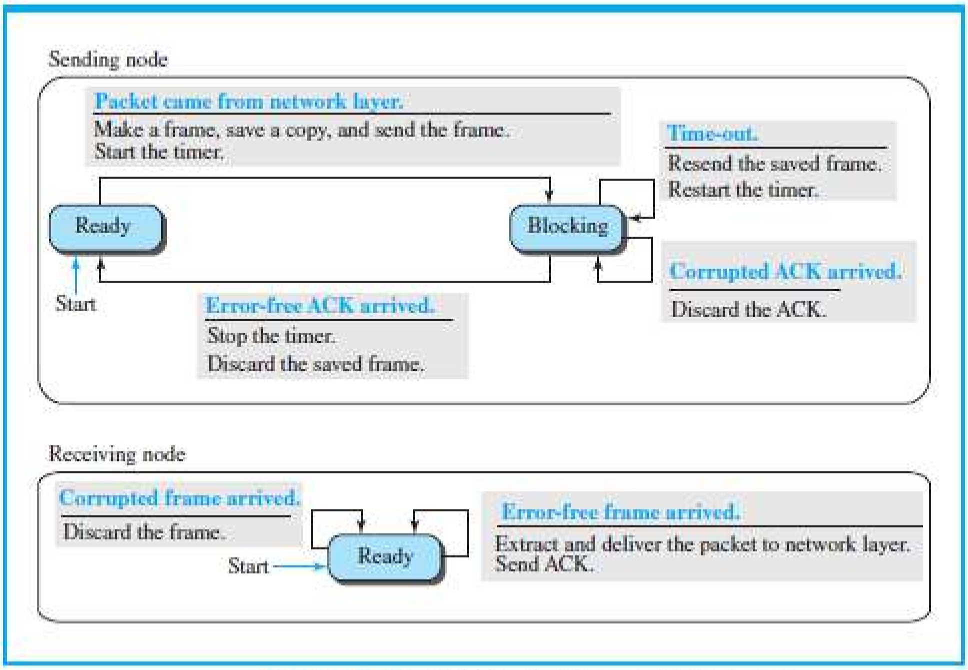


Figure 11.11 FSM for the Stop-and-Wait protocol

• Here is how it works (Figure 11.11):

1) Sender States

➢ Sender is initially in the ready state, but it can move between the ready and blocking state.

i) Ready State: When the sender is in this state, it is only waiting for a packet from the network layer.

If a packet comes from the network layer, the sender creates a frame, saves a copy of the frame, starts the only timer and sends the frame. The sender then moves to the blocking state.

ii) Blocking State: When the sender is in this state, three events can occur:

a) If a time-out occurs, the sender resends the saved copy of the frame and restarts the timer.

b) If a corrupted ACK arrives, it is discarded.

c) If an error-free ACK arrives, the sender stops the timer and discards the saved copy of the frame. It then moves to the ready state.

2) Receiver

➢ The receiver is always in the ready state. Two events may occur:

a) If an error-free frame arrives, the message in the frame is delivered to the network layer and an ACK is sent.

b) If a corrupted frame arrives, the frame is discarded.

5b. What is framing? Explain bit and character stuffing with an example. (04 Marks)

Ans:

Framing

• A frame is a group of bits.
• Framing means organizing the bits into a frame that are carried by the physical layer.
• The data-link-layer needs to form frames, so that each frame is distinguishable from another.

Byte Stuffing

• In byte stuffing, a special byte is added to the data-section of the frame when there is a character with the same pattern as the flag.
• The data-section is stuffed with an extra byte. This byte is called the escape character (ESC), which has a predefined bit pattern.
• When a receiver encounters the ESC character, the receiver
→ removes ESC character from the data-section and
→ treats the next character as data, not a delimiting flag. (Figure 11.2).

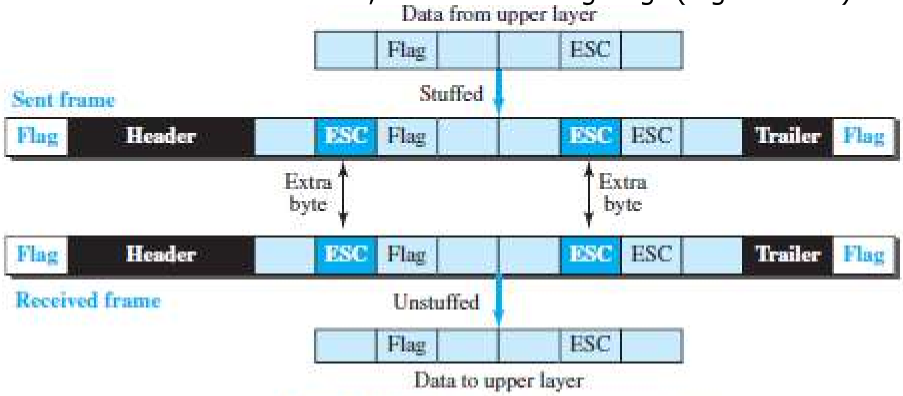


Figure 11.2 *Byte stuffing and unstuffing*

Bit Stuffing

• In bit stuffing, if a 0 and five consecutive 1 bits are encountered, an extra 0 is added. This extra stuffed bit is eventually removed from the data by the receiver. (Figure 11.4).
• This guarantees that the flag field sequence does not inadvertently appear in the frame.

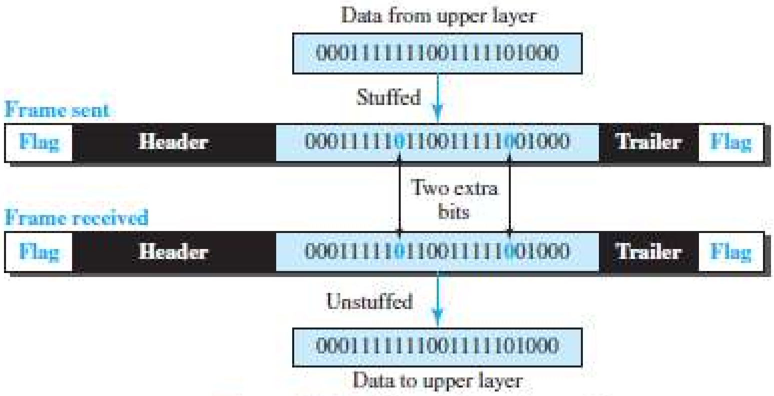


Figure 11.4 *Bit stuffing and unstuffing*

5c. Write short notes on HDLC. (08 Marks)

Ans:

High-Level Data Link Control (HDLC)

• HDLC is a bit-oriented protocol for communication over point-to-point and multipoint links.

Configurations and Transfer Modes

• HDLC provides 2 common transfer modes:

1) Normal response mode (NRM) & 2) Asynchronous balanced mode (ABM).

1) NRM

➢ The station configuration is unbalanced (Figure 11.14).
➢ We have one primary station and multiple secondary stations.
➢ A primary station can send commands, a secondary station can only respond.
➢ The NRM is used for both point-to-point and multiple-point links.

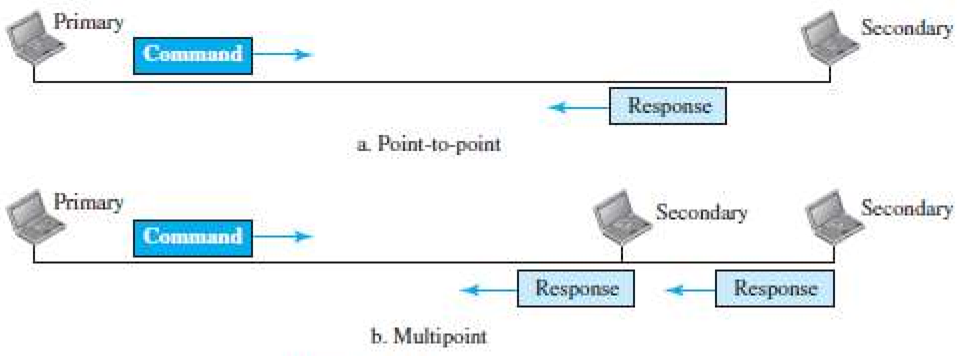


Figure 11.14 *Normal response mode*

2) ABM

➢ The configuration is balanced (Figure 11.15).
➢ Link is point-to-point, and each station can function as a primary and a secondary (acting as peers).
➢ This is the common mode today.

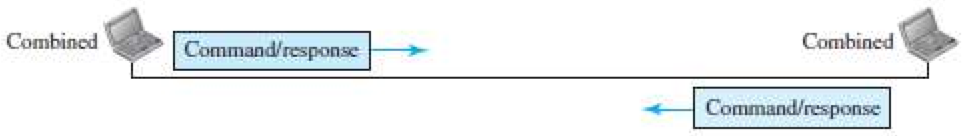


Figure 11.15 *Asynchronous balanced mode*

Framing

• HDLC defines three types of frames:

1) Information frames (I-frames): are used to transport user data and control information relating to user data (piggybacking).
2) Supervisory frames (S-frames): are used only to transport control information.
3) Unnumbered frames (U-frames): are reserved for system management. Information carried by U-frames is intended for managing the link itself.

• Each type of frame serves as an envelope for the transmission of a different type of message.

Frame Format

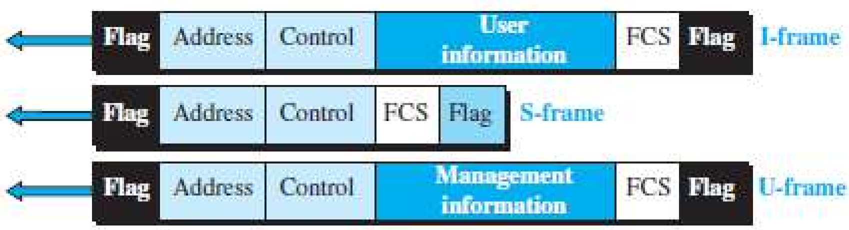


Figure 11.16 *HDLC frames*

• Various fields of HDLC frame (Figure 11.16):

1) Flag Field

➢ This field has a synchronization pattern 01111110.
➢ This field identifies both the beginning and the end of a frame.

2) Address Field

- This field contains the address of the secondary station.
- If a primary station created the frame, it contains a to-address.
- If a secondary creates the frame, it contains a from-address.
- This field can be 1 byte or several bytes long, depending on the needs of the network.

3) Control Field

- This field is one or two bytes used for flow and error control.

4) Information Field

- This field contains the user's data from the network-layer or management information.
- Its length can vary from one network to another.

5) FCS Field

- This field is the error-detection field. (FCS → Frame Check Sequence)
- This field can contain either a 2- or 4-byte standard CRC.

6a. Explain CDMA. (06 Marks)

Ans:

CHANNELIZATION PROTOCOLS

• Channelization is a multiple-access method.
• The available bandwidth of a link is shared b/w different stations in time, frequency, or through code.

CDMA

• CDMA simply means communication with different codes.
• CDMA differs from TDMA because
→ only one channel occupies the entire bandwidth of the link.
• CDMA differs from FDMA because
→ all stations can send data simultaneously; there is no timesharing.

Implementation

• Let us assume we have four stations 1, 2, 3, and 4 connected to the same channel.
• The data from station-1 are d_1, from station-2 are d_2, and so on.
• The code assigned to the first station is c_1, to the second is c_2, and so on.
• We assume that the assigned codes have 2 properties.
1) If we multiply each code by another, we get 0.
2) If we multiply each code by itself, we get 4 (the number of stations).

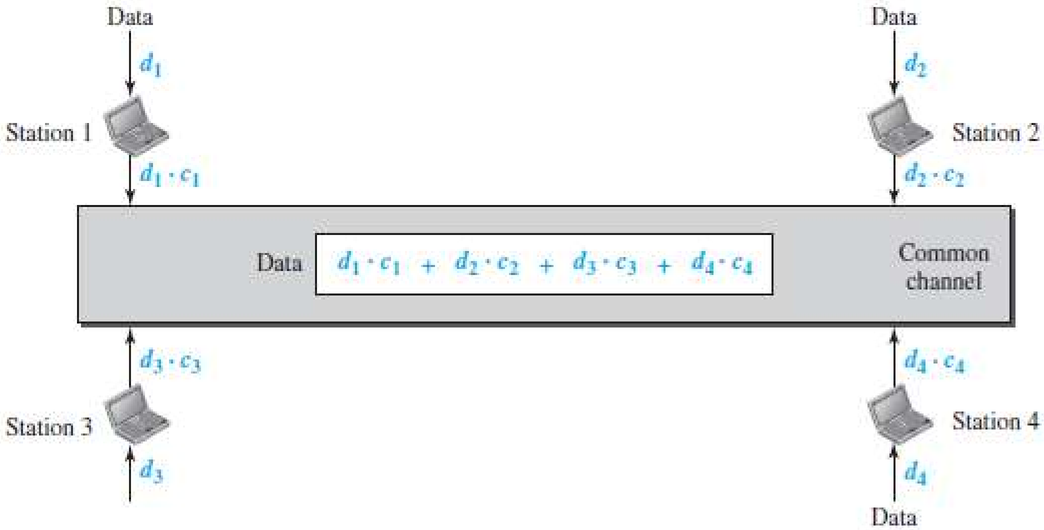


Figure 12.23 *Simple idea of communication with code*

• Here is how it works (Figure 12.23):
➢ Station-1 multiplies the data by the code to get $d_1.c_1$.
➢ Station-2 multiplies the data by the code to get $d_2.c_2$. And so on.
➢ The data that go on the channel are the sum of all these terms.

$$d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4$$

➢ The receiver multiplies the data on the channel by the code of the sender.
➢ For example, suppose stations 1 and 2 are talking to each other.
➢ Station-2 wants to hear what station-1 is saying.
➢ Station-2 multiplies the data on the channel by c_1 the code of station-1.
$(c_1.c_1)=4$, $(c_2.c_1)=0$, $(c_3.c_1)=0$, and $(c_4.c_1)=0$,
Therefore, station-2 divides the result by 4 to get the data from station-1.

$$\begin{aligned} \text{data} &= (d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4) \cdot c_1 \\ &= d_1 \cdot c_1 \cdot c_1 + d_2 \cdot c_2 \cdot c_1 + d_3 \cdot c_3 \cdot c_1 + d_4 \cdot c_4 \cdot c_1 = 4 \times d_1 \end{aligned}$$

Data Representation

• We follow the following rules for encoding:
1) To send a 0 bit, a station encodes the bit as -1
2) To send a 1 bit, a station encodes the bit as +1
3) When a station is idle, it sends no signal, which is interpreted as a 0.

Encoding and Decoding

• Here is how it works (Figure 12.26):

- ➢ Each station multiplies the corresponding number by its chip (its orthogonal sequence).
- ➢ The result is a new sequence which is sent to the channel.
- ➢ The sequence on the channel is the sum of all 4 sequences.
- ➢ Now imagine station-3, which is silent, is listening to station-2.
- ➢ Station-3 multiplies the total data on the channel by the code for station-2, which is [+1 -1 +1-1], to get

$[-1\ -1\ -3\ +1] \bullet [+1\ -1\ +1\ -1] = -4/4 = -1 \quad \rightarrow$ bit 1

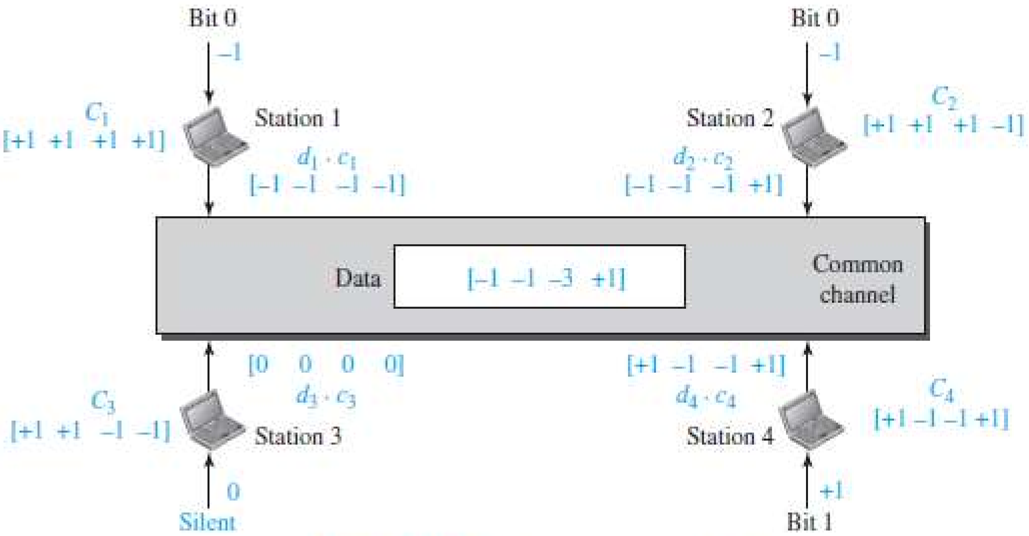


Figure 12.26 *Sharing channel in CDMA*

6b. A slotted ALOHA network transmits 200 bit frames using a shared channel with 200 Kbits/sec bandwidth. Find throughput if system produces

i) 1000 frames/sec

ii) 500 frames/sec

iii) 250 frames/sec. (06 Marks)

Ans:

Solution

The frame transmission time is 200/200 kbps or 1 ms.

a. In this case G is 1. So $S = G \times e^{-G} = 0.368$ (36.8 percent). This means that the throughput is $1000 \times 0.0368 = 368$ frames. Only 368 out of 1000 frames will probably survive. Note that this is the maximum throughput case, percentagewise.

b. Here G is 1/2. In this case $S = G \times e^{-G} = 0.303$ (30.3 percent). This means that the throughput is $500 \times 0.0303 = 151$. Only 151 frames out of 500 will probably survive.

c. Now G is 1/4. In this case $S = G \times e^{-G} = 0.195$ (19.5 percent). This means that the throughput is $250 \times 0.195 = 49$. Only 49 frames out of 250 will probably survive.

6c. Explain 802.3 MAC frame format. (08 Marks)

Ans:

802.3 MAC Frame Format

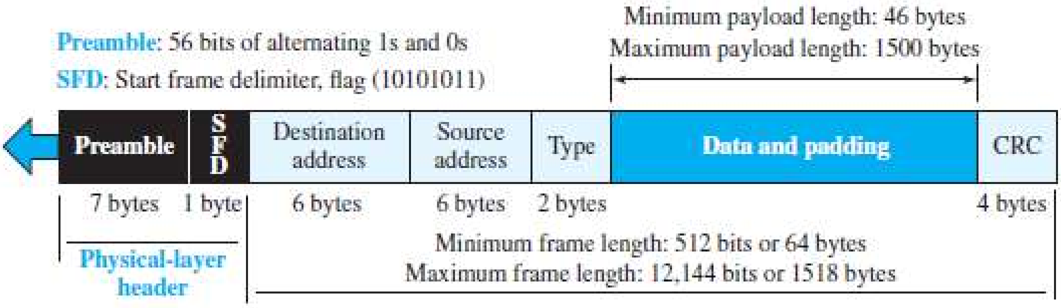


Figure 13.3 *Ethernet frame*

- The Ethernet frame contains 7 fields (Figure 13.3):

1) Preamble

➢ This field contains 7 bytes (56 bits) of alternating 0s and 1s.

➢ This field

→ alerts the receiving-system to the coming frame and

→ enables the receiving-system to synchronize its input timing.

➢ The preamble is actually added at the physical-layer and is not (formally) part of the frame.

2) Start frame delimiter (SFD)

➢ This field signals the beginning of the frame.

➢ The SFD warns the stations that this is the last chance for synchronization.

➢ This field contains the value: 10101011.

➢ The last 2 bits (11) alerts the receiver that the next field is the destination-address.

3) Destination-address (DA)

➢ This field contains the physical-address of the destination-station.

4) Source-address (SA)

➢ This field contains the physical-address of the sender-station.

5) Length or type

➢ This field is defined as a i) type field or ii) length field.

i) In original Ethernet, this field is used as the type field.

¤ Type field defines the upper-layer protocol using the MAC frame.

ii) In IEEE standard, this field is used as the length field.

¤ Length field defines the number of bytes in the data-field.

6) Data

➢ This field carries data encapsulated from the upper-layer protocols.

➢ Minimum data size = 46 bytes. Maximum data size = 1500 bytes.

7) CRC

➢ This field contains error detection information such as a CRC-32.

7a. Explain the architecture of IEEE 802.11. (10 Marks)

Ans:

IEEE 802.11 Architecture

• Two kinds of services defined are: 1) Basic service set (BSS) and 2) Extended service set (ESS)

1) BSS

• IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless-LAN.
• A basic service set is made of (Figure 15.4):
→ stationary or mobile wireless stations and
→ optional central base station, known as the access point (AP).
• There are 2 types of architecture:

1) Ad hoc Architecture

➢ The BSS without an AP is a stand-alone network and cannot send data to other BSSs.
➢ Stations can form a network without the need of an AP.
➢ Stations can locate one another and agree to be part of a BSS.

2) Infrastructure Network

➢ A BSS with an AP is referred to as an infrastructure network.

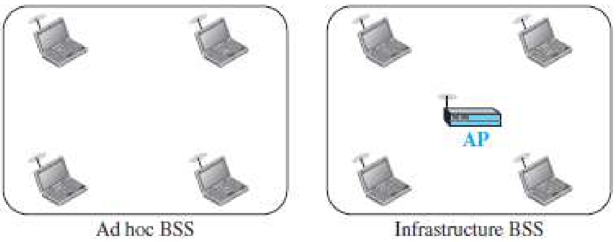


Figure 15.4 *Basic service sets (BSSs)*

2) ESS

• The ESS is made up of 2 or more BSSs with APs (Figure 15.5).
• The BSSs are connected through a distribution-system, which is usually a wired LAN.
• The distribution-system connects the APs in the BSSs.
• IEEE 802.11 does not restrict the distribution-system;
The distribution-system can be any IEEE LAN such as an Ethernet.
• The ESS uses 2 types of stations:
1) Mobile stations are normal stations inside a BSS.
2) Stationary stations are AP stations that are part of a wired LAN.

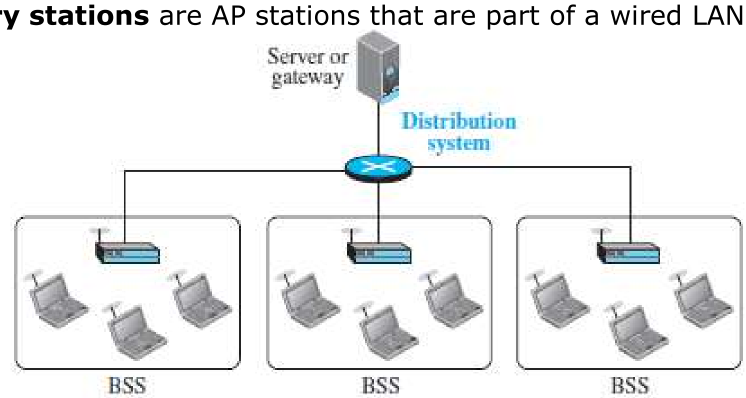


Figure 15.5 *Extended service set (ESS)*

• When BSSs are connected, the stations within reach of one another can communicate without the use of an AP.
• However, communication b/w two stations in two different BSSs usually occurs via two APs.

3) Station Types

• IEEE 802.11 defines three types of stations based on their mobility in a wireless-LAN:
1) No-transition 2) BSS-transition 3) ESS-transition mobility

1) A station with no-transition mobility is either
→ stationary (not moving) or
→ moving only inside a BSS.

2) A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS.

3) A station with ESS-transition mobility can move from one ESS to another.

7b. Explain connecting devices. (10 Marks)

Ans:

CONNECTING DEVICES

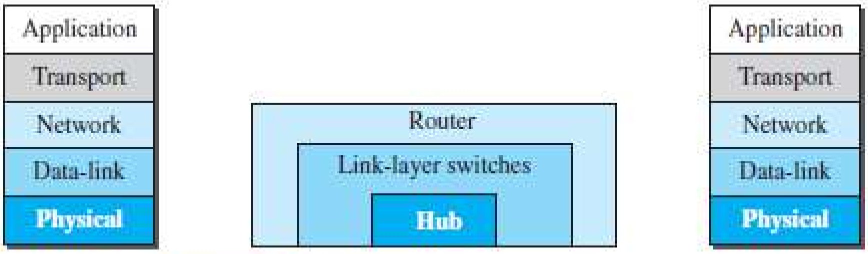


Figure 17.1 *Three categories of connecting devices*

Passive Hubs

• A passive hub is just a connector.
• It connects the wires coming from different branches.
• In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point.
• This type of a hub is part of the media; its location in the Internet model is below the physical layer.

Repeater

• A repeater is a device that operates only in the physical layer (Figure 15.2).
• Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data.
• A repeater receives a signal and, before it becomes too weak or corrupted, regenerates and retimes the original bit pattern.
• The repeater then sends the refreshed signal.
• A repeater can extend the physical length of a LAN.
• A repeater forwards every frame; it has no filtering capability
• A repeater is a regenerator, not an amplifier

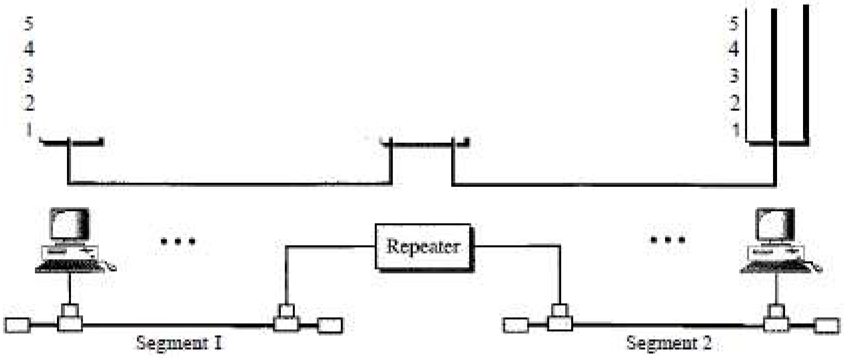


Figure 15.2 *A repeater connecting two segments of a LAN*

Active Hubs

• An active hub is actually a multipart repeater.
• It is normally used to create connections between stations in a physical star topology.
• Hubs can also be used to create multiple levels of hierarchy (Figure 15.4).

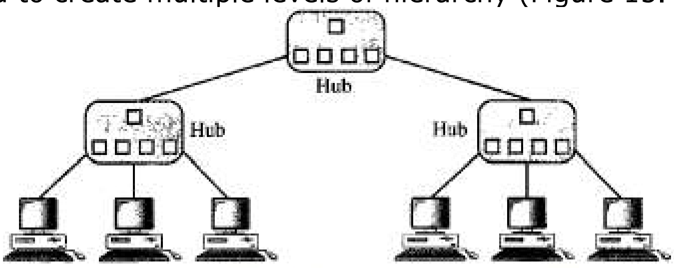


Figure 15.4 *A hierarchy of hubs*

Bridges

• A bridge operates in both the physical and the data link layer (Figure 15.5).
• As a physical layer device, it regenerates the signal it receives.
• As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame.
• A bridge has filtering capability.
• It can check the destination address of a frame and decide if the frame should be forwarded or dropped.
• If the frame is to be forwarded, the decision must specify the port.
• A bridge has a table that maps addresses to ports.
• A bridge has a table used in filtering decisions.
• A bridge does not change the physical (MAC) addresses in a frame

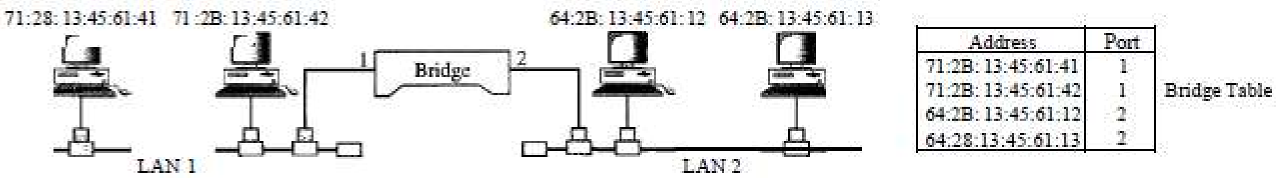


Figure 15.5 *A bridge connecting two LANs*

Routers

• A router is a three-layer device that routes packets based on their logical addresses(host-to-host addressing).
• A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route (Figure 15.11).
• The routing tables are normally dynamic and are updated using routing protocols.

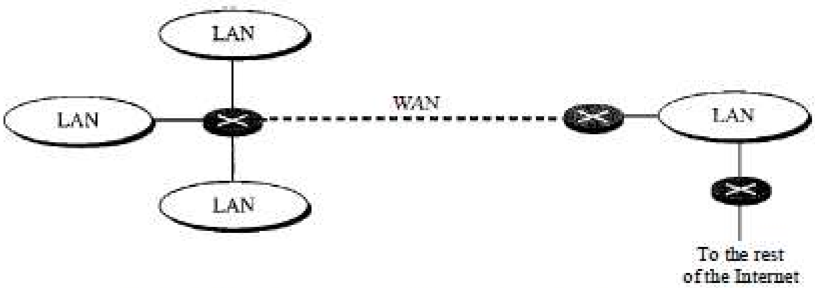


Figure 15.11 *Routers connecting independent LANs and WANs*

Gateway

• A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model.
• A gateway takes an application message, reads it, and interprets it.
• This means that it can be used as a connecting device between two internetworks that use different models.
• For example, a network designed to use the OSI model can be connected to another network using the Internet model.
• The gateway connecting the two systems can take a frame as it arrives from the first system, move it up to the OSI application layer, and remove the message.
• Gateways can provide security.

8a. Draw IPV4 header format and explain. (08 Marks)

Ans:

IP Header Format

• IP uses the packets called datagrams.

• A datagram consist of 2 parts (Figure 19.2): 1) Payload 2) Header.

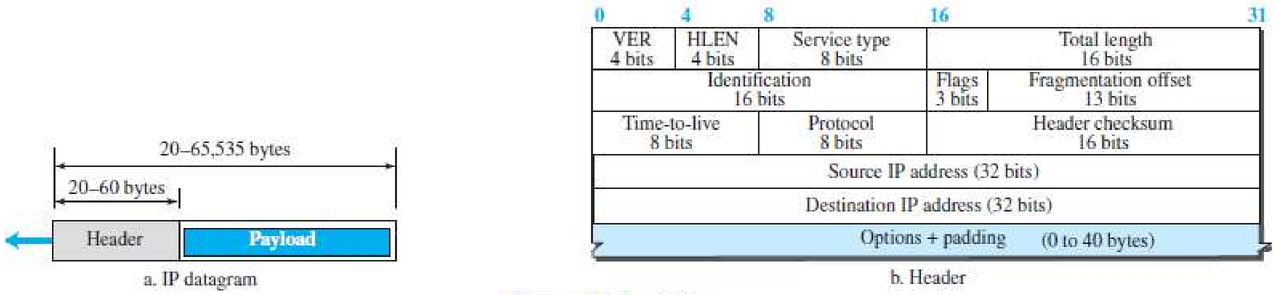


Figure 19.2 *IP datagram*

1) Payload

• Payload (or Data) is the main reason for creating a datagram.

• Payload is the packet coming from other protocols that use the service of IP.

2) Header

• Header contains information essential to routing and delivery.

• IP header contains following fields:

1) Version Number (VER)

➢ This field indicates version number used by the packet. Current version=4

2) Header Length (HLEN)

➢ This field specifies length of header.

➢ When a device receives a datagram, the device needs to know

→ when the header stops and

→ when the data starts.

3) Service Type

➢ This field specifies priority of packet based on delay, throughput, reliability & cost requirements.

4) Total Length

➢ This field specifies the total length of the datagram (header plus data).

➢ Maximum length=65535 bytes.

5) Identification, Flags, and Fragmentation Offset

➢ These 3 fields are used for fragmentation and reassembly of the datagram.

➢ Fragmentation occurs when the size of the datagram is larger than the MTU of the network.

6) Time-to-Live (TTL)

➢ This field is indicates amount of time, the packet is allowed to remain in the network.

➢ If TTL becomes 0 before packet reaches destination, the router

→ discards packet and

→ sends an error-message back to the source.

7) Protocol

➢ This field specifies upper-layer protocol that is to receive the packet at the destination-host.

➢ For example: For TCP, protocol = 6 For UDP, protocol = 17

8) Header Checksum

➢ This field is used to verify integrity of header only.

➢ If the verification process fails, packet is discarded.

9) Source and Destination Addresses

➢ These 2 fields contain the IP addresses of source and destination hosts.

10) Options

➢ This field allows the packet to request special features such as

→ security level

→ route to be taken by packet and

→ timestamp at each router.

➢ This field can also be used for network testing and debugging.

11) Padding

➢ This field is used to make the header a multiple of 32-bit words.

8b. A ISP is granted a block of address starting with 190.100.0.0/16 (655.536 address). The ISP needs to distribute these addressing to 3 groups of customers.

i) First group has 64 customers each needs 256 address.

ii) Second group has 128 customers each needs 128 address.

iii) The third group has 128 customers each needs 64 address.

Design the subblock and findout. How many addresses are still available after their allocations? (07 Marks)

Ans:

Solution:

Group 1

➢ For this group, each customer needs 256 addresses. This means the suffix length is 8 (2^8=256). The prefix length is then 32−8 = 24.

01: 190.100.0.0/24 → 190.100.0.255/24
02: 190.100.1.0/24 →190.100.1.255/24
....
64: 190.100.63.0/24 → 190.100.63.255/24
Total = 64 ×256 = 16,384

Group 2

➢ For this group, each customer needs 128 addresses. This means the suffix length is 7 (2^7=128). The prefix length is then 32 −7 = 25.

The addresses are:
001 : 190.100.64.0/25 → 190.100.64.127/25
002 : 190.100.64.128/25 → 190.100.64.255/25
003: 190.100.127.128/25 → 190.100.127.255/25
Total =128×128 = 16,384

Group 3

➢ For this group, each customer needs 64 addresses. This means the suffix length is 6 (2^6=64). The prefix length is then 32−6 =26.

001:190.100.128.0/26 → 190.100.128.63/26
002:190.100.128.64/26 → 190.100.128.127/26
....
128 :190.100.159.192/26 → 190.100.159.255/26
Total =128 ×64 = 8,192

Number of granted addresses : 65,536
Number of allocated addresses: 40,960
Number of available addresses: 24,576

8c. Compare between IPV4 & IPV6. (05 Marks)

Ans:

	IPv4	IPv6
Address	32 bits (4 bytes) 12:34:56:78	128 bits (16 bytes) 1234:5678:9abc:def0: 1234:5678:9abc:def0
Packet size	576 bytes required, fragmentation optional	1280 bytes required without fragmentation
Packet fragmentation	Routers and sending hosts	Sending hosts only
Packet header	Does not identify packet flow for QoS handling	Contains Flow Label field that specifies packet flow for QoS handling
	Includes a checksum	Does not include a checksum
	Includes options up to 40 bytes	Extension headers used for optional data
IP to MAC resolution	broadcast ARP	Multicast Neighbor Solicitation
Broadcast	Yes	NO
Multicast	Yes	NO
IPSec	optional, external	required

USN | | | | | | | | | | | 10CS55

Fifth Semester B.E. Degree Examination, Dec. 2013/Jan. 2014

Computer Networks – I

Time: 3 hrs. Max. Marks:100

Note: ***Answer FIVE full questions, selecting atleast TWO questions from each part.***

PART – A

1 a. What is data communication? List and explain the five components of data communication system. **(06 Marks)**

b. Discuss the ISO–OSI layered model, bringing out the functionalities of each layer. **(10 Marks)**

c. Differentiate between :
   i) ARP and RARP
   ii) UDP and TCP. **(04 Marks)**

2 a. Write a descriptive note on three causes of transmission impairment. **(08 Marks)**

b. Explain the transmission modes? **(06 Marks)**

c. Explain delta modulation? **(06 Marks)**

3 a. What is FDM? Briefly explain its multiplexing and demultiplexing process. **(06 Marks)**

b. Four sources create 250 characters per second. The frame contain one character from each source and one extra bit for synchronization. Find :
   i) The data rate of each source
   ii) Duration of each character in each source
   iii) Frame rate
   iv) Duration of output frame
   v) Frame size in bits
   vi) Data rate of link. **(06 Marks)**

c. What is time division multiplexing? Explain how statistical TDM overcomes the disadvantages of synchronous TDM. **(08 Marks)**

4 a. Describe different types of errors. **(03 Marks)**

b. Explain error detection and error correction with respect to block coding. **(08 Marks)**

c. Find the codeword, using CRC given data word "1001" and generator "1011". **(09 Marks)**

PART – B

5 a. Explain briefly, with neat figure stop and wait ARQ and Go Back N ARQ. **(12 Marks)**

b. Explain the frame format and transitional phases of point to point protocol. **(08 Marks)**

6 a. Explain :
   i) CSMA
   ii) CSMA/CD **(12 Marks)**

b. Describe 802.3 Mac frame. **(08 Marks)**

7 a. Explain IEEE 802.11 architecture. **(10 Marks)**

b. Bring out the differences between repeaters, bridges, routers and gateways. **(10 Marks)**

8 a. Explain with respect to IPV4, classful addressing and classless addressing. **(10 Marks)**

b. Explain in detail IPV6 packet format. **(10 Marks)**

1a. What is data communication? List and explain the five components of data communication system. (06 Marks)

Ans:

DATA COMMUNICATIONS

• Data Communication is defined as exchange of data between 2 devices over a transmission-medium.
• A communication-system is made up of
  → hardware (physical equipment) and
  → software (programs)
• For data-communication, the communicating-devices must be part of a communication-system.
• Four attributes of a communication-system:

1) Delivery
➢ The system must deliver data to the correct destination.

2) Accuracy
➢ The system must deliver the data accurately.
➢ Normally, the corrupted-data are unusable.

3) Timeliness
➢ The system must deliver audio/video data in a timely manner.
➢ This kind of delivery is called real-time transmission.
➢ Data delivered late are useless.

4) Jitter
➢ Jitter refers to the variation in the packet arrival-time.
➢ In other words, jitter is the uneven delay in the delivery of audio/video packets.

Components of Communication System

• Five components of a communication-system (Figure 1.1):
1) Message
2) Sender
3) Receiver
4) Transmission-Medium
5) Protocol

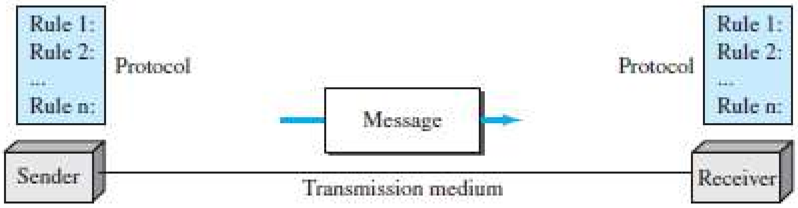


Figure 1.1 *Five components of data communication*

1) Message
➢ Message is the information (or data) to be communicated.
➢ Message may consist of
  → number/text
  → picture or
  → audio/video

2) Sender
➢ Sender is the device that sends the data-message.
➢ Sender can be
  → computer and
  → mobile phone

3) Receiver
➢ Receiver is the device that receives the message.
➢ Receiver can be
  → computer and
  → mobile phone

4) Transmission Medium
➢ Transmission-medium is physical-path by which a message travels from sender to receiver.

- Transmission-medium can be wired or wireless.
- Examples of wired medium:
  - → twisted-pair wire (used in landline telephone)
  - → coaxial cable (used in cable TV network)
  - → fiber-optic cable
- Examples of wireless medium:
  - → radio waves
  - → microwaves
  - → infrared waves (ex: operating TV using remote control)

5) Protocol

- A protocol is a set of rules that govern data-communications.
- In other words, a protocol represents an agreement between the communicating-devices.
- Without a protocol, 2 devices may be connected but not communicating.

1b. Discuss OSI layered model, bringing out functionalities of each layer.(10 Marks)
Ans: For answer, refer Solved Paper June-2013 Q.No.1a.

1c. Differentiate between
i) ARP and RARP
ii) UDP and TCP (04 Marks)

Ans:

i) ARP

- ARP is used to associate a Internet-address with a physical-address.
- In other words, ARP is used to find the physical-address of the node when its Internet-address is known.
- On a typical physical-network, each device on a link is identified by a physical-address.
- Usually, physical-address is imprinted on the NIC (network interface card).

RARP

- RARP is used to find the Internet-address of the node when its physical-address is known.
- RARP is used
  - → when a computer is connected to a network for the first time or
  - → when a diskless computer is booted.

ii) TCP

- TCP is a reliable connection-oriented protocol.
- A connection is established b/w the sender and receiver before the data can be transmitted.
- TCP provides
  - → flow control
  - → error control and
  - → congestion control

UDP

- UDP is the simplest of the 3 transport protocols.
- It is an unreliable, connectionless protocol.
- It does not provide flow, error, or congestion control.
- Each datagram is transported separately & independently.
- It is suitable for application program that
  - → needs to send short messages &
  - → cannot afford the retransmission.

2a. Write a descriptive note on three causes of transmission impairment. (08 Marks)

Ans:

THREE CAUSES OF TRANSMISSION IMPAIRMENT

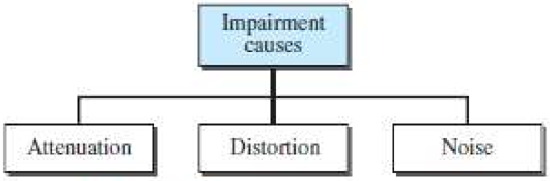


Figure 3.26 *Causes of impairment*

1) Attenuation

• As signal travels through the medium, its strength decreases as distance increases. This is called attenuation (Figure 3.27).
• As the distance increases, attenuation also increases.
• For example:
Voice-data becomes weak over the distance & loses its contents beyond a certain distance.
• To compensate for this loss, amplifiers are used to amplify the signal.

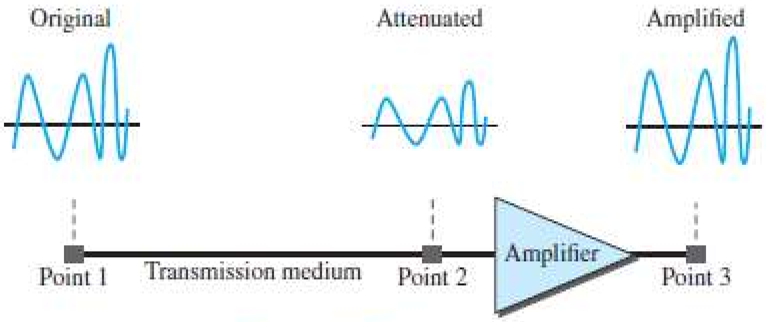


Figure 3.27 *Attenuation*

Decibel

➢ The decibel (dB) measures the relative strengths of
→ 2 signals or
→ one signal at 2 different points.
➢ The decibel is negative if a signal is attenuated.
The decibel is positive if a signal is amplified.

$$dB = 10 \log_{10} \frac{P_2}{P_1}$$

where P_1 and P_2 = powers of a signal at points 1 and 2, respectively.

2) Distortion

• Distortion means that the signal changes its form or shape (Figure 3.29).
• Distortion can occur in a composite signal made of different frequencies.
• Different signal-components
→ have different propagation speed through a medium.
→ have different delays in arriving at the final destination.
• Differences in delay create a difference in phase if delay is not same as the period-duration.
• Signal-components at the receiver have phases different from what they had at the sender.
• The shape of the composite signal is therefore not the same.

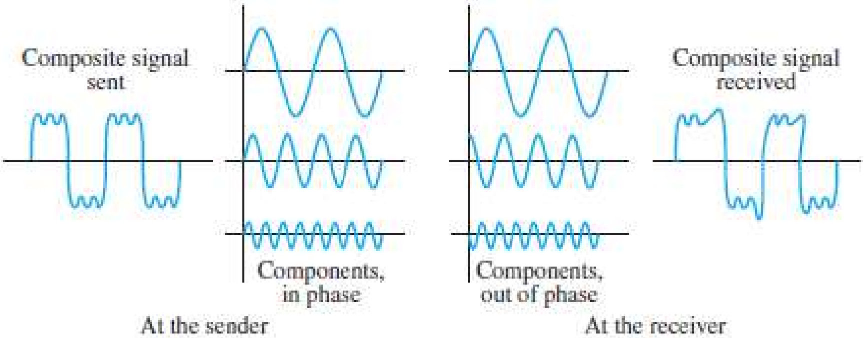


Figure 3.29 *Distortion*

3) Noise

• Noise is defined as an unwanted data (Figure 3.30).
• In other words, noise is the external energy that corrupts a signal.
• Due to noise, it is difficult to retrieve the original data/information.
• Four types of noise:

i) Thermal Noise

➢ It is random motion of electrons in wire which creates extra signal not originally sent by transmitter.

ii) Induced Noise

➢ Induced noise comes from sources such as motors & appliances.
➢ These devices act as a sending-antenna.
The transmission-medium acts as the receiving-antenna.

iii) Crosstalk

➢ Crosstalk is the effect of one wire on the other.
➢ One wire acts as a sending-antenna and the other as the receiving-antenna.

iv) Impulse Noise

➢ Impulse Noise is a spike that comes from power-lines, lightning, and so on.

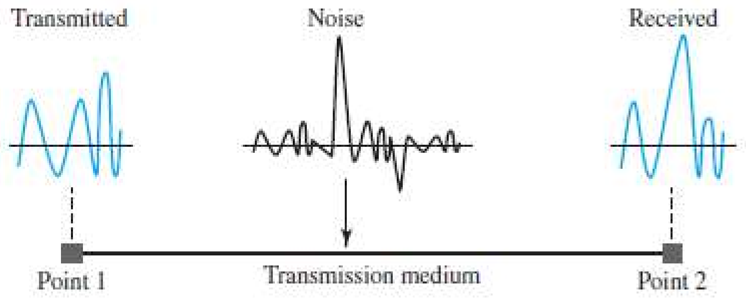


Figure 3.30 *Noise*

Signal-to-Noise Ratio (SNR)

¤ SNR is used to find the theoretical bit-rate limit.
¤ SNR is defined as

$$SNR = \frac{\text{average signal power}}{\text{average noise power}}$$

¤ A high-SNR means the signal is less corrupted by noise.
A low-SNR means the signal is more corrupted by noise.

2b. Explain the transmission modes? (06 Marks)

Ans:

TRANSMISSION MODES

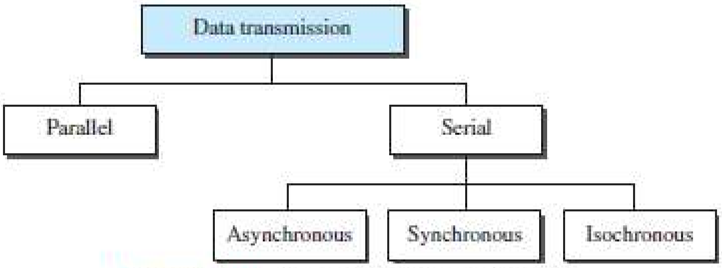


Figure 4.31 *Data transmission and modes*

1) PARALLEL TRANSMISSION

- Multiple bits are sent with each clock-tick (Figure 4.32).
- 'n' bits in a group are sent simultaneously.
- 'n' wires are used to send 'n' bits at one time.
- Each bit has its own wire.
- Typically, the 8 wires are bundled in a cable with a connector at each end.

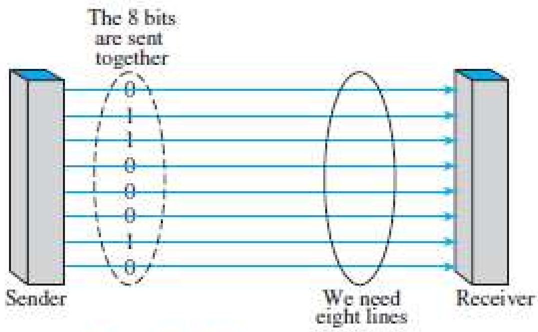


Figure 4.32 *Parallel transmission*

- Advantage:
  1) Speed: Parallel transmission can increase the transfer speed by a factor of n over serial transmission.
- Disadvantage:
  1) Cost: Parallel transmission requires n communication lines just to transmit the data-stream.

2) SERIAL TRANSMISSION

- One bit is sent with each clock-tick using only a single link (Figure 4.33).

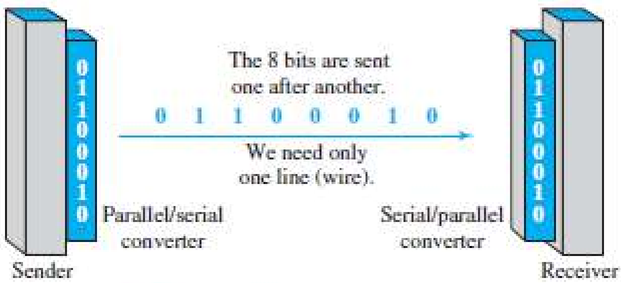


Figure 4.33 *Serial transmission*

- Advantage:
  1) Cost: Serial transmission reduces cost of transmission over parallel by a factor of n.
- Disadvantage:
  1) Since communication within devices is parallel, following 2 converters are required at interface:
     i) Parallel-to-serial converter
     ii) Serial-to-parallel converter
- Three types of serial transmission: asynchronous, synchronous, and isochronous.

i) Asynchronous Transmission

• Asynchronous transmission is so named because the timing of signal is not important (Fig 4.34)
• Prior to data transfer, both sender & receiver agree on pattern of information to be exchanged.
• Normally, patterns are based on grouping the bit-stream into bytes.
• The sender transmits each group to the link without regard to a timer.
• As long as those patterns are followed, the receiver can retrieve the info. w/o regard to a timer.
• There may be a gap between bytes.
• We send
  → 1 start bit (0) at the beginning of each byte
  → 1 stop bit (1) at the end of each byte.
• Start bit alerts the receiver to the arrival of a new group.
  Stop bit lets the receiver know that the byte is finished.
• Here, the term asynchronous means "asynchronous at the byte level".
  However, the bits are still synchronized & bit-durations are the same.

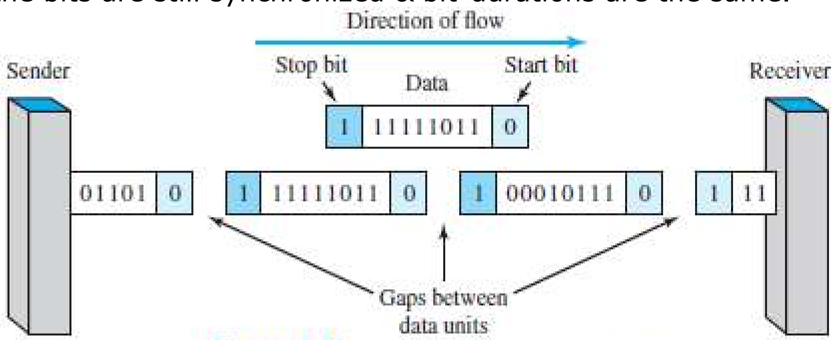


Figure 4.34 *Asynchronous transmission*

ii) Synchronous Transmission

• We send bits one after another without start or stop bits or gaps (Figure 4.35).
• The receiver is responsible for grouping the bits.
• The bit-stream is combined into longer "frames," which may contain multiple bytes.
• If the sender wants to send data in separate bursts, the gaps b/w bursts must be filled with a special sequence of 0s & 1s (that means idle).

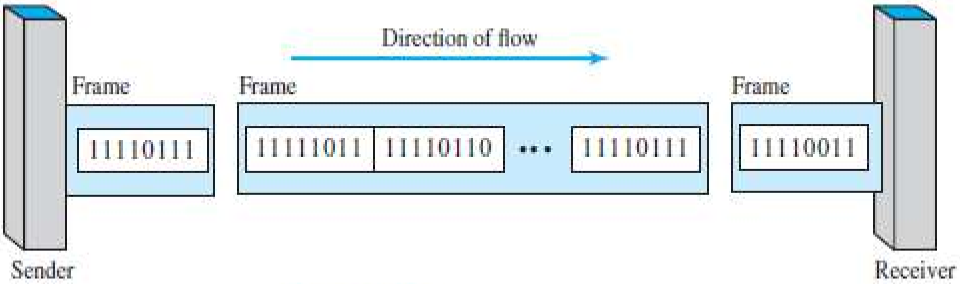


Figure 4.35 *Synchronous transmission*

iii) Isochronous

• Synchronization between characters is not enough; the entire stream of bits must be synchronized.
• The isochronous transmission guarantees that the data arrive at a fixed rate.
• In real-time audio/video, jitter is not acceptable. Therefore, synchronous transmission fails.
• For example: TV images are broadcast at the rate of 30 images per second. The images must be viewed at the same rate.

2c. Explain delta modulation. (06 Marks)

Ans:

Delta Modulation (DM)

• PCM finds the value of the signal amplitude for each sample; DM finds the change from the previous sample.

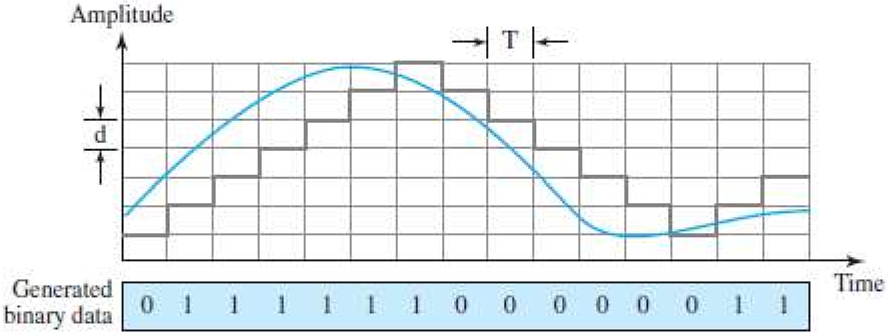


Figure 4.28 *The process of delta modulation*

Modulator

➢ The modulator is used at the sender site to create a stream of bits from an analog signal.

➢ The process records the small positive or negative changes, called delta δ.

➢ If the delta is positive, the process records a 1; if it is negative, the process records a 0.

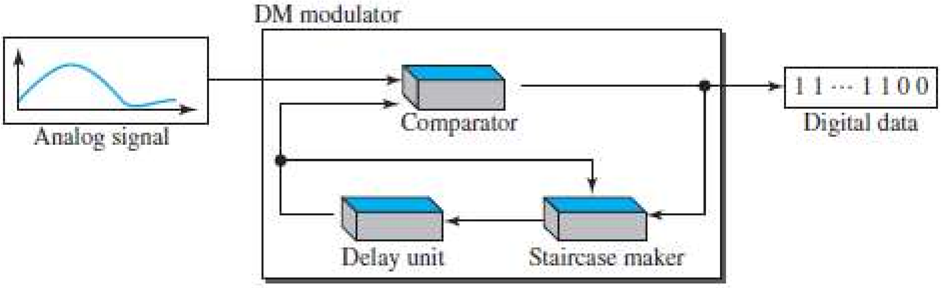


Figure 4.29 *Delta modulation components*

Demodulator

➢ The demodulator takes the digital data and, using the staircase maker and the delay unit, creates the analog signal.

➢ The created analog signal, however, needs to pass through a low-pass filter for smoothing.

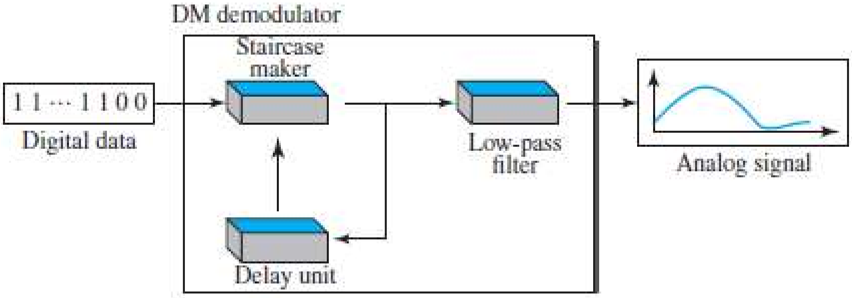


Figure 4.30 *Delta demodulation components*

Quantization Error

➢ It is obvious that DM is not perfect.

➢ Quantization error is always introduced in the process.

➢ The quantization error of DM, however, is much less than that for PCM.

3a. What is FDM? Briefly explain its multiplexing & demultiplexing process. (06 Marks)
Ans:
Frequency Division Multiplexing (FDM)
• FDM is an analog multiplexing technique that combines analog signals (Figure 6.3).
• FDM can be used when the bandwidth of a link is greater than the combined bandwidths of the signals to be transmitted..

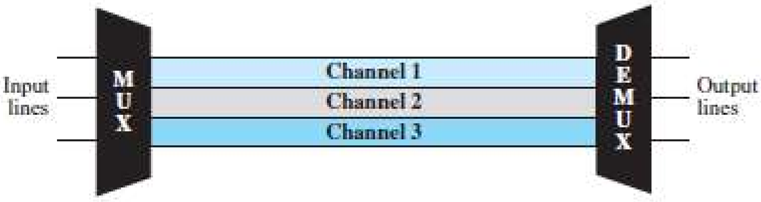


Figure 6.3 *Frequency-division multiplexing*

1) Multiplexing Process
• Here is how it works (Figure 6.4):
1) Each sending-device generates modulated-signals with different carrier-frequencies (f1, f2, & f3).
2) Then, these modulated-signals are combined into a single multiplexed-signal.
3) Finally, the multiplexed-signal is transported by the link.

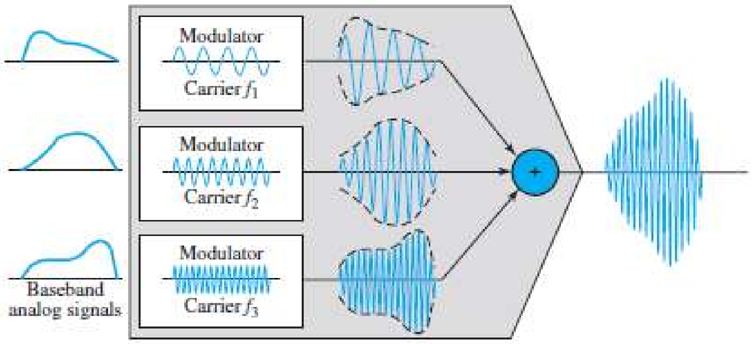


Figure 6.4 *FDM process*

• Carrier-frequencies are separated by sufficient bandwidth to accommodate the modulated-signal.
• Channels can be separated by strips of unused bandwidth called guard bands.
• Guard bands prevent signals from overlapping.
• In addition, carrier-frequencies must not interfere with the original data frequencies.
• Although FDM is considered as analog multiplexing technique, the sources can produce digital-signal.
• The digital-signal can be sampled, changed to analog-signal, and then multiplexed by using FDM.

2) Demultiplexing Process
• Here is how it works (Figure 6.5):
1) The demultiplexer uses filters to divide the multiplexed-signal into individual-signals.
2) Then, the individual signals are passed to a demodulator.
3) Finally, the demodulator
→ separates the individual signals from the carrier signals and
→ passes the individual signals to the output-lines.

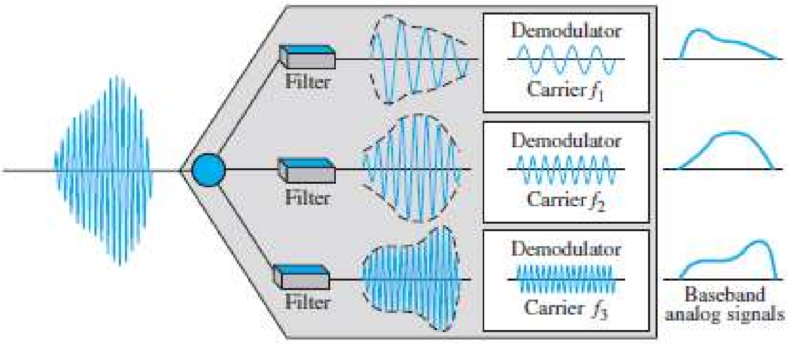


Figure 6.5 *FDM demultiplexing example*

3b. Four sources create 250 characters per second. The frame contain one character from each source and one extra bit for synchronization. Find

i) The data rate of each source
ii) Duration of each character in each source
iii) Frame rate
iv) Duration of output frame
v) Frame size in bits
vi) Data rate of link (06 Marks)

Ans:

Solution

We can answer the questions as follows:

1. The data rate of each source is $250 \times 8 = 2000$ bps = 2 kbps.
2. Each source sends 250 characters per second; therefore, the duration of a character is 1/250 s, ter is 1/250 s, or 4 ms.
3. Each frame has one character from each source, which means the link needs to send eeds to send 250 frames per second to keep the transmission rate of each source.
4. The duration of each frame is 1/250 s, or 4 ms. Note that the duration of each frame is the frame is the same as the duration of each character coming from each source.
5. Each frame carries 4 characters and 1 extra synchronizing bit. This means that each frame is each frame is $4 \times 8 + 1 = 33$ bits.
6. The link sends 250 frames per second, and each frame contains 33 bits. This means that the leans that the data rate of the link is 250×33, or 8250 bps. Note that the bit rate of the link is greater than s greater than the combined bit rates of the four channels. If we add the bit rates of four channels, we get nnels, we get 8000 bps. Because 250 frames are traveling per second and each contains 1 extra bit for extra bit for synchronizing, we need to add 250 to the sum to get 8250 bps.

3c. What is TDM? Explain how TDM overcomes the disadvantages of synchrononous TDM. (08 Marks)

Ans:

Time-Division Multiplexing (TDM)

- TDM is a digital multiplexing technique that combines digital signals (Figure 6.12).
- TDM combines several low-rate channels into one high-rate one.
- Each connection occupies a portion of time in the link.

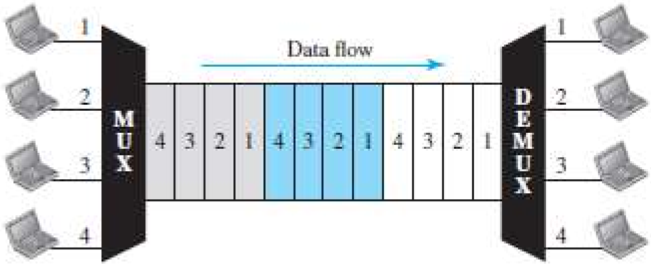


Figure 6.12 *TDM*

- Two types of TDM:
  1) Synchronous and 2) Statistical.

Statistical TDM

- Problem: Synchronous TDM is not efficient.
  For ex: If a source does not have data to send, the corresponding slot in the output-frame is empty (Figure 6.26a).
  Solution: Use statistical TDM (Figure 6.26b).
  Slots are dynamically allocated to improve bandwidth-efficiency.
  Only when an input-line has data to send, the input-line is given a slot in the output-frame.
- The number of slots in each frame is less than the number of input-lines.
- The multiplexer checks each input-line in round robin fashion.
  If the line has data to send;
  Then, multiplexer allocates a slot for an input-line;
  Otherwise, multiplexer skips the line and checks the next line.

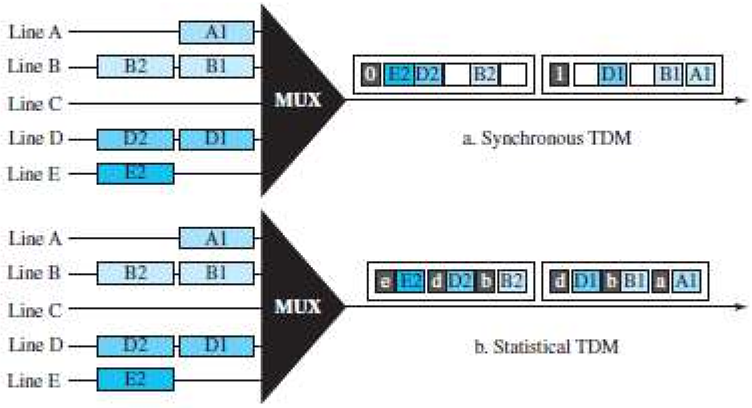


Figure 6.26 *TDM slot comparison*

1) Addressing

Synchronous TDM	Statistical TDM
An output-slot needs to carry only data of the destination (Figure 6.26a).	An output-slot needs to carry both data & address of the destination (Figure 6.26b).
There is no need for addressing. Synchronization and pre-assigned relationships between the inputs and outputs serve as an address.	There is no fixed relationship between the inputs and outputs because there are no pre-assigned or reserved slots. We need to include the address of the receiver inside each slot to show where it is to be delivered.

2) Slot Size

➢ Usually, a block of data is many bytes while the address is just a few bytes.
➢ A slot carries both data and address.
➢ Therefore, address-size must be very small when compared to data-size.
This results in efficient transmission.

3) No Synchronization Bit

➢ In statistical TDM, the frames need not be synchronized, so synchronization-bits are not needed.

4) Bandwidth

➢ Normally, the capacity of the link is less than the sum of the capacities of each channel.
➢ The designers define the capacity of the link based on the statistics of the load for each channel.

4a. Describe different types of errors. (03 Marks)

Ans:

Types of Errors

• When bits flow from 1 point to another, they are subject to unpredictable-changes '.' of interference.
• The interference can change the shape of the signal.
• Two types of errors: 1) Single-bit error 2) Burst-error.

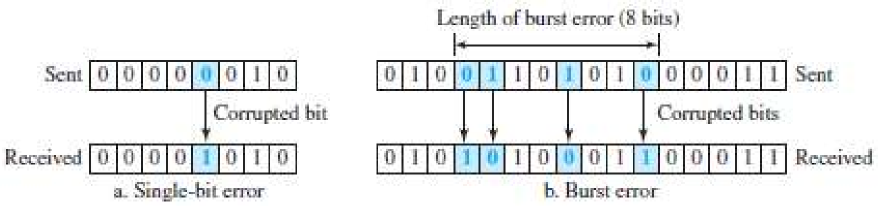


Figure 10.1 *Single-bit and burst error*

1) Single-Bit Error

➢ Only 1 bit of a given data is changed
→ from 1 to 0 or
→ from 0 to 1 (Figure 10.1a).

2) Burst Error

➢ Two or more bits in the data have changed
→ from 1 to 0 or
→ from 0 to 1 (Figure 10.1b).
➢ A burst-error occurs more than a single-bit error. This is because:
Normally, the duration of noise is longer than the duration of 1-bit.
➢ When noise affects data, the noise also affects the bits.
➢ The no. of corrupted-bits depends on
→ data-rate and
→ duration of noise.

4b. Explain error detection and error correction wrt block coding. (08 Marks)

Ans:

Block Coding

• The message is divided into k-bit blocks. These blocks are called data-words.
• Here, r-redundant-bits are added to each block to make the length n=k+r.
• The resulting n-bit blocks are called code-words.
• Block-coding process is 1-to-1; the same data-word is always encoded as the same code-word.

Error Detection

• If the following 2 conditions are met, the receiver can detect a change in the original code-word:
  1) The receiver has a list of valid code-words.
  2) The original code-word has changed to an invalid code-words.

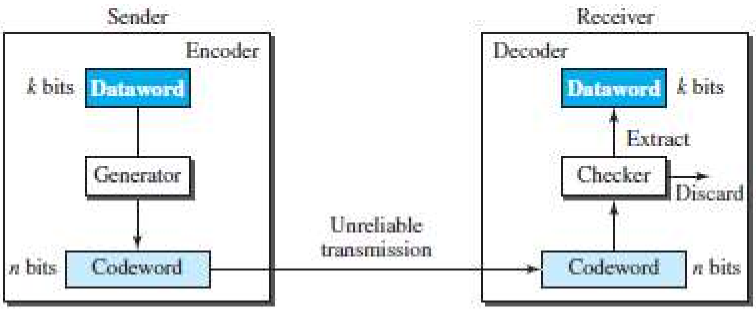


Figure 10.2 *Process of error detection in block coding*

• Here is how it works (Figure 10.2):
  1) At Sender
  i) The sender creates code-words out of data-words by using a generator.
  The generator applies the rules and procedures of encoding.
  ii) During transmission, each code-word sent to the receiver may change.
  2) At Receiver
  i) a) If the received code-word is the same as one of the valid code-words,
  the code-word is accepted;
  the corresponding data-word is extracted for use.
  b) If the received code-word is invalid, the code-word is discarded.
  ii) However, if the code-word is corrupted but the received code-word still matches a valid code-word, the error remains undetected.

• An error-detecting code can detect only the types of errors for which it is designed; other types of errors may remain undetected.

Example

Let us assume that $k = 2$ and $n = 3$. Table 10.1 shows the list of datawords and codewords.

Table 10.1 *A code for error detection*

Dataword	*Codeword*	*Dataword*	*Codeword*
00	000	10	101
01	011	11	110

Assume the sender encodes the dataword 01 as 011 and sends it to the receiver. Consider the following cases:

1. The receiver receives 011. It is a valid codeword. The receiver extracts the dataword 01 from it.
2. The codeword is corrupted during transmission, and 111 is received (the leftmost bit is corrupted). This is not a valid codeword and is discarded.
3. The codeword is corrupted during transmission, and 000 is received (the right two bits are corrupted). This is a valid codeword. The receiver incorrectly extracts the dataword 00. Two corrupted bits have made the error undetectable.

4c. Find code word, using CRC given data word '1001' and generator '1011'. (09 Marks)

Ans: **For answer, refer Solved Paper June-2013 Q.No.4b.**

5a. Explain briefly, with figure i) Stop and Wait ARQ and ii) Go Back N ARQ. (12 Marks)

Ans (i): **For answer, refer Solved Paper June-2013 Q.No.5a.**

Ans (ii):

Go-Back-N ARQ Protocol

• We send several frames before receiving acknowledgments; we keep a copy of these frames until the acknowledgments arrive.

Sequence-numbers

- Frames from a sending station are numbered sequentially.
- If m bits are used for sequence-number, the sequence-numbers range from 0 to 2^{m-1}.
  For example, if m=4, the only sequence-numbers are 0 to 15.
- However, we can repeat the sequence.
- So the sequence-numbers are
  0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,0,1,2,3,4,5,6,7,8,9,10,11,...

Sliding Window

- Sliding window defines the range of sequence-numbers that can be used for the sender & receiver.
- The range which is the used for the sender is called the send sliding window.
  The range that is the used for the receiver is called the receiver sliding window.
- The send window is an imaginary box covering the sequence-numbers of the data-frames.
- In each window position,
  Some sequence-numbers define the frames that have been sent.
  Some sequence-numbers define the frames that can be sent.
- The maximum size of the window is $2^m - 1$.
- The size can be fixed and set to the maximum value.
- Figure 11.12 shows a sliding window of size 15 (m =4).

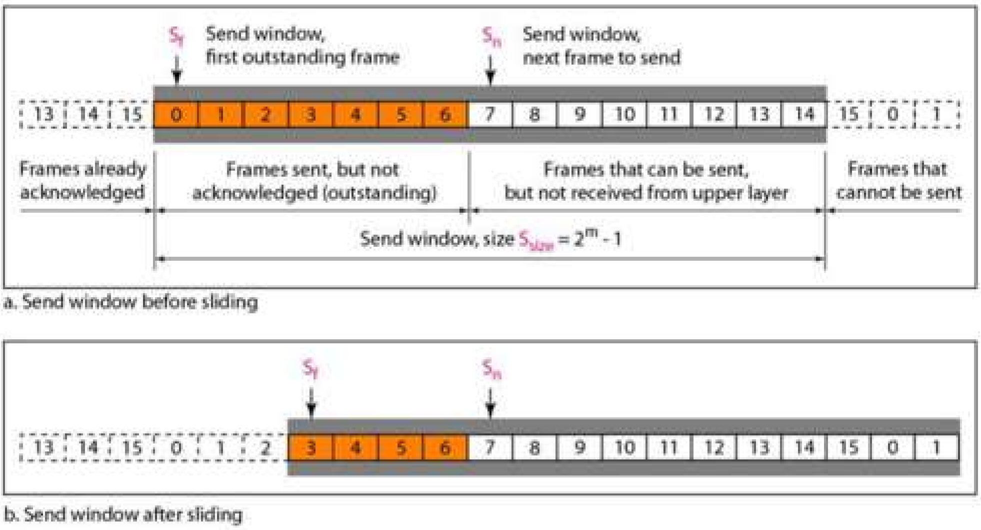


Figure 11.12 *Send window for Go-Back-NARQ*

5b. Explain frame format and transitional phases of point to point protocol. (08 Marks)

Ans:

PPP Frame Format (Point to Point Protocol)

• PPP uses a character-oriented (or byte-oriented) frame (Figure 11.20).

Figure 11.20 *PPP frame format*

• Various fields of PPP frame are:

1) Flag
- This field has a synchronization pattern 01111110.
- This field identifies both the beginning and the end of a frame.

2) Address
- This field is set to the constant value 11111111 (broadcast address).

3) Control
- This field is set to the constant value 00000011.
- PPP does not provide any flow control.
- Error control is also limited to error detection.

4) Protocol
- This field defines what is being carried in the payload field.
- Payload field carries either i) user data or ii) other control information.
- By default, size of this field = 2 bytes.

5) Payload field
- This field carries either i) user data or ii) other control information.
- By default, maximum size of this field = 1500 bytes.
- This field is byte-stuffed if the flag-byte pattern appears in this field.
- Padding is needed if the payload-size is less than the maximum size.

6) FCS
- This field is the PPP error-detection field.
- This field can contain either a 2- or 4-byte standard CRC.

PPP Transition Phases

• The transition diagram starts with the dead state (Figure 11.21).

1) Dead State
- In dead state, there is no active carrier and the line is quiet.

2) Establish State
- When 1 of the 2 nodes starts communication, connection goes into the establish state.
- In establish state, options are negotiated between the two parties.

3) Authenticate State
- If the 2 parties agree that they need authentication,
  Then the system needs to do authentication;
  Otherwise, the parties can simply start communication.

4) Open State
- Data transfer takes place in the open state.

5) Terminate State
- When 1 of the endpoints wants to terminate connection, system goes to terminate state

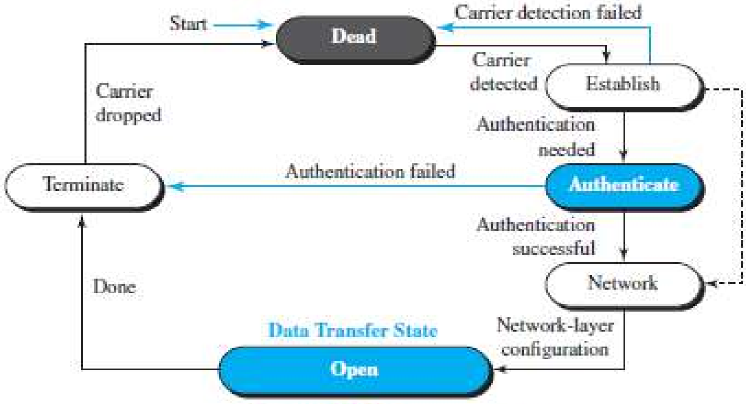


Figure 11.21 *Transition phases*

6a. Explain i) CSMA ii) CSMA/CD. (12 Marks)

Ans (i):

CSMA

- CSMA is based on the principle "sense before transmit" or "listen before talk."
- Here is how it works:
  1) Each station checks the state of the medium: idle or busy.
  2) i) If the medium is idle, the station sends the data.
     ii) If the medium is busy, the station defers sending.
- CSMA can reduce the possibility of collision, but it cannot eliminate it.

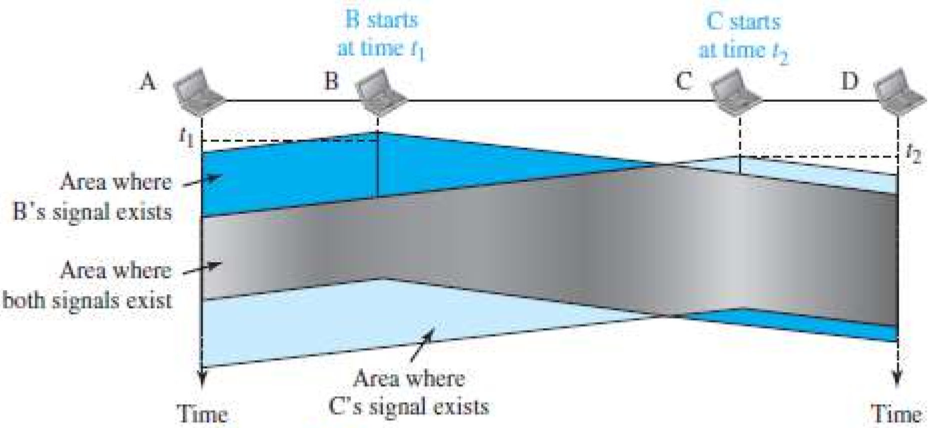


Figure 12.7 *Space/time model of a collision in CSMA*

Vulnerable Time

➢ The vulnerable time is the propagation time T_p. (Figure 12.7).

➢ Collision occurs when
  → a station sends a frame, and
  → other station also sends a frame during propagation time.

Persistence Methods

➢ Q: What should a station do if the channel is busy or idle?
  Three methods can be used to answer this question:
  1) 1-persistent method 2) Non-persistent method and 3) p-persistent method

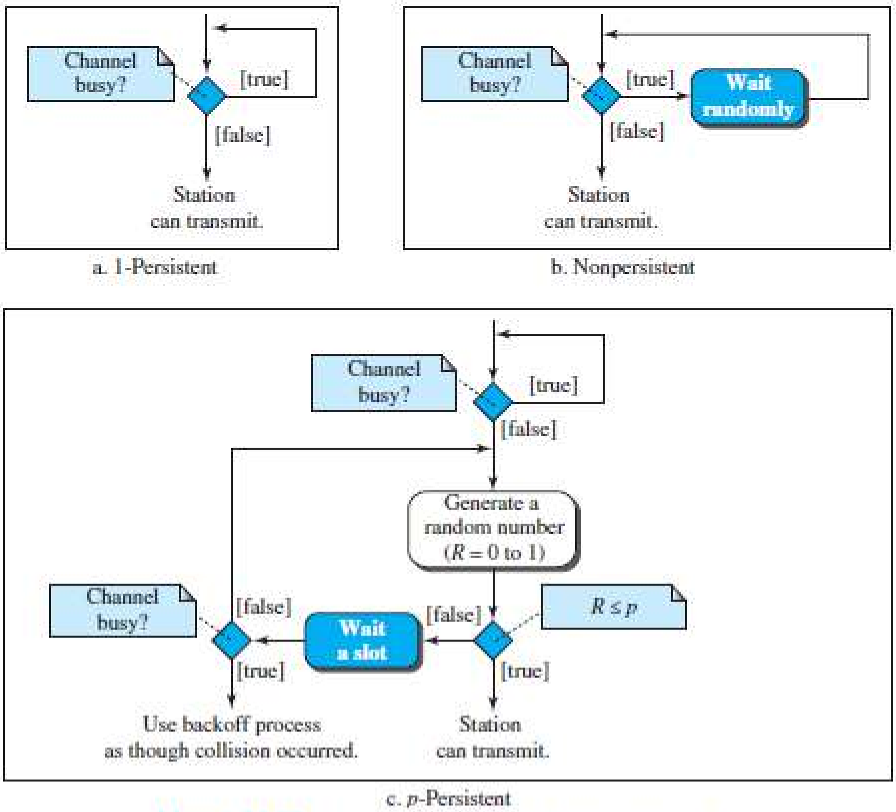


Figure 12.10 *Flow diagram for three persistence methods*

1) 1-Persistent
¤ Before sending a frame, a station senses the line (Figure 12.10a).
i) If the line is idle, the station sends immediately (with probability = 1).
ii) If the line is busy, the station continues sensing the line.

2) Non-persistent
¤ Before sending a frame, a station senses the line (Figure 12.10b).
i) If the line is idle, the station sends immediately.
ii) If the line is busy, the station waits a random amount of time and then senses the line again.

3) P-Persistent
¤ After the station finds the line idle, it follows these steps(Figure 12.10c):
1) With probability p, the station sends the frame.
2) With probability q=1-p, the station waits for the beginning of the next time-slot and checks the line again.
i) If line is idle, it goes to step 1.
ii) If line is busy, it assumes that collision has occurred and uses the back off procedure.

Ans (ii):

CSMA/CD

• Disadvantage of CSMA: CSMA does not specify the procedure after a collision has occurred.
Solution: CSMA/CD enhances the CSMA to handle the collision.
• Here is how it works (Figure 12.12):
1) A station
→ sends the frame &
→ then monitors the medium to see if the transmission was successful or not.
2) If the transmission was unsuccessful (i.e. there is a collision), the frame is sent again.

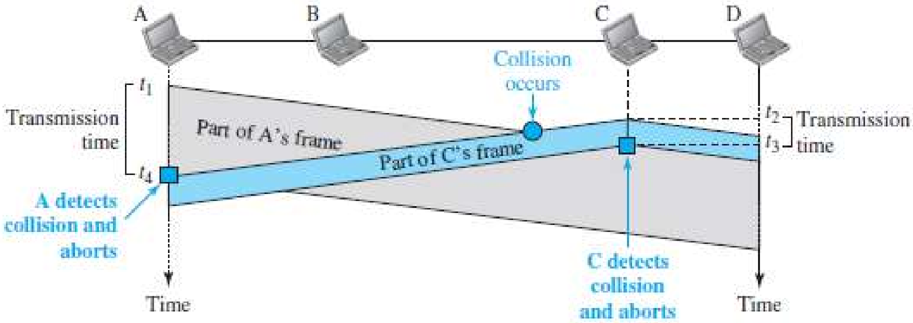


Figure 12.12 *Collision and abortion in CSMA/CD*

• In the Figure 12.12,
➢ At time t_1, station A has executed its procedure and starts sending the bits of its frame.
➢ At time t_2, station C has executed its procedure and starts sending the bits of its frame.
➢ The collision occurs sometime after time t_2.
➢ Station C detects a collision at time t_3 when it receives the first bit of A's frame.
Station C immediately aborts transmission.
➢ Station A detects collision at time t_4 when it receives the first bit of C's frame.
Station A also immediately aborts transmission.
• Station A transmits for the duration $t_4 - t_1$.
Station C transmits for the duration $t_3 - t_2$.
• For the protocol to work:
Length of any frame divided by the bit rate must be more than either of these durations.

Minimum Frame Size

• For CSMA/CD to work, we need to restrict the frame-size.
• Before sending the last bit of the frame, the sender must
→ detect a collision and
→ abort the transmission.
• This is so because the sender
→ does not keep a copy of the frame and
→ does not monitor the line for collision-detection.
• Frame transmission time T_{fr} is given by
$T_{fr}=2T_p$ where T_p=maximum propagation time

Procedure

• CSMA/CD is similar to ALOHA with 2 differences (Figure 12.13):

1) Addition of the persistence process.

¤ We need to sense the channel before sending the frame by using non-persistent, 1-persistent or p-persistent.

2) Frame transmission.

i) In ALOHA, first the entire frame is transmitted and then acknowledgment is waited for.

ii) In CSMA/CD, transmission and collision-detection is a continuous process.

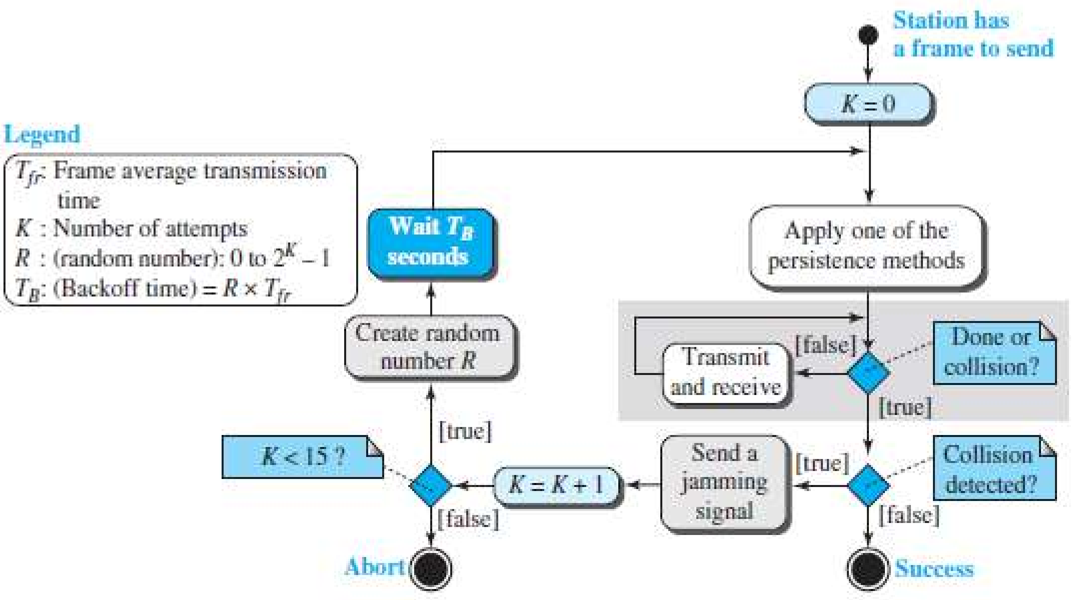


Figure 12.13 *Flow diagram for the CSMA/CD*

Throughput

• The throughput of CSMA/CD is greater than pure or slotted ALOHA.

• The maximum throughput is based on

→ different value of G

→ persistence method used (non-persistent, 1-persistent, or p-persistent) and

→ 'p' value in the p-persistent method.

• For 1-persistent method, the maximum throughput is 50% when G =1.

• For non-persistent method, the maximum throughput is 90% when G is between 3 and 8.

6b. Describe 802.3 MAC frame. (08 Marks)

Ans: For answer, refer Solved Paper June-2013 Q.No.6c.

7a. Explain IEEE 802.11 architecture. (10 Marks)

Ans: For answer, refer Solved Paper June-2013 Q.No.7a.

7b. Bring out the differences b/w repeaters, bridges, routers and gateways. (10 Marks)

Ans: For answer, refer Solved Paper June-2013 Q.No.7b.

8a. Explain wrt IPV4, classful addressing and classless addressing. (10 Marks)

Ans:

Classful Addressing

• IPv4 addressing used the concept of classes.
• This architecture is called classful addressing.
• In classful addressing, the address space is divided into five classes: A, B, C, D, and E.
• Each class occupies some part of the address space.

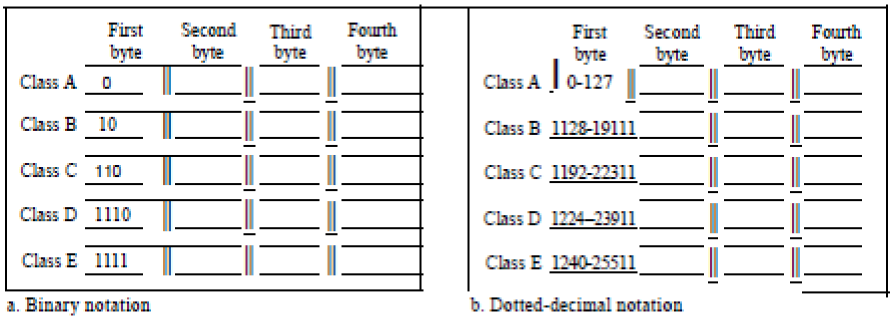


Figure 19.2 *Finding the classes in binary and dotted-decimal notation*

Classes and Blocks

Table 19.1 *Number of blocks and block size in classful IPv4 addressing*

Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

➢ Class A addresses were designed for large organizations with a large number of attached hosts or routers.
➢ Class B addresses were designed for midsize organizations with tens of thousands of attached hosts or routers.
➢ Class C addresses were designed for small organizations with a small number of attached hosts or routers.
➢ In classfnl addressing, a large part of the available addresses were wasted.
➢ In classful addressing, an IP address in class A, B, or C is divided into netid and hostid.
➢ These parts are of varying lengths, depending on the class of the address.

Mask

➢ The mask can help us to find the netid and the hostid.
➢ For example, the mask for a class A address has eight 1s, which means the first 8 bits of any address in class A define the netid; the next 24 bits define the hostid.

Table 19.2 *Default masks for classful addressing*

Class	*Binary*	*Dotted-Decimal*	*CIDR*
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

Classless Addressing

• To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented.

• In this scheme, there are no classes, but the addresses are still granted in blocks

Address Blocks

➢ In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses.

➢ The size of the block (the number of addresses) varies based on the nature and size of the entity.

➢ For example,

A householdmay be given only two addresses;

A large organization may be given thousands of addresses.

Restriction

• To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:

1) The addresses in a block must be contiguous, one after another.
2) The number of addresses in a block must be a power of 2 (I, 2, 4, 8, ...).
3) The first address must be evenly divisible by the number of addresses.

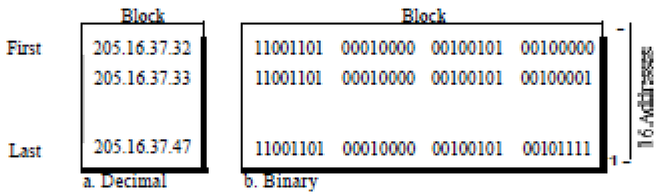


Figure 19.3 *A block of 16 addresses granted to a small organization*

Mask

➢ In classless addressing the mask for a block can take any value from 0 to 32. It is very convenient to give just the value of n preceded by a slash (CIDR notation).

➢ In IPv4 addressing, a block of addresses can be defined as x.y.z.t/n in which x.y.z.t defines one of the addresses and the */n* defines the mask.

8c. Explain in detail IPV6 packet format. (10 Marks)

Ans:

IPV6 PACKET FORMAT

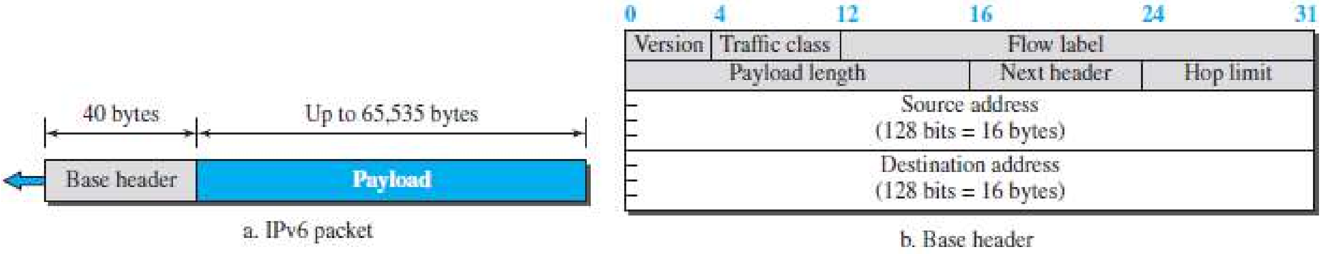


Figure 22.6 *IPv6 datagram*

- IP header contains following fields (Figure 22.6):

1) Version

➢ This specifies version number of protocol. For IPv6, version=6.

2) Traffic Class

➢ This field is used to distinguish different payloads with different delivery requirements. (Traffic class replaces the type-of-service field in IPv4).

3) Flow Label

➢ This field is designed to provide special handling for a particular flow of data.

4) Payload Length

➢ This indicates length of data (excluding header). Maximum length=65535 bytes.

➢ The length of the base-header is fixed (40 bytes); only the length of the payload needs to be defined.

5) Next Header

➢ This identifies type of extension header that follows the basic header.

6) Hop Limit

➢ This specifies number of hops the packet can travel before being dropped by a router. (Hop limit serves the same purpose as the TTL field in IPv4).

7) Source and Destination Addresses

➢ These identify source host and destination host respectively.

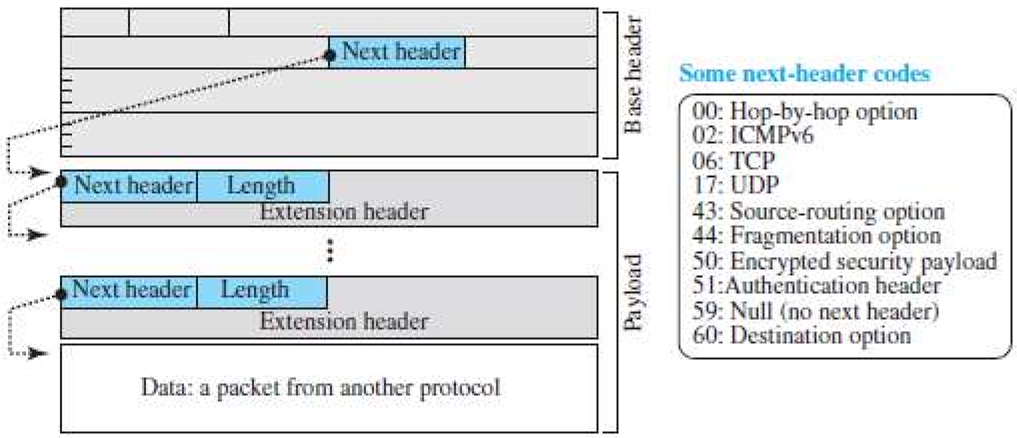


Figure 22.7 *Payload in an IPv6 datagram*

8) Payload

➢ The payload contains zero or more extension headers (options) followed by the data from other protocols (UDP, TCP, and so on).

➢ The payload can have many extension headers as required by the situation.

➢ Each extension header has 2 mandatory fields (Figure 22.7):

1) Next header and
2) Length

- Two mandatory fields are followed by information related to the particular option.

Concept of Flow & Priority in IPv6

• To a router, a flow is a sequence of packets that share the same characteristics such as
  → traveling the same path
  → using the same resources or
  → having the same kind of security
• A router that supports the handling of flow labels has a flow label table.
• The table has an entry for each active flow label.
  Each entry defines the services required by the corresponding flow label.
• When a router receives a packet, the router consults its flow label table.
• Then, the router provides the packet with the services mentioned in the entry.

Fragmentation & Reassembly

• Fragmentation of the packet is done only by the source, but not by the routers.
  The reassembling is done by the destination.
• At routers, the fragmentation is not allowed to speed up the processing in the router.
• Normally, the fragmentation of a packet in a router needs a lot of processing. This is because
  1) The packets need to be fragmented.
  2) All fields related to the fragmentation need to be recalculated.
• The source will
  → check the size of the packet and
  → make the decision to fragment the packet or not.
• If packet-size is greater than the MTU of the network, the router will drop the packet.
• Then, the router sends an error message to inform the source.

USN | | | | | | | | | | 10CS55

Fifth Semester B.E. Degree Examination, June/July 2014
Computer Networks – I

Time: 3 hrs. Max. Marks:100

Note: ***Answer FIVE full questions, selecting atleast TWO questions from each part.***

PART – A

1 a. What is data communication? What are its four fundamental characteristics? With a neat diagram, explain the components of data communication system. **(08 Marks)**
b. Assume that five devices are connected in a mesh topology. How many cables are needed? How many ports are needed for each device? **(02 Marks)**
c. With a neat diagram, explain the functionalities of each layer of OSI reference model. **(10 Marks)**

2 a. Explain the different causes for transmission impairments during signal transmission through media. **(06 Marks)**
b. Define bandwidth. A periodic signal has bandwidth of 20 Hz. The highest frequency is 60 Hz. What is the lowest frequency? Draw the spectrum, if signal contains all frequencies of same amplitude. **(04 Marks)**
c. What is line coding? Describe and represent the information sequence '101000110' using Biphase and Bipolar schemes. **(10 Marks)**

3 a. What is multiplexing? With neat diagram, explain FDM. **(06 Marks)**
b. What is spread spectrum? Explain with an example direct sequence spread spectrum. **(06 Marks)**
c. With a neat diagram, explain how message can be sent from one system to another using datagram networks. **(08 Marks)**

4 a. Define hamming distance. Explain simple parity check code C(5, 4) with $d_{min} = 2$. How many bits can be corrected? **(06 Marks)**
b. Find the code word c(x), using CRC for the information $d(x) = x^3 + 1$ with generator polynomial $t(x) = x^3 + x + 1$. **(08 Marks)**
c. Explain with an example. The computation of internet checksum. List the steps undertaken by the sender and receiver for error detection. **(06 Marks)**

PART – B

5 a. Why bit stuffing and byte stuffing are needed? Explain them, with examples. **(06 Marks)**
b. With neat figures, explain briefly: i) Go–back n ii) selective repeat ARQ protocols. **(10 Marks)**
c. Explain the frame format of PPP protocol. **(04 Marks)**

6 a. Describe CSMA/CD protocol, with neat flow diagram. **(06 Marks)**
b. What is channelization? Explain CODE division multiple access, with an example. **(08 Marks)**
c. Discuss 802.3 MAC frame format and frame length. **(06 Marks)**

7 a. Explain the different types of addressing mechanisms in IEEE 802.11. **(06 Marks)**
b. With neat diagram, explain layers of Bluetooth. **(06 Marks)**
c. What is a bridge? Explain with an example the bridge learning and forwarding process of transparent bridge. **(08 Marks)**

8 a. Explain the following fields in IPV4 packet header :
i) Identification ii) flags iii) fragmentation offset. **(06 Marks)**
b. What is NAT? How can NAT help in address depletion with a neat diagram? **(06 Marks)**
c. What is the need to change from IPV4 to IPV6? Write IPV6 basic header and describe its fields. **(08 Marks)**

* * * * *

1a. What is data communication? What are its four fundamental characteristics? With a neat diagram, explain the components of data communication system. (08 Marks)
Ans: For answer, refer Solved Paper Dec-2013 Q.No.1a.

1b. Assume that five devices are connected in mesh topology. How many cables are needed? How many ports are needed for each device? (02 Marks)
Ans:

Solution:
- For 'n' nodes, there are n(n-1)/2 duplex-mode links.
  Here n=5, therefore number of cables needed = 5(5-1)/2 = 10
- Every device must have (n–1) I/O ports to be connected to the other (n-1) devices.
  Here n=5, number of ports needed for each device = 5-1 = 4

1c. With a diagram, explain the functionalies of each layer of OSI model (10 Marks)
Ans: For answer, refer Solved Paper June-2013 Q.No.1a.

2a. Explain the different causes for transmission impairments during signal transmission through media. (06 Marks)
Ans: For answer, refer Solved Paper Dec-2013 Q.No.2a.

2b. Define bandwidth: A periodic signal has bandwidth 20 Hz.The highest frequency is 60 Hz. What is the lowest frequency? Draw the spectrum, if signal contains all frequencies of same amplitude. (04 Marks)
Ans:

Bandwidth
- Bandwidth is defined as the range of frequencies that the channel can carry. (Figure 3.13).
- Bandwidth of a signal is expressed in terms of its frequencies.
- Bandwidth is calculated by the difference b/w the max. frequency and the min. frequency.

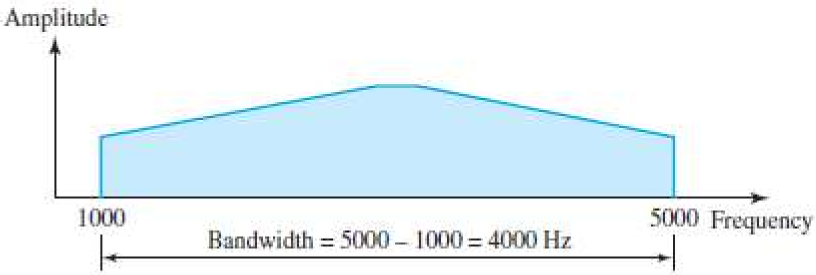


Figure 3.13 *The bandwidth of signals*

Solution

Let f_h be the highest frequency, f_l the lowest frequency, and B the bandwidth. Then

$$B = f_h - f_l \longrightarrow 20 = 60 - f_l \longrightarrow f_l = 60 - 20 = 40 \text{ Hz}$$

The spectrum contains all integer frequencies. We show this by a series of spikes (see Figure 3.15).

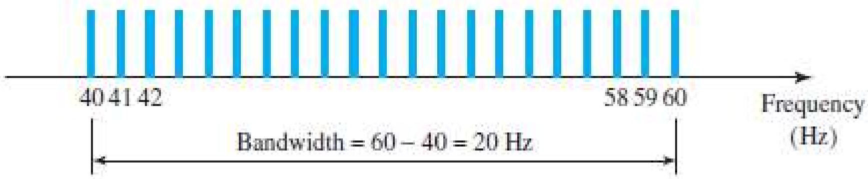


Figure 3.15

2c. What is line coding? Describe and represent the information sequence '101000110' using Biphase and Bipolar schemes. (10 Marks)

Ans:

LINE CODING

• Line-coding is the process of converting digital-data to digital-signals (Figure 4.1).
• The data are stored in computer memory as sequences of bits (0s or 1s).
• Line-coding converts a sequence of bits to a digital-signal.

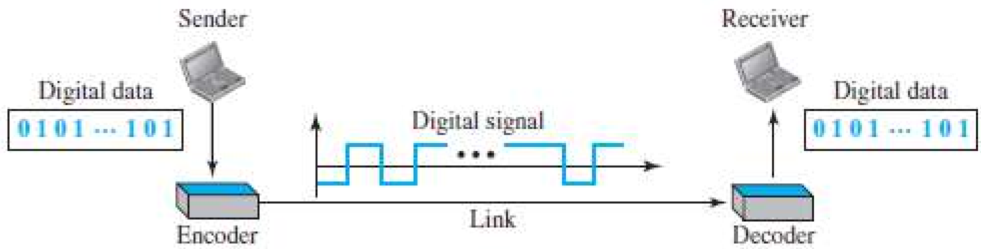
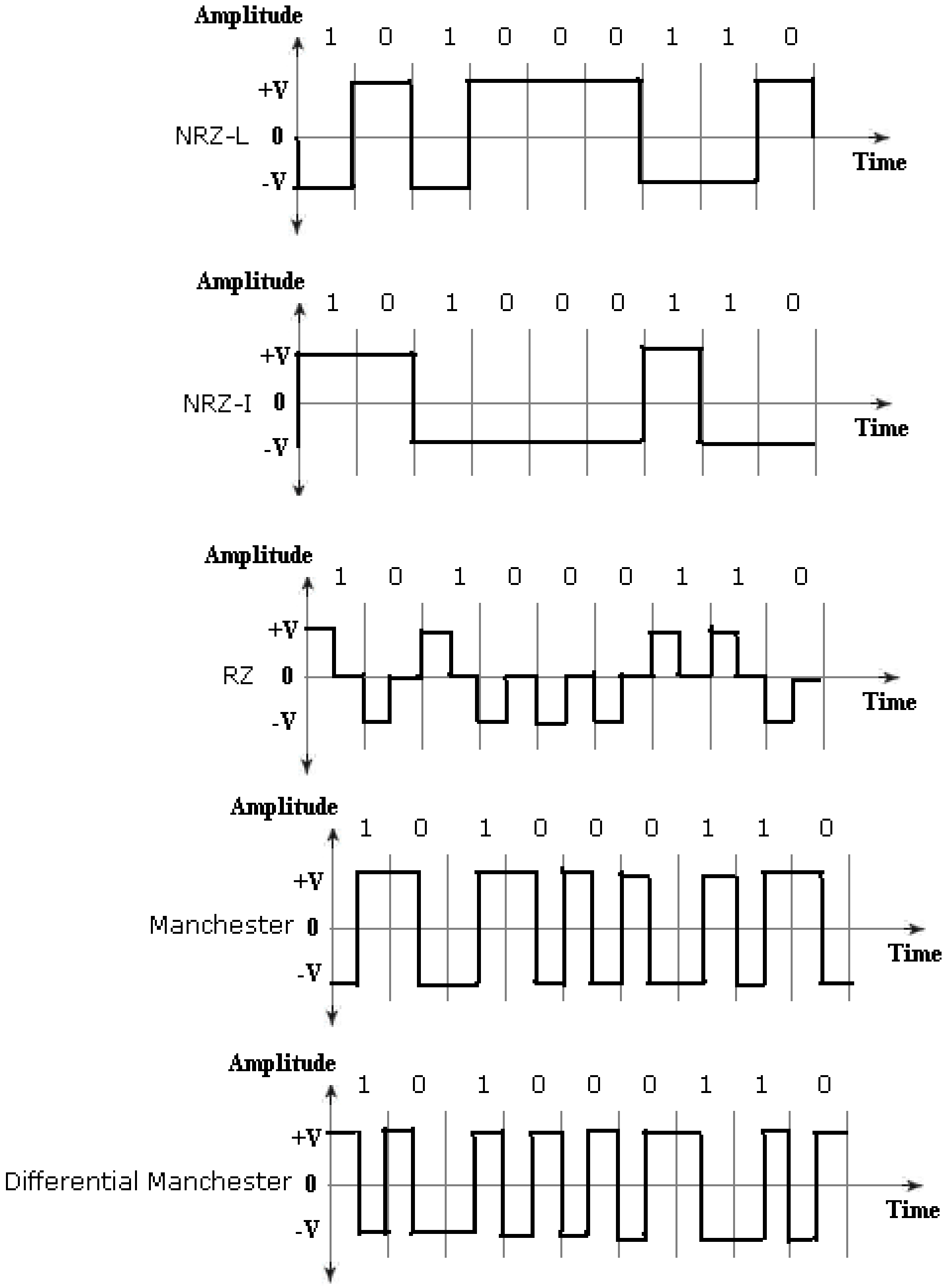


Figure 4.1 *Line coding and decoding*

Solution:



3a. What is multiplexing? With neat diagram, explain FDM. (06 Marks)

Ans:

MULTIPLEXING

• Multiplexing allows simultaneous transmission of multiple signals across a single data-link.

Figure 6.3 Frequency-division multiplexing

Frequency Division Multiplexing (FDM)

• FDM is an analog multiplexing technique that combines analog signals.
• FDM can be used when the bandwidth of a link is greater than the combined bandwidths of the signals to be transmitted.

1) Multiplexing Process

• Here is how it works (Figure 6.4):

1) Each sending-device generates modulated-signals with different carrier-frequencies (f1, f2, & f3).
2) Then, these modulated-signals are combined into a single multiplexed-signal.
3) Finally, the multiplexed-signal is transported by the link.

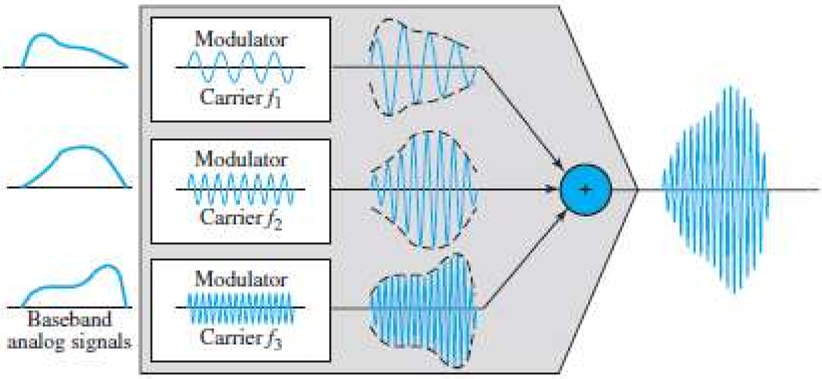


Figure 6.4 FDM process

• Carrier-frequencies are separated by sufficient bandwidth to accommodate modulated-signal.
• Channels can be separated by strips of unused bandwidth called guard bands.
• Guard bands prevent signals from overlapping.
• In addition, carrier-frequencies must not interfere with the original data frequencies.
• Although FDM is considered as analog multiplexing technique,sources can produce digital-signal
• Digital-signal can be sampled, changed to analog-signal, and then multiplexed by using FDM.

2) Demultiplexing Process

• Here is how it works (Figure 6.5):

1) The demultiplexer uses filters to divide the multiplexed-signal into individual-signals.
2) Then, the individual signals are passed to a demodulator.
3) Finally, the demodulator
   → separates the individual signals from the carrier signals and
   → passes the individual signals to the output-lines.

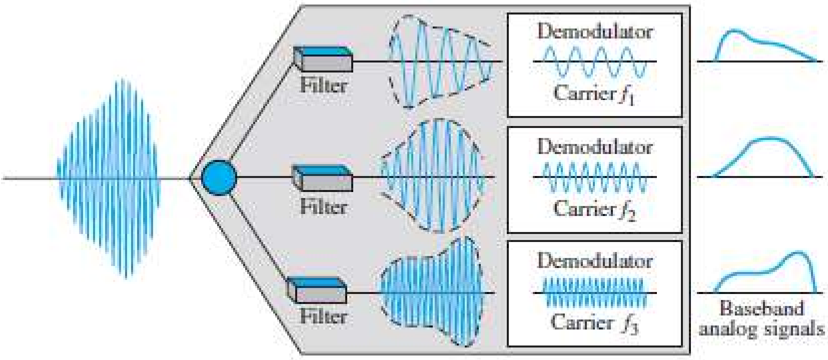


Figure 6.5 FDM demultiplexing example

3b. What is spread spectrum? Explain with an example DSSS. (06 Marks)

Ans:

SPREAD SPECTRUM

- Spread-spectrum is used in wireless applications. (Figure 6.27).
- Spread-spectrum is used to provide secure communication by spreading the original spectrum needed for each station.

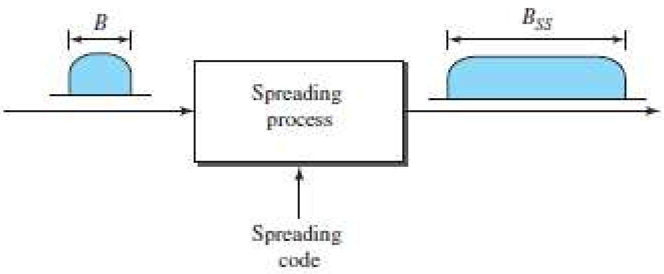


Figure 6.27 *Spread spectrum*

Where B = required bandwidth
B_{ss}= expanded bandwidth

- Two types of spread-spectrum:
  1) Frequency hopping spread-spectrum (FHSS) and
  2) Direct sequence spread-spectrum (DSSS).

Direct Sequence Spread-Spectrum (DSSS)

- This technique expands the bandwidth of the original signal.
- Each data-bit is replaced with 'n' bits using a spreading-code.
- Each bit is assigned a code of 'n' bits called chips.
- The chip-rate is 'n' times that of the data-bit (Figure 6.32).

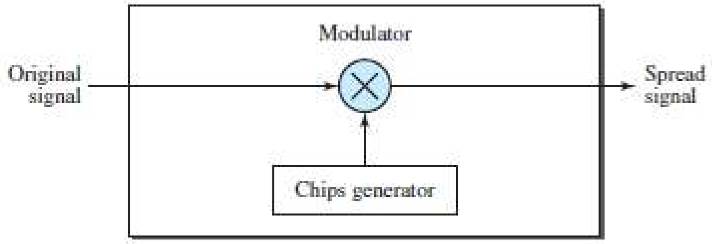


Figure 6.32 *DSSS*

- For example (Figure 6.33):
  - Consider the Barker sequence used in a wireless LAN. Here n =11.
  - Assume: The original signal and the chips in the chip-generator use polar NRZ encoding.
  - The spreading-code is 11 chips having the pattern 10110111000.
  - If the original signal-rate is N, the rate of the spread signal is 1/N.
  - This means that the required bandwidth for the spread signal is 11 times larger than the bandwidth of the original signal.

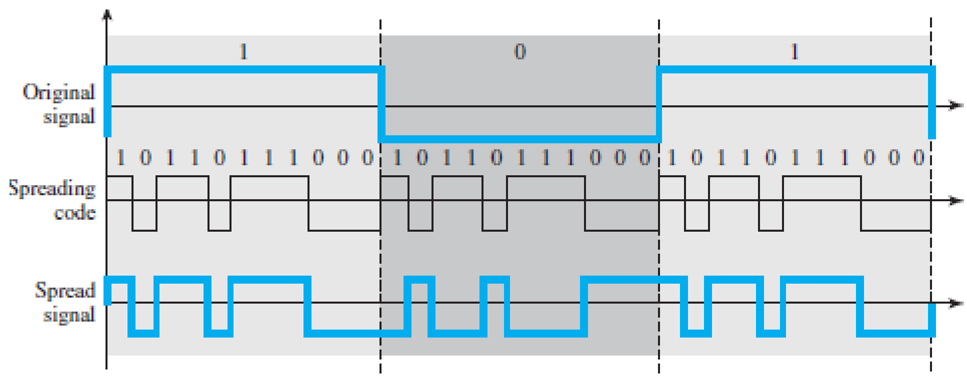


Figure 6.33 *DSSS example*

- The spread signal can provide privacy if the attacker does not know the code.
- It can also provide immunity against interference if each station uses a different code.

3c. With a neat diagram, explain how message can be sent from one system to another using datagram networks. (08 Marks)

Ans:

Datagram Networks

- This is analogous to postal system.
- The message is divided into packets of fixed or variable size (Figure 8.7).
- Each packet is routed independently through the network.
- Each packet has a header that contains source and destination addresses.
- Each switch examines the header to determine the next hop in the path to the destination.
- If the transmission line is busy
  then the packet is placed in the queue until the line becomes free.
- Advantage:
  1) High utilization of transmission-line can be achieved by sharing among multiple packets.
  2) There is no resource reservation; resources are allocated on-demand.
- Disadvantages:
  1) Packets may arrive out-of-order, and re-sequencing may be required at the destination
  2) Loss of packets may occur when a switch has insufficient buffer
- It is the responsibility of an upper-layer protocol to
  → reorder the datagrams or
  → ask for lost datagrams.
- The datagram-networks are referred to as connectionless networks. This is because
  1) The switch does not keep information about the connection state.
  2) There are no setup or teardown phases.
  3) Each packet is treated the same by a switch regardless of its source or destination.

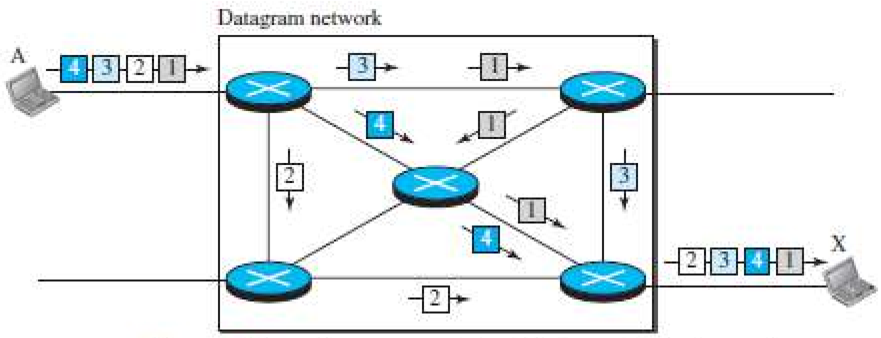


Figure 8.7 *A datagram network with four switches (routers)*

Routing Table

- ➢ Each switch has a routing-table which is based on the destination-address.
- ➢ The routing-tables are dynamic & updated periodically. (Figure 8.8).
- ➢ The destination-addresses and the corresponding forwarding output-ports are recorded in the tables.

Destination address	Output port
1232	1
4150	2
⋮	⋮
9130	3

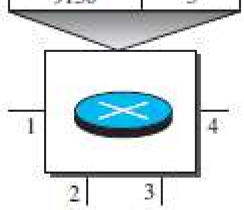


Figure 8.8 *Routing table in a datagram network*

Efficiency

¤ Datagram-networks are more efficient when compared to circuit-switched-network. This is because

1) Resources are allocated only when there are packets to be transferred.
2) If there is a delay, the resources can be re-allocated.

Delay

¤ Datagram-networks may have greater delay when compared to circuit-switched-network. This is because each packet may experience a wait at a switch before it is forwarded.

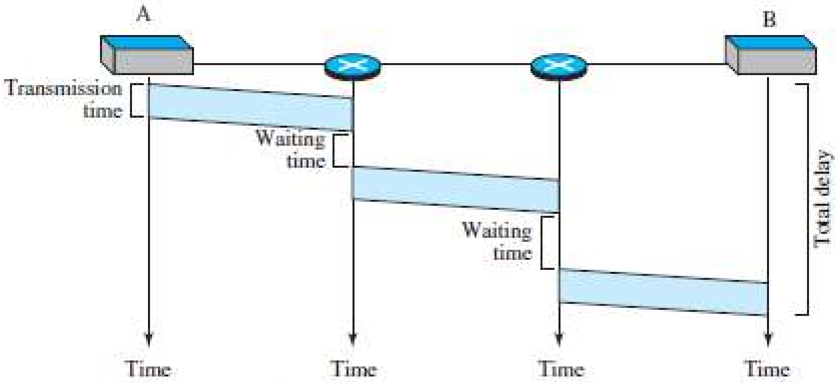


Figure 8.9 *Delay in a datagram network*

¤ In Figure 8.9, there are three transmission times (3T), three propagation delays, and two waiting times (W1+ W2).

$$\text{Total delay} = 3T + 3\tau + w_1 + w_2$$

4a. Define hamming distance. Explain simple parity check code C(5, 4) with d_{min} = 2. How many bits can be corrected. (06 Marks)

Ans: For answer, refer Solved Paper June-2013 Q.No.4a.

4b. Find code word c(x), using CRC for the information d(x) = x^3+1 with generator polynomial t(x) = x^3+x+ 1. (08 Marks)

Ans: For answer, refer Solved Paper June-2013 Q.No.4b.

4c. Explain with an example, the computation of Internet checksum. List the steps undertaken by the sender and receiver for error detection. (06 Marks)

Ans: For answer, refer Solved Paper June-2013 Q.No.4c.

5a. Why bit stuffing and byte stuffing are needed? Explain with examples. (06 Marks)

Ans: For answer, refer Solved Paper June-2013 Q.No.5b.

5b. With neat figures, explain briefly:
i) Go-back N
ii) Selective repeat ARQ protocols. (10 Marks)

Ans (i): For answer, refer Solved Paper Dec-2013 Q.No.5a.(ii).

Ans (ii):

Selective Repeat ARQ Protocol

- In a noisy link, a frame has a higher probability of damage, which means the resending of multiple frames.
- This resending uses up the bandwidth and slows down the transmission.
- For noisy links, there is another mechanism that does not resend N frames when just one frame is damaged; only the damaged frame is resent.
- This mechanism is called Selective Repeat ARQ.
- It is more efficient for noisy links, but the processing at the receiver is more complex.
- The Selective Repeat Protocol also uses two windows: 1) a send window and 2) a receive window. (Figure 11.18).
- The size of the send window is much smaller; it is 2^{m-1}.
- The smaller window size means less efficiency in filling the pipe, but the fact that there are fewer duplicate frames can compensate for this.

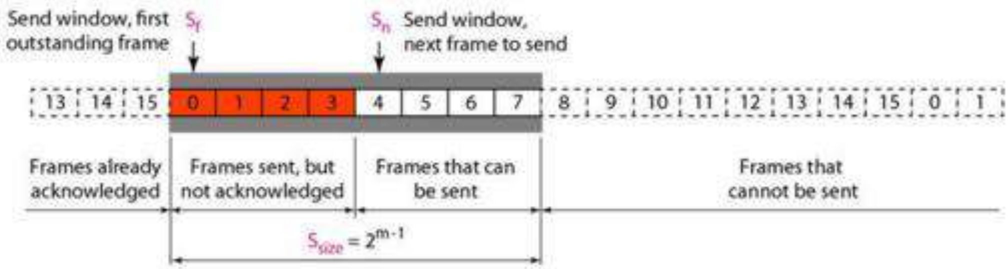


Figure 11.18 *Send window for Selective Repeat ARQ*

- 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. (Figure 11.19).
- 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.
- We need, however, to mention that the receiver never delivers packets out of order to the network-layer.

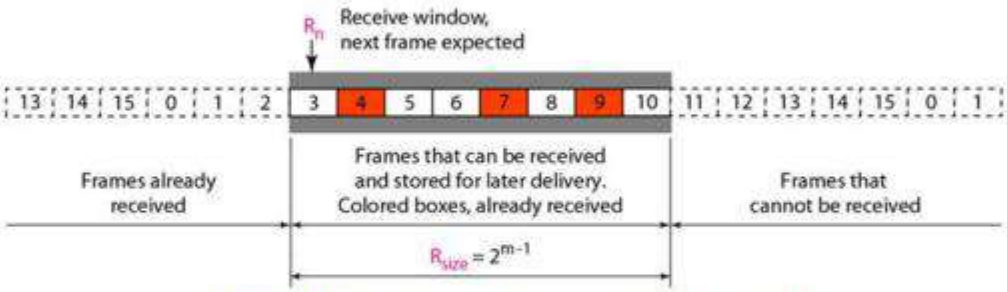


Figure 11.19 *Receive window for Selective Repeat ARQ*

5c. Explain the frame format of PPP protocol. (04 Marks)

Ans: For answer, refer Solved Paper Dec-2013 Q.No.5b.

6a. Describe CSMA/CD protocol, with neat flow diagram. (06 Marks)

Ans: For answer, refer Solved Paper Dec-2013 Q.No.6a.(ii)

6b. What is channelization? Explain CDMA, with an example. (08 Marks)

Ans: For answer, refer Solved Paper June-2013 Q.No.6a.

6c. Discuss i) Frame Format and ii) Frame Length of 802.3 MAC (06 Marks)

Ans (i): **For answer, refer Solved Paper June-2013 Q.No.6c.**

Ans (ii):

Frame Length

• Ethernet has imposed restrictions on both minimum & maximum lengths of a frame (Fig 13.5).

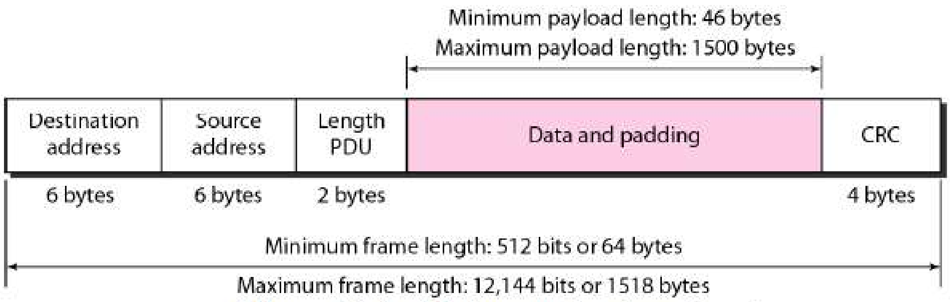


Figure 13.5 *Minimum and maximum lengths*

• The minimum length restriction is required for the correct operation of CSMA/CD.
• Minimum length of frame = 64 bytes.
  1) Minimum data size = 46 bytes.
  2) Header size + Trailer size = 14 + 4 = 18 bytes.
• The minimum length of data from the upper layer = 46 bytes.
• If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.
• Maximum length of frame =1518 bytes.
  1) Maximum data size = 1500 bytes.
  2) Header size + trailer size = 14 + 4 = 18 bytes.
• The maximum length restriction has 2 reasons:
  1) Memory was very expensive when Ethernet was designed.
     A maximum length restriction helped to reduce the size of the buffer.
  2) This restriction prevents one station from
     → monopolizing the shared medium
     → blocking other stations that have data to send.

7a. Explain the different types of addressing mechanisms in IEEE 802.11. (06 Marks)

Ans:

IEEE 802.11 Addressing

• In an Ethernet-network, each station has its own NIC (6-byte → 48 bits).
• The NIC provides the station with a 6-byte physical-address (or Ethernet-address).
• For example, the following shows an Ethernet MAC address:

06:01 :02:01:2C:4B

6 bytes = 12 hex digits = 48 bits

(NIC → network interface card)

Unicast, Multicast, and Broadcast Addresses

• A source-address is always a unicast address i.e. the frame comes from only one station.

Figure 13.4 *Unicast and multicast addresses*

• However, the destination-address can be 1) Unicast 2) Multicast or 3) Broadcast.
• As shown in Figure 13.4,

If LSB of first byte in a destination-address is 0,

Then, the address is unicast;

Otherwise, the address is multicast.

1) A unicast destination-address defines only one recipient.

¤ The relationship between the sender and the receiver is one-to-one.

2) A multicast destination-address defines a group of addresses.

¤ The relationship between the sender and the receivers is one-to-many.

3) The broadcast address is a special case of the multicast address.

¤ The recipients are all the stations on the LAN.

¤ A broadcast destination-address is 48 1s (6-byte → 48 bits).

• Standard Ethernet uses a coaxial cable (bus topology) or a set of twisted-pair cables with a hub (star topology) (Figure 13.5).

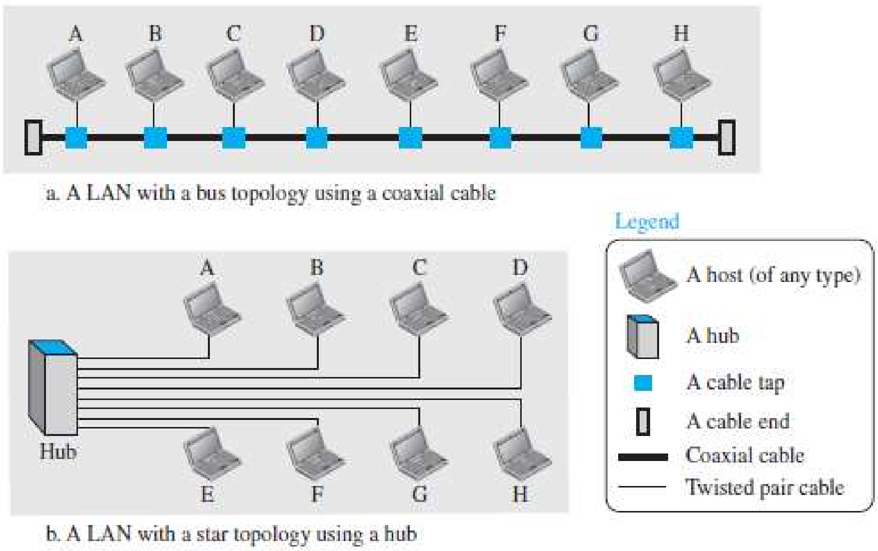


Figure 13.5 *Implementation of standard Ethernet*

7b. With neat diagram, explain layers of Bluetooth. (06 Marks)
Ans:
Bluetooth Layers
• Bluetooth uses several layers that do not exactly match those of the Internet model (Fig 15.19)

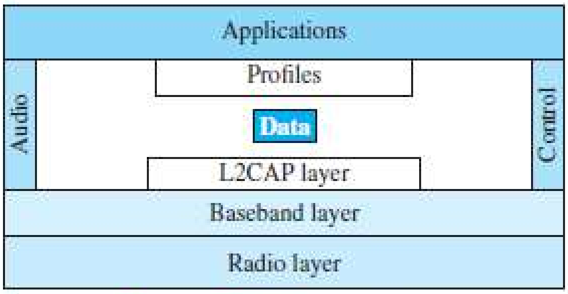


Figure 15.19 *Bluetooth layers*

1) Radio Layer
• The radio layer is roughly equivalent to the physical layer of the Internet model.
• Bluetooth devices are low-power and have a range of 10 m.

1) Band
➢ Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.

2) FHSS
➢ Bluetooth uses the FHSS in the physical layer to avoid interference from other devices or other networks.

3) Modulation
➢ To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering).
➢ GFSK has a carrier frequency.

2) Baseband Layer
• The baseband layer is roughly equivalent to the MAC sublayer in LANs.
• The access method is TDMA.
• The primary and secondary communicate with each other using time slots.
• The communication is only between the primary and a secondary; secondaries cannot communicate directly with one another.

TDMA
➢ Bluetooth uses a form of TDMA that is called TDD-TDMA (timedivision duplex TDMA).
➢ TDD-TDMA is a kind of half-duplex communication in which the secondary and receiver send and receive data, but not at the same time (halfduplex);

Links
➢ Two types of links can be created between a primary and a secondary:

1) SCA link (Synchronous Connection-oriented Link)
¤ This link is used when avoiding latency is more important than data-integrity.
(Latency → delay in data delivery Integrity → error-free delivery)

2) ACL link (Asynchronous Connectionless Link)
¤ This link is used when data-integrity is more important than avoiding latency.

3) L2CAP
• The L2CAP is roughly equivalent to the LLC sublayer in LANs.
• It is used for data exchange on an ACL link. (L2CAP → Logical Link Control and Adaptation Protocol)
• The L2CAP has specific duties: 1) Multiplexing
2) Segmentation and reassembly
3) QoS (quality of service) and
4) Group management.

7c. What is a bridge? Explain with an example the bridge learning and forwarding process of transparent bridge. (08 Marks)

Ans:

Bridges

• A bridge operates in both the physical and the data link layer (Figure 15.5).
• As a physical layer device, it regenerates the signal it receives.
• As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame.
• A bridge has filtering capability.
• It can check the destination address of a frame and decide if the frame should be forwarded or dropped.
• If the frame is to be forwarded, the decision must specify the port.
• A bridge has a table that maps addresses to ports.
• A bridge has a table used in filtering decisions.
• A bridge does not change the physical (MAC) addresses in a frame

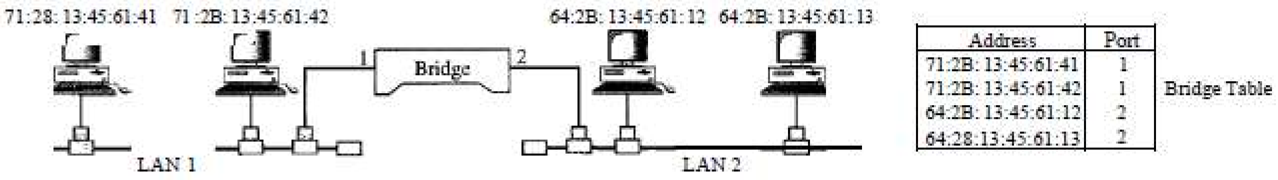


Figure 15.5 *A bridge connecting two LANs*

Transparent Bridges

• A transparent bridge is a bridge in which the stations are completely unaware of the bridge's existence.
• If a bridge is added or deleted from the system, reconfiguration of the stations is unnecessary.
• According to the IEEE 802.1 d specification, a system equipped with transparent bridges must meet three criteria:

1) Frames must be forwarded from one station to another.
2) The forwarding table is automatically made by learning frame movements in the network.
3) Loops in the system must be prevented.

Forwarding

• A transparent bridge must correctly forward the frames. (Figure 15.6).

Learning

• The earliest bridges had forwarding tables that were static.
• The systems administrator would manually enter each table entry during bridge setup.
• If a station was added or deleted, the table had to be modified manually

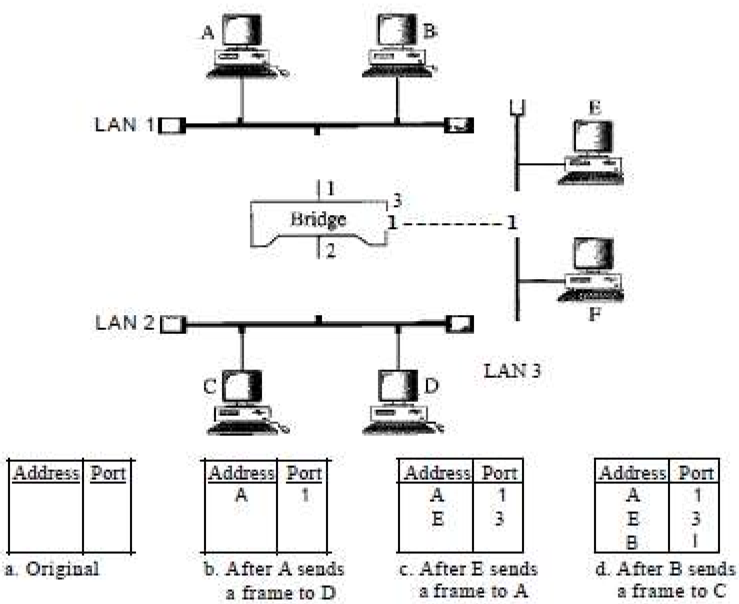


Figure 15.6 *A learning bridge and the process of learning*

8a. Explain the following fields in IPV4 packet header: (06 Marks)
i) Identification ii) flags iii) fragmentation offset.

Ans:

Fragmentation

Maximum Transfer Unit (MTU)

• Each network imposes a restriction on maximum size of packet that can be carried. This is called the MTU (maximum transmission unit).

• For example:
For Ethernet, MTU = 1500 bytes

• When IP wants send a packet that is larger than MTU of physical-network, IP breaks packet into smaller fragments. This is called fragmentation (Figure 19.5).

• Source host or router is responsible for fragmentation.
Destination host is responsible for reassembly.

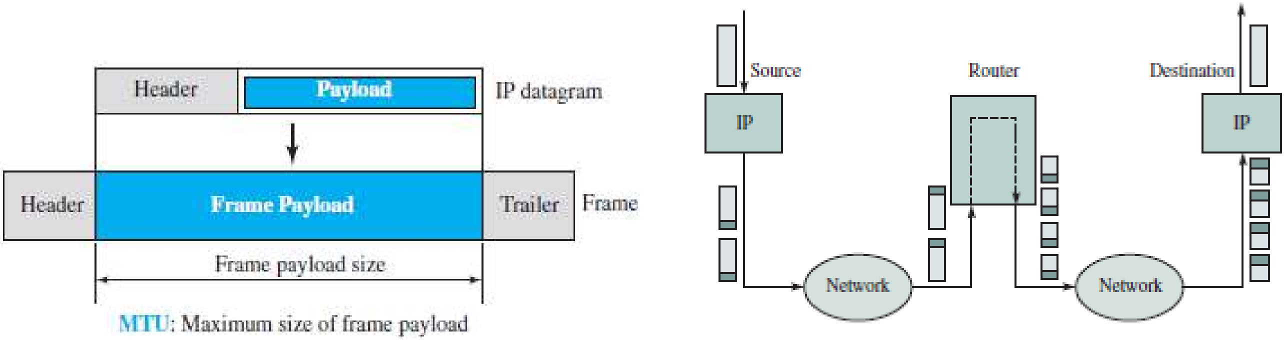


Figure 19.5: Packet Fragmentation

Fields Related to Fragmentation & Reassembly

• Three fields in the IP header are used to manage fragmentation and reassembly:
1) Identification 2) Flags 3) Fragmentation offset.

1) Identification

• This field is used to identify to which datagram a particular fragment belongs to (so that fragments for different packets do not get mixed up).

• To guarantee uniqueness, the IP protocol uses an up-counter to label the datagrams.

• When the IP protocol sends a datagram, IP protocol
→ copies the current value of the counter to the identification field and
→ increments the up-counter by 1.

• When a datagram is fragmented, the value in the identification field is copied into all fragments.

• The identification number helps the destination in reassembling the datagram.

2) Flags

• This field has 3 bits.
1) The leftmost bit is not used.
2) DF bit (Don't Fragment):
i) If DF=1, the router should not fragment the datagram. Then, the router
→ discards the datagram and
→ sends an error-message to the source host.
ii) If DF=0, the router can fragment the datagram if necessary.
3) MF bit (More Fragment):
i) If MF=1, there are some more fragments to come.
ii) If MF=0, this is last fragment.

3) Fragmentation Offset

• This field identifies location of a fragment in a packet.

• This field is the offset of the data in the original datagram.

8b. What is NAT? How can NAT help in address depletion with a diagram? (06 Marks)

Ans:

NAT (Network address translation)

• NAT enables a user to have a large set of addresses internally and one address, or a small set of addresses, externally. (Figure 19.10).
• The traffic inside can use the large set; the traffic outside, the small set.
• To separate the addresses used inside the home/business and the ones used for the Internet, the Internet authorities have reserved 3 sets of addresses as private addresses (Table 19.3).

Table 19.3 *Addresses for private networks*

Range			Total
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

• Any organization can use an address out of this set without permission from the Internet authorities.
• Everyone knows that these reserved addresses are for private networks.
• They are unique inside the organization, but they are not unique globally.
• No router will forward a packet that has one of these addresses as the destination address.
• The site must have only one single connection to the global Internet through a router that runs the NAT software.

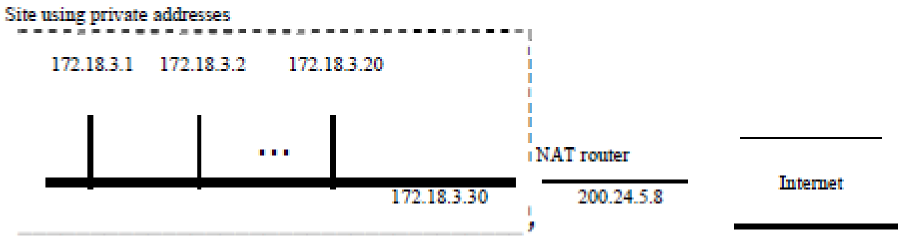


Figure 19.10 *A NAT implementation*

Address Translation

• All the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address. (Figure 19.11).
• All incoming packets also pass through the NAT router, which replaces the destination address in the packet (the NAT router global address) with the appropriate private address (Fig19.11)

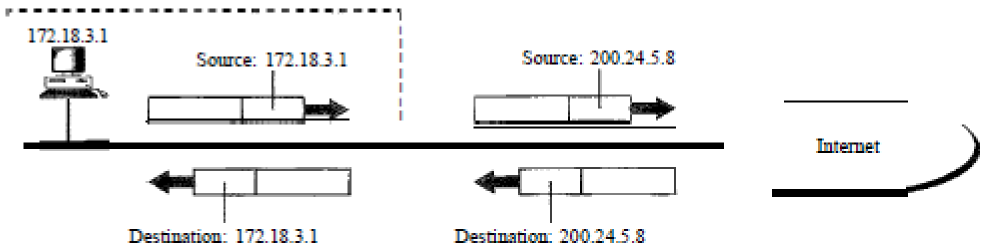


Figure 19.11 *Addresses in a NAT*

8c. i) What is the need to change from IPV4 to 1PV6? ii) Write IPV6 header and describe its fields. (08 Marks)

Ans (i):

Need to Change from IPv4 to IPv6

1) Header Format

- IPv6 uses a new header format.
- Options are
  - → separated from the base-header and
  - → inserted between the base-header and the data.
- This speeds up the routing process (because most of the options do not need to be checked by routers).

2) New Options

- IPv6 has new options to allow for additional functionalities.

3) Extension

- IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

4) Resource Allocation

- In IPv6,
  - → type-of-service (TOS) field has been removed
  - → two new fields: 1) traffic class and 2) flow label, are added to enable the source to request special handling of the packet.
- This mechanism can be used to support real-time audio and video.

5) Security

- The encryption option provides confidentiality of the packet.
- The authentication option provides integrity of the packet.

Ans (ii): **For answer, refer Solved Paper Dec-2013 Q.No.8b.**

USN | | | | | | | | | | | **10CS55**

Fifth Semester B.E. Degree Examination, Dec.2014/Jan.2015
Computer Networks – I

Time: 3 hrs. Max. Marks: 100

Note: ***Answer any FIVE full questions, selecting atleast TWO questions from each part.***

PART – A

1 a. What are the components of data communication system? Explain in brief. **(05 Marks)**
b. With a neat diagram, explain the interaction between layers in the OSI model. **(10 Marks)**
c. What is the difference between a physical and logical address? Explain with example. **(05 Marks)**

2 a. Distinguish between low pass channel and a band pass channel. **(06 Marks)**
b. A network with bandwidth of 10Mbps can pass only an average of 18,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network? **(04 Marks)**
c. Compare and contrast between PCM and DM. **(06 Marks)**
d. Explain polar biphase Manchester and differential Manchester encoding schemes with example. **(04 Marks)**

3 a. Explain following modulation techniques:
i) Amplitude modulation
ii) Frequency modulation. **(06 Marks)**
b. A multiplexer combines four 100kbps channels using a time slot of 2 bits. Show the output with four arbitrary inputs. What is the frame rate? What is the frame duration? What is the bit rate? What is the bit duration? **(04 Marks)**
c. With relevant diagrams, explain the data transfer phase in a virtual circuit network. **(10 Marks)**

4 a. Explain CRC error detection method with an example. **(06 Marks)**
b. Explain the structure of encoder and decoder for a Hamming code. **(04 Marks)**
c. What is internet checksum? If a sender needs to send four data items 0×3456, $0 \times ABCC$, $0 \times 02BC$ and $0 \times EEEE$, answer the following:
i) Find the checksum at sender site.
ii) Find the checksum at receiver's site if there is no error. **(10 Marks)**

PART – B

5 a. Explain GO-BACK-N ARQ and selective-repeat-ARQ. List the differences between them. **(10 Marks)**
b. Explain the different frame types in HDLC. **(06 Marks)**
c. Write a short note on piggybacking. **(04 Marks)**

6 a. With a flow diagram, explain the working of CSMA/CD. **(10 Marks)**
b. Explain the following channelization techniques: i) TDMA ii) CDMA. **(10 Marks)**

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.

7 a. What do you mean by hidden and exposed station problems in IEEE 802.11 protocol. Explain in detail. (06 Marks)
b. With neat diagram, explain the architecture of Piconet and Scatternet Bluetooth networks. (06 Marks)
c. Explain the working of global system for mobile (GSM) in detail. (08 Marks)

8 a. Explain IPV_6 header format with its extension headers. (10 Marks)
b. Write short note for following:
i) Token passing
ii) Gigabit Ethernet
iii) Polling
iv) FHSS. (10 Marks)

* * * * *

1a. What are the components of data communication system? Explain. (05 Marks)
Ans: For answer, refer Solved Paper Dec-2013 Q.No.1a.

1b. With a neat diagram, explain interaction b/w layers in the OSI model. (10 Marks)
Ans:
OSI MODEL
• The OSI model describes an abstract reference-model for network-architecture.
• Purpose of reference model: To provide a framework for the development of protocols.
• OSI consists of 7 separate layers.
• Each layer defines a part of the process of moving information across a network.
Layered Architecture
• The OSI model consists of 7 layers:
1) Physical (layer 1)
2) Data link (layer 2)
3) Network (layer 3)
4) Transport (layer 4)
5) Session (layer 5)
6) Presentation (layer 6) and
7) Application (layer 7).

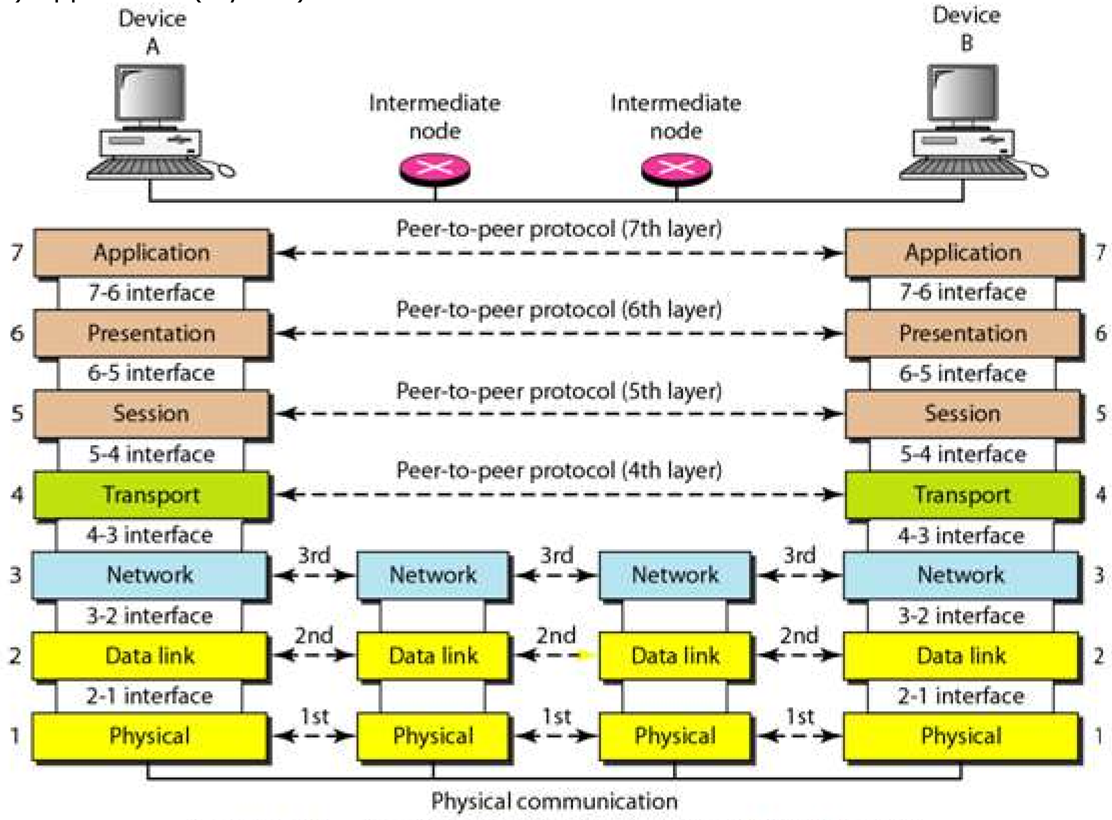


Figure 2.3 *The interaction between layers in the OSI model*

• Figure 2.3 shows the layers involved when a message is sent from device-A to device-B.
• As the message travels from device-A to device-B, the message may pass through many intermediate-nodes.
• Usually, the intermediate-nodes uses only first 3 layers of the OSI model.
• Each layer calls upon the services of the layer just below it.
For example: Layer-3 calls upon the services of Layer-2.
Peer-to-Peer Processes
• The processes on each machine that communicate at a given layer are called peer-to-peer processes.
• At the physical-layer, communication is direct: In figure 2.3, device-A sends a stream of bits to device-B (through intermediate-nodes).
• At the higher layers,
→ firstly, data must move down through the layers on device-A
→ then, data must move over to intermediate-nodes
→ finally, data must move back up through the layers on device-B.

• Here is how data transmission occurs:

1) In the sending-device, each layer
   → adds a header to the message received from the above layer and
   → passes the whole package to the below layer.
2) At Layer-1, the entire package is
   → converted to an electrical signal &
   → transmitted to the receiving-device.
3) At the receiving-device,
   → the message is unwrapped layer by layer
   → each layer receives and removes the data meant for it.
   For example:
   i) Layer-2 removes the data meant for it & passes the remaining data to Layer-3.
   ii) Then, Layer-3 removes data meant for it & passes remaining data to Layer-4.

Interfaces Between Layers

- An interface between layers makes it possible for the passing of the message
  → down through the layers of the sending-device and
  → back up through the layers of the receiving-device.
- Each interface defines the services a layer must provide for the layer above it.
- Well-defined interfaces & layer-functions provide modularity to a network.

1c. What is the difference between a physical and logical address? Explain with example. (05 Marks)

Ans:

Logical address

• At the network-layer, addresses are called IP addresses.
• IP address uniquely defines the connection of a device to the Internet.
• IP address is assigned to each system in the Internet.
• The IP addresses are global, with the whole Internet as the scope.
• Address size = 32 bits.
Eg: 192.12.41.91 in hexadecimal format

Physical Address

• At the data link-layer, addresses are called MAC addresses
• The MAC address defines a specific host or router in a network (LAN or WAN).
• The MAC address is burned into the ROM of the NIC card.
• The MAC address is unique for each system and cannot be changed.
• The MAC addresses are locally defined addresses.
• Address size = 48 bits.
Eg: 12.14.14.19.25.37 in hexadecimal format

2a. Distinguish between low pass channel and a band pass channel. (06 Marks)

Ans:

Transmission of Digital Signals

• Two methods for transmitting a digital signal:

1) Baseband transmission 2) Broadband transmission (using modulation).

1) Baseband Transmission

• Baseband transmission means sending a digital signal over a channel without changing the digital signal to an analog signal (Figure 3.19).

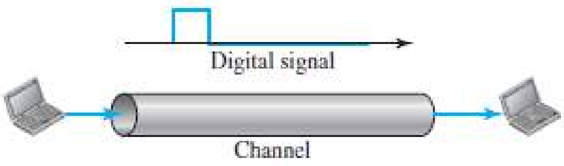


Figure 3.19 *Baseband transmission*

• Baseband transmission requires that we have a low-pass channel.
• Low-pass channel means a channel with a bandwidth that starts from zero.
• For example, we can have a dedicated medium with a bandwidth constituting only one channel.

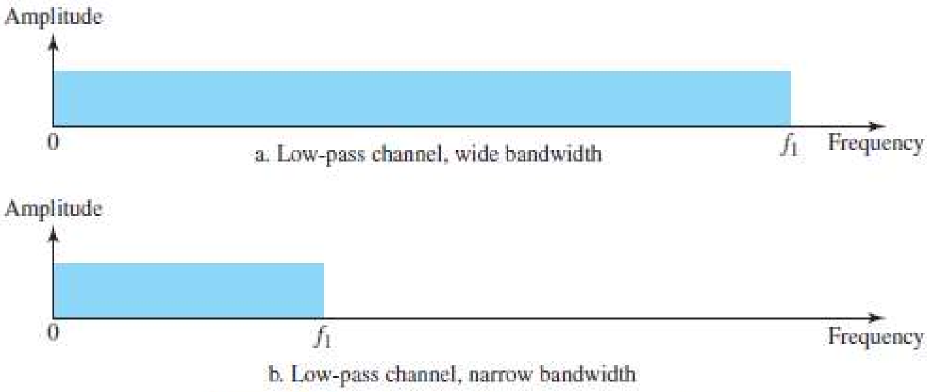


Figure 3.20 *Bandwidths of two low-pass channels*

• Two cases of a baseband communication:

Case 1: Low-pass channel with a wide bandwidth (Figure 3.20a).
Case 2: Low-pass channel with a limited bandwidth (Figure 3.20b).

Low-Pass Channel with Wide Bandwidth

➢ To preserve the shape of a digital signal, we need to send the entire spectrum i.e. the continuous range of frequencies between zero and infinity.

➢ This is possible if we have a dedicated medium with an infinite bandwidth between the sender and receiver.

➢ If we have a medium with a very wide bandwidth, 2 stations can communicate by using digital signals with very good accuracy (Figure 3.21).

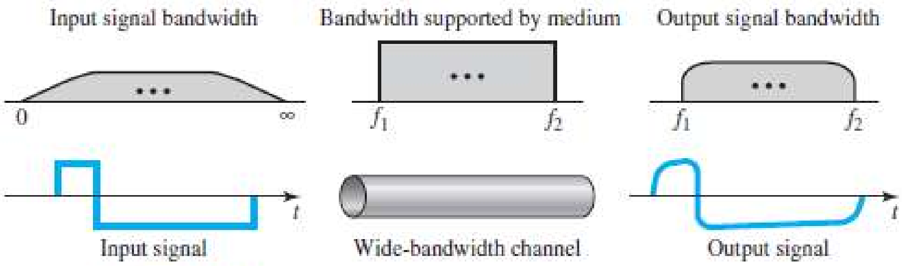


Figure 3.21 *Baseband transmission using a dedicated medium*

2) Broadband Transmission (Using Modulation)

• Broadband transmission or modulation means changing the digital signal to an analog signal for transmission.
• Modulation allows us to use a bandpass channel (Figure 3.24).
• Bandpass channel means a channel with a bandwidth that does not start from zero.
• This type of channel is more available than a low-pass channel.

Figure 3.24 *Bandwidth of a bandpass channel*

• If the available channel is a bandpass channel,
We cannot send the digital signal directly to the channel;
We need to convert digital signal to an analog signal before transmission (Figure 3.25).

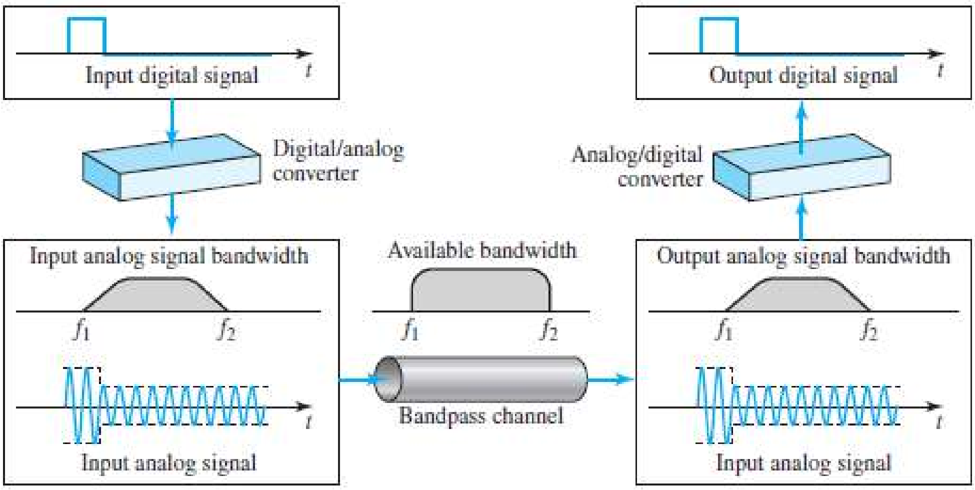


Figure 3.25 *Modulation of a digital signal for transmission on a bandpass channel*

2b. A network with bandwidth of 10Mbps can pass only an average of 18,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network? (04 Marks)

Ans:

Solution

We can calculate the throughput as

$$\text{Throughput} = (12{,}000 \times 10{,}000) / 60 = 2 \text{ Mbps}$$

2c. Compare and contrast between i) PCM and ii) DM. (06 Marks)

Ans(i): For answer, refer Solved Paper June-2013 Q.No.2c.

Ans(ii): For answer, refer Solved Paper Dec-2013 Q.No.2c.

2d. Explain polar biphase Manchester and differential Manchester encoding schemes with example. (04 Marks)

Ans:

1) Manchester Encoding

• This is a combination of NRZ-L & RZ schemes.

• There is always a transition at the middle of the bit. Either

i) from high to low (for 0) or

ii) from low to high (for 1).

• It uses only two voltage levels (Figure 4.8).

• The duration of the bit is divided into 2 halves.

• The voltage

→ remains at one level during the first half &

→ moves to the other level in the second half.

• The transition at the middle of the bit provides synchronization.

2) Differential Manchester

• This is a combination of NRZ-I and RZ schemes.

• There is always a transition at the middle of the bit, but the bit-values are determined at the beginning of the bit.

• If the next bit is 0, there is a transition.

If the next bit is 1, there is none.

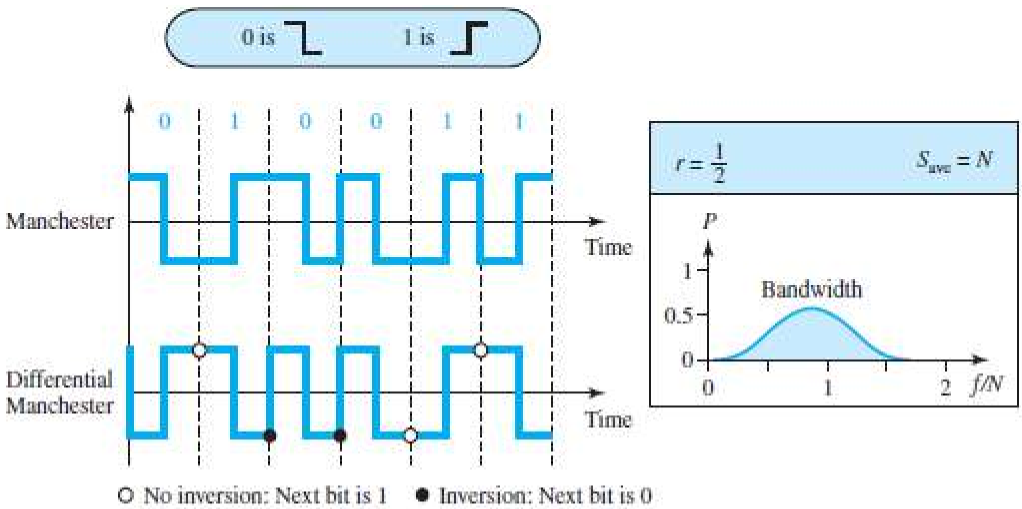


Figure 4.8 *Polar biphase: Manchester and differential Manchester schemes*

3a. A multiplexer combines four 100 kbps channels using a time slot of 2 bits. Show the output with arbitarary inputs. What is the frame rate? What is the frame duration? What is the bit rate? Whart is the bit duration? (04 Marks)

Ans:

Solution

Figure 6.17 shows the output for four arbitrary inputs. The link carries 50,000 frames per second since each frame contains 2 bits per channel. The frame duration is therefore 1/50,000 s or 20 μs. The frame rate is 50,000 frames per second, and each frame carries 8 bits; the bit rate is 50,000 × 8 = 400,000 bits or 400 kbps. The bit duration is 1/400,000 s, or 2.5 μs. Note that the frame duration is 8 times the bit duration because each frame is carrying 8 bits.

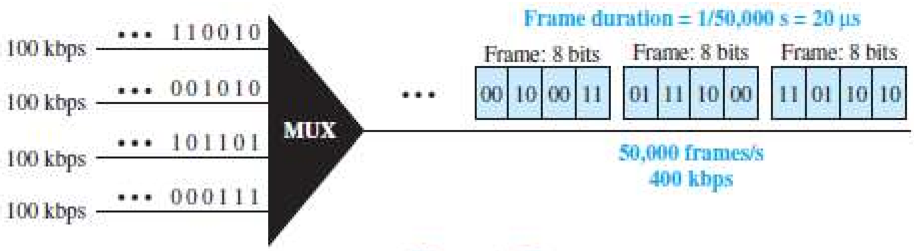


Figure 6.17

3b. Explain following modulation techniques (06 Marks)
i) Amplitude modulation ii) Frequency modulation

Ans(i):

Amplitude Modulation

• In AM transmission, the carrier signal is modulated so that its amplitude varies with the changing amplitudes of the modulating signal (Figure 5.16).

• The frequency and phase of the carrier remain the same; only the amplitude changes to follow variations in the information.

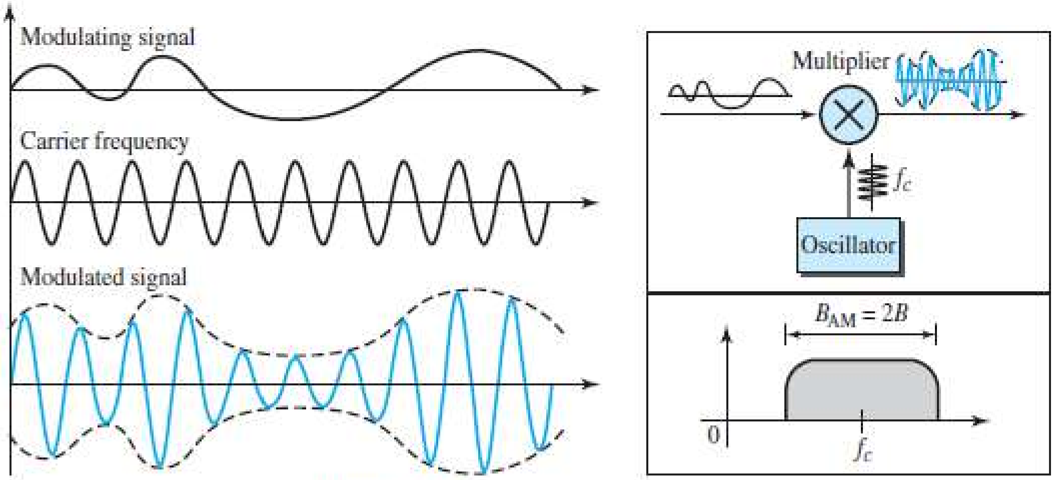


Figure 5.16 *Amplitude modulation*

AM Bandwidth

➢ The modulation creates a bandwidth that is twice the bandwidth of the modulating signal and covers a range centered on the carrier frequency.

➢ However, the signal components above and below the carrier frequency carry exactly the same information.

➢ For this reason, some implementations discard one-half of the signals and cut the bandwidth in half.

Ans(ii):

Frequency Modulation

•In FM transmission, the frequency of the carrier signal is modulated to follow the changing voltage level (amplitude) of the modulating signal (Figure 5.18).

• The peak amplitude and phase of the carrier signal remain constant, but as the amplitude of the information signal changes, the frequency of the carrier changes correspondingly

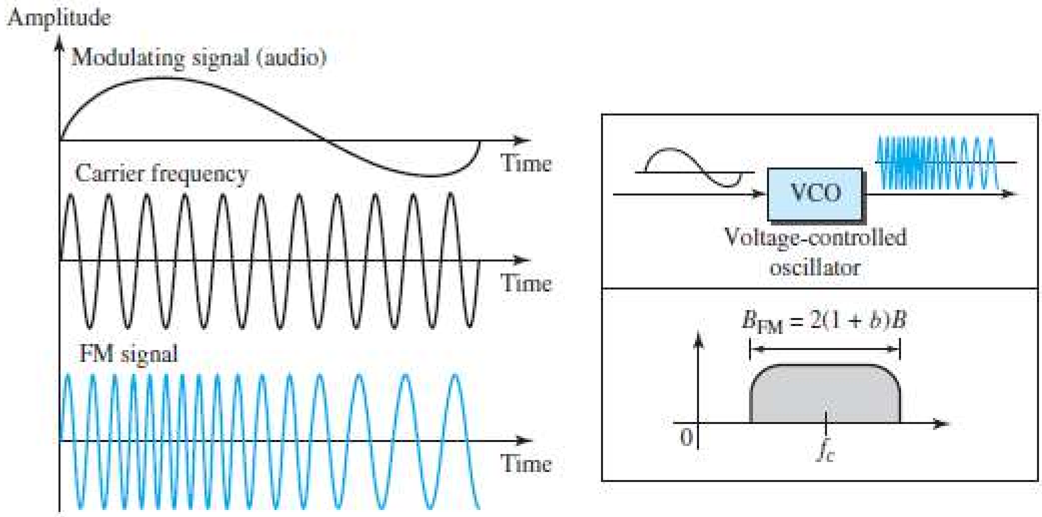


Figure 5.18 *Frequency modulation*

FM Bandwidth

➢ The actual bandwidth is difficult to determine exactly, but it can be shown empirically that it is several times that of the analog signal or $2(1 + \beta)B$ where β is a factor that depends on modulation technique with a common value of 4.

3c. With diagram, explain data transfer phase in virtual circuit network. (10 Marks)

Ans:

Virtual Circuit Network (VCN)

• This is similar to telephone system.
• A virtual-circuit network is a combination of circuit-switched-network and datagram-network.
• The network has switches that allow traffic from sources to destinations.

Three Phases

• A source and destination need to go through 3 phases: setup, data-transfer, and teardown.

1) In setup phase, the source and destination use their global addresses to help switches make table entries for the connection.
2) Data-transfer occurs between these 2 phases.
3) In the teardown phase, the source and destination inform the switches to delete the corresponding entry.

1) Data Transfer Phase

• To transfer a frame from a source to its destination, all switches need to have a table-entry for this virtual-circuit.
• The table has four columns.
• The switch holds 4 pieces of information for each virtual-circuit that is already set up.

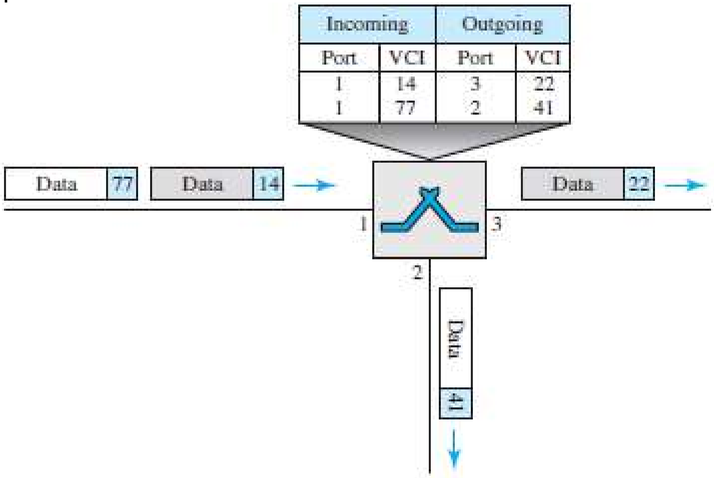


Figure 8.12 *Switch and tables in a virtual-circuit network*

➢ As shown in Figure 8.12, a frame arrives at port 1 with a VCI of 14.
➢ When the frame arrives, the switch looks in its table to find port 1 and a VCI of 14.
➢ When it is found, the switch knows to change the VCI to 22 & send out the frame from port 3.

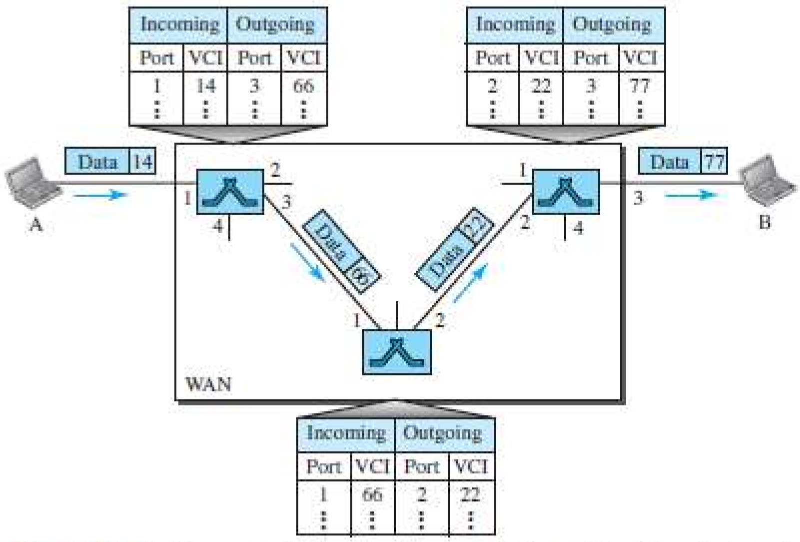


Figure 8.13 *Source-to-destination data transfer in a virtual-circuit network*

➢ As shown in Figure 8.13, each switch changes the VCI and routes the frame.
➢ The data-transfer phase is active until the source sends all its frames to the destination.
➢ The procedure at the switch is the same for each frame of a message.
➢ The process creates a virtual circuit, not a real circuit, b/w the source and destination.

2) Setup Phase

• A switch creates an entry for a virtual-circuit.
• For example, suppose source A needs to create a virtual-circuit to B.
• Two steps are required: i) Setup-request and ii) Acknowledgment.

i) Setup Request

➢ A setup-request frame is sent from the source to the destination (Figure 8.14).

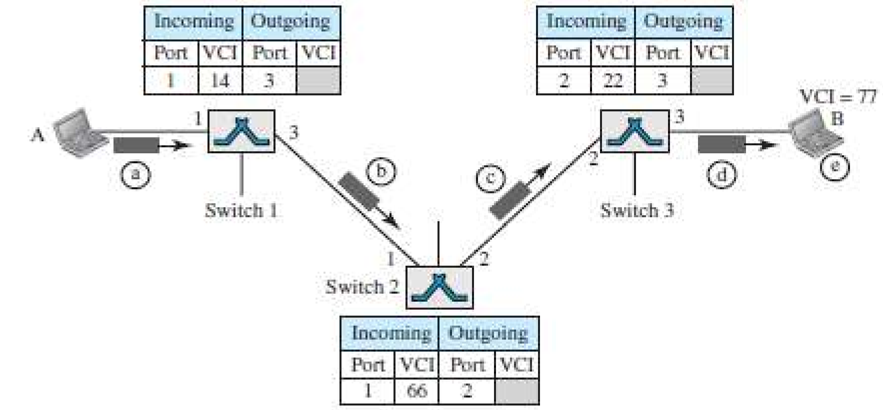


Figure 8.14 *Setup request in a virtual-circuit network*

ii) Acknowledgment

➢ A special frame, called the acknowledgment-frame, completes the entries in the switching-tables (Figure 8.15).

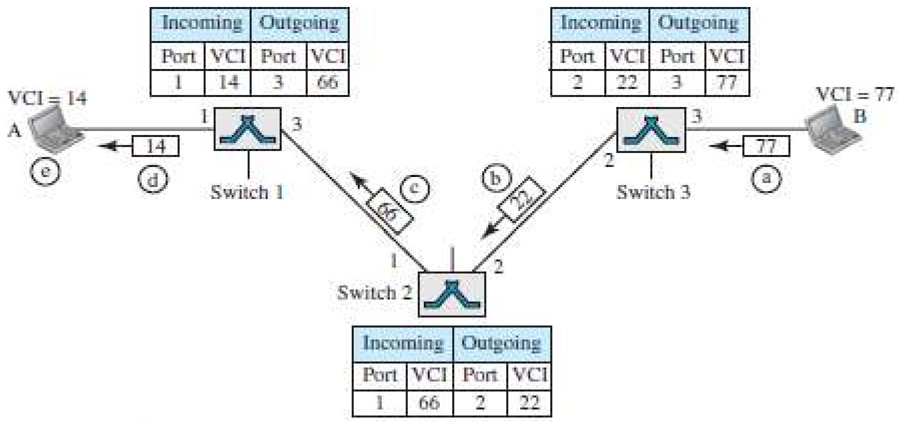


Figure 8.15 *Setup acknowledgment in a virtual-circuit network*

3) Teardown Phase

• Source-A, after sending all frames to B, sends a special frame called a teardown request.
• Destination-B responds with a teardown confirmation frame.
• All switches delete the corresponding entry from their tables.

4a. Explain CRC error detection method with an example (06 Marks)

Ans:

Cyclic Redundancy Check (CRC)

• CRC is a cyclic code that is used in networks such as LANs and WANs.

Table 10.3 *A CRC code with C(7, 4)*

Dataword	*Codeword*	*Dataword*	*Codeword*
0000	0000000	1000	1000101
0001	0001011	1001	1001110

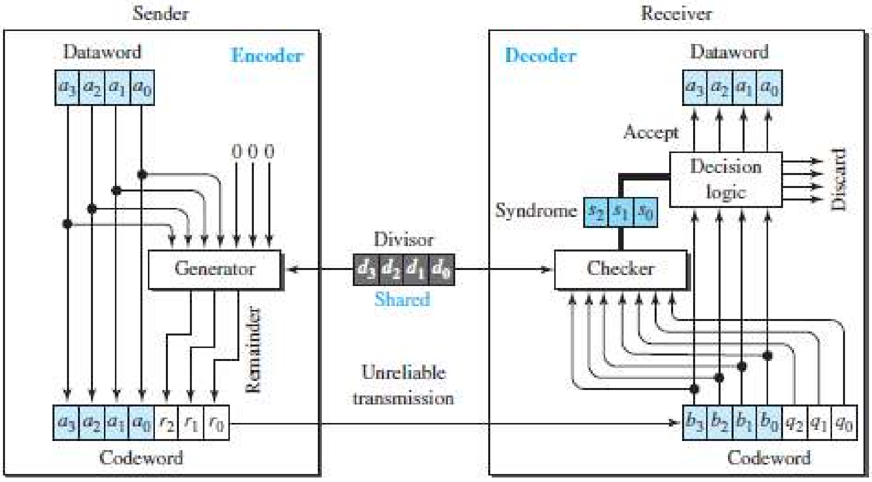


Figure 10.5 *CRC encoder and decoder*

• Let Size of data-word = k bits (here k=4). Size of code-word = n bits (here n=7).
  Size of divisor = n-k+1 bits (here n-k+1=4). (Augmented → increased)

• Here is how it works (Figure 10.5):

1) At Sender

- ➢ n-k 0s is appended to the data-word to create augmented data-word. (here n-k=3).
- ➢ The augmented data-word is fed into the generator (Figure 10.6).
- ➢ The generator divides the augmented data-word by the divisor.
- ➢ The remainder is called check-bits ($r_2r_1r_0$).
- ➢ The check-bits ($r_2r_1r_0$) are appended to the data-word to create the code-word.

2) At Receiver

- ➢ The possibly corrupted code-word is fed into the checker.
- ➢ The checker is a replica of the generator.
- ➢ The checker divides the code-word by the divisor.
- ➢ The remainder is called syndrome bits ($r_2r_1r_0$).
- ➢ The syndrome bits are fed to the decision-logic-analyzer.
- ➢ The decision-logic-analyzer performs following functions:

i) For No Error

¤ If all syndrome-bits are 0s, the received code-word is accepted.

¤ Data-word is extracted from received code-word.

ii) For Error

¤ If all syndrome-bits are not 0s, the received code-word is discarded (Fig 10.7b).

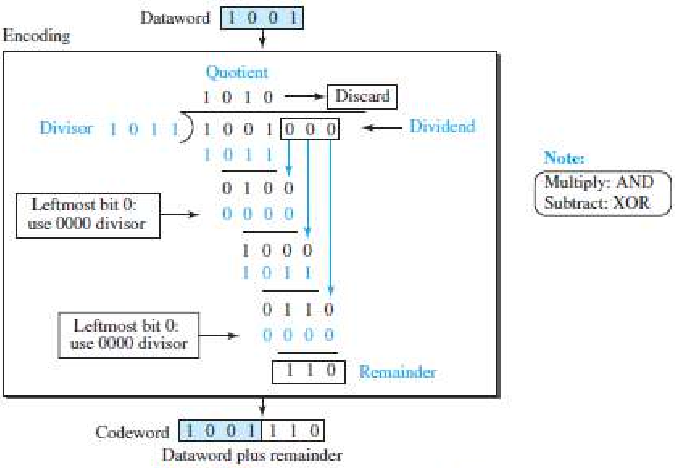


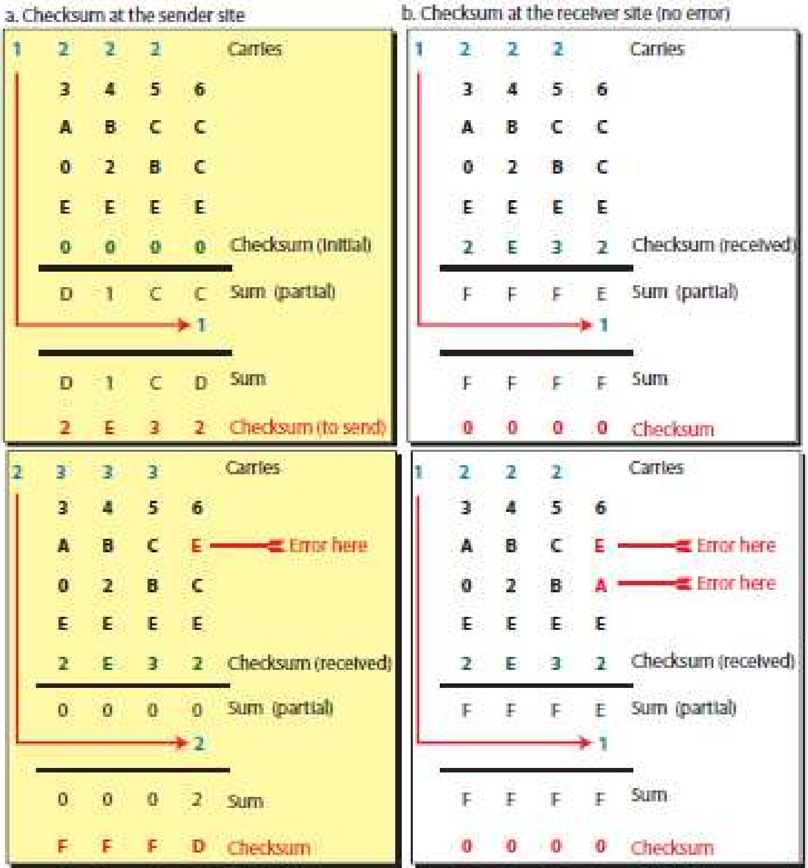
Figure 10.6 *Division in CRC encoder*

4b. Explain the structure of encoder and decoder for a Hamming code. (04 Marks)
Ans: For answer, refer Solved Paper June-2013 Q.No.4a.

4c. What is internet checksum? If a sender needs to send four data items 0X3456, 0XABCC, 0X02BC, 0XEEEE, answer the following
i) Find the checksum at sender's site.
ii) Find the checksum at receiver's site if there is no error. (10 Marks)

Ans:

Solution:



c. Checksum at the receiver site (one caught error) d. Checksum at the receiver site (two errors, but not caught)

a. In part a, we calculate the checksum to be sent (0x2E32)
b. In part b, there is no error in transition. The receiver recalculates the checksum to be all 0x0000. The receiver correctly assumes that there is no error.
c. In part c, there is one single error in transition. The receiver calculates the checksum to be 0FFFD. The receiver correctly assumes that there is some error and discards the packet.
d. In part d, there are two errors that cancel the effect of each other. The receiver calculates the checksum to be 0x0000. The receiver erroneously assumes that there is no error and accepts the packet. This is an example that shows that the checksum may slip in finding some types of errors.

5a. Explain i) GO-BACK-N ARQ and ii) selective-repeat-ARQ. List the differences between them. (10 Marks)
Ans (i): For answer, refer Solved Paper Dec-2013 Q.No.5a.(ii).
Ans (ii): For answer, refer Solved Paper June-2014 Q.No.5b.(ii).

5b. Explain the different frame types in HDLC. (06 Marks)

Ans:

Three Types of Frames

1) Information frames (I-frames): are used to transport user data and control information relating to user data (piggybacking).
2) Supervisory frames (S-frames): are used only to transport control information.
3) Unnumbered frames (U-frames): are reserved for system management.
   Information carried by U-frames is intended for managing the link itself.

• Each type of frame serves as an envelope for the transmission of a different type of message.

Control Fields of HDLC Frames

• The control field determines the type of frame and defines its functionality (Figure 11.17).

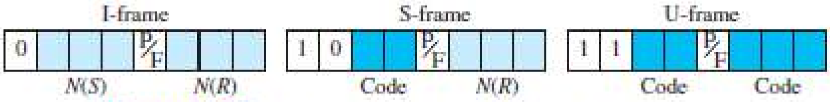


Figure 11.17 *Control field format for the different frame types*

1) Control Field for I-Frames

• The subfields in the control field are:

1) The first bit defines the type.
   If the first bit of the control field is 0, this means the frame is an I-frame.
2) The next 3 bits N(S) define the sequence-number of the frame.
   With 3 bits, we can define a sequence-number between 0 and 7
3) Last 3 bits N(R) correspond to the acknowledgment-number when piggybacking is used
4) The single bit between N(S) and N(R) is called the P/F bit.
   The P/F field is a single bit with a dual purpose. It can mean poll or final.
   i) It means poll when the frame is sent by a primary station to a secondary (when the address field contains the address of the receiver).
   ii) It means final when the frame is sent by a secondary to a primary (when the address field contains the address of the sender).

2) Control Field for S-Frames

• The subfields in the control field are:

1) If the first 2 bits of the control field is 10, this means the frame is an S-frame.
2) The last 3 bits N(R) corresponds to the acknowledgment-number (ACK) or negative acknowledgment-number (NAK).
3) The 2 bits called code is used to define the type of S-frame itself.
   With 2 bits, we can have four types of S-frames:

   1) Receive ready (RR) = 00
   ¤ This acknowledges the receipt of frame or group of frames.
   ¤ The value of N(R) is the acknowledgment-number.

   2) Receive not ready (RNR) = 10
   ¤ This is an RR frame with 1 additional function:
      i) It announces that the receiver is busy and cannot receive more frames.
   ¤ It acts as congestion control mechanism by asking the sender to slow down.
   ¤ The value of N(R) is the acknowledgment-number.

   3) Reject (REJ) = 01
   ¤ It is a NAK frame used in Go-Back-N ARQ to improve the efficiency of the process.
   ¤ It informs the sender, before the sender time expires, that the last frame is lost or damaged.
   ¤ The value of N(R) is the negative acknowledgment-number.

   4) Selective reject (SREJ) = 11
   ¤ This is a NAK frame used in Selective Repeat ARQ.
   ¤ The value of N(R) is the negative acknowledgment-number.

3) Control Field for U-Frames

• U-frame codes are divided into 2 sections:

i) A 2-bit prefix before the P/F bit
ii) A 3-bit suffix after the P/F bit.

• Together, these two segments (5 bits) can be used to create up to 32 different types of U-frames.

5c. Write a short note on piggybacking. (04 Marks)

Ans:

Piggybacking

• The technique of temporary delaying outgoing acknowledgements so that they can be hooked onto next outgoing data frame is known as Piggybacking.

• Piggybacking technique is used to improve the efficiency of the bidirectional protocols.

• As shown in Figure 5.1,

  ➢ When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B;

  ➢ When a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A

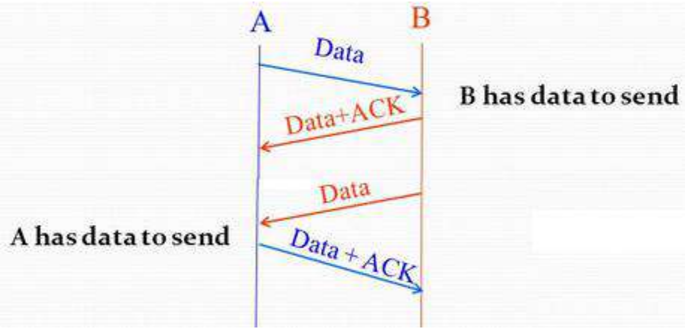


Figure 5.1: Piggybacking

6a. With a flow diagram, explain the working of CSMA/CD. (10 Marks)

Ans: **For answer, refer Solved Paper Dec-2013 Q.No.6a.(ii)**

6b. Explain the following channelization techniques: i) CDMA ii) TDMA. (10 Marks)

Ans(i): **For answer, refer Solved Paper June-2013 Q.No.6a.**

Ans (ii):

TDMA

• The stations share the bandwidth of the channel in time (Figure 12.22).
• Each time-slot is reserved for a specific station.
• Each station can send the data in the allocated time-slot.

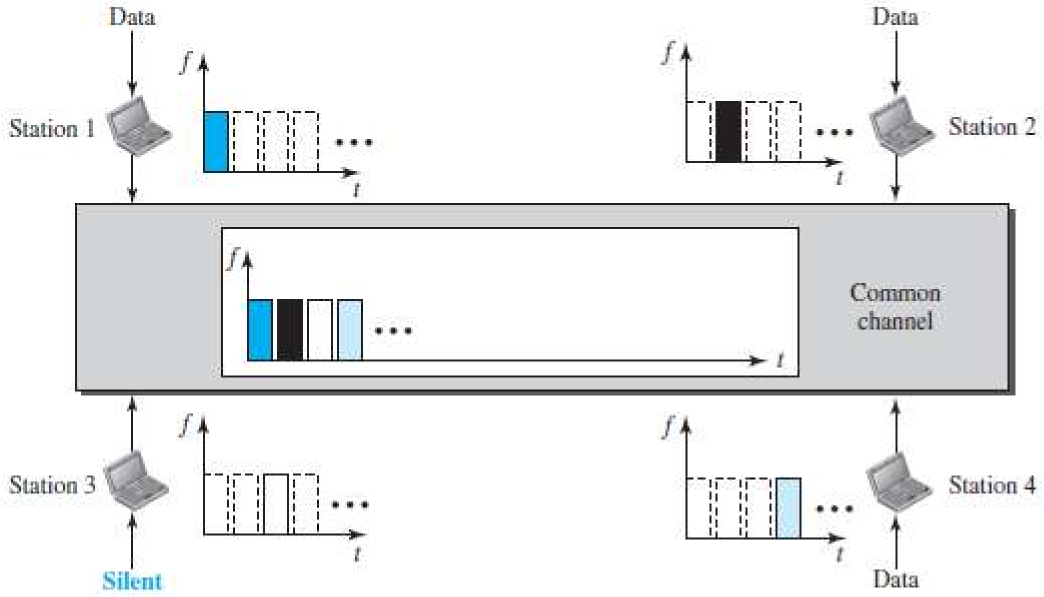


Figure 12.22 *Time-division multiple access (TDMA)*

• Main problem: Achieving synchronization between the different stations.
i.e. 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.
• To compensate for the delays, we can insert guard-times.
• Normally, synchronization is accomplished by having some synchronization bits at the beginning of each slot.
• TDMA vs. TDM

1) TDM

➢ TDM is a multiplexing method in the physical layer.
➢ TDM
→ combines the individual-data from slower channels and
→ transmits the aggregated- data by using a faster channel.
➢ The multiplexer interleaves data units from each channel.

2) TDMA

➢ TDMA is an access method in the data link layer.
➢ In each station, the data link layer tells the physical layer to use the allocated time-slot.
➢ There is no physical multiplexer at the physical layer.

7a. What do you mean by hidden and exposed station problems in IEEE 802.11 protocol. Explain in detail. (06 Marks)

Ans:

Hidden Station Problem

• Figure 15.3 shows an example of the hidden station problem.
• Every station in transmission range of Station B can hear any signal transmitted by station B.
• Every station in transmission range of Station C can hear any signal transmitted by station C.
• Station C is outside the transmission range of B;
Likewise, station B is outside the transmission range of C.
• However, Station A is in the area covered by both B and C;
Therefore, Station A can hear any signal transmitted by B or C.

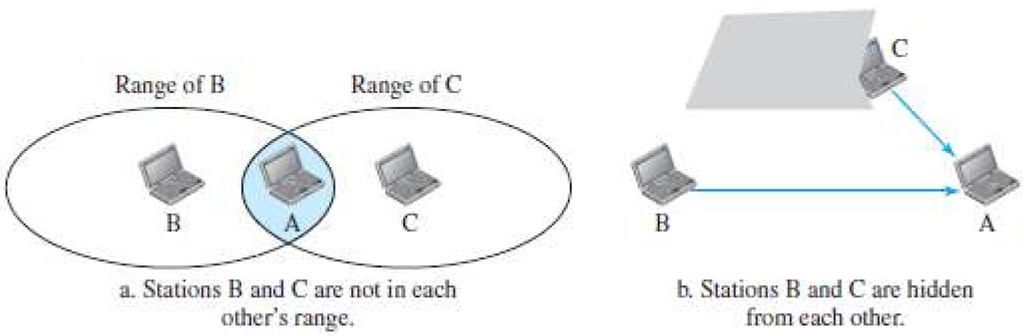


Figure 15.3 *Hidden station problem*

Exposed Station Problem

• In this problem, a station refrains from using a channel even when the channel is available for use.
• In the figure 14.12, station A is transmitting to station B.
• Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B.
• However, station C is exposed to transmission from A i.e. station C hears what A is sending and thus refrains from sending.
• In other words, C is too conservative and wastes the capacity of the channel.

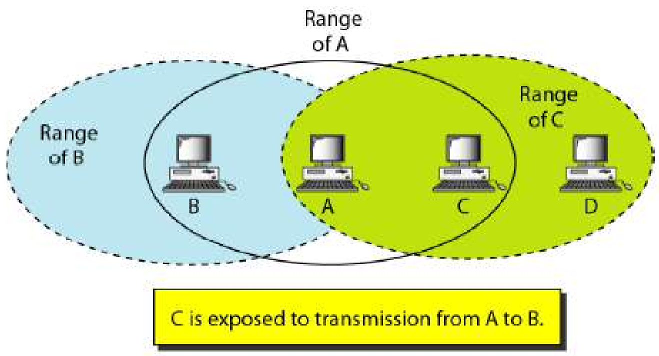


Figure 14.12 *Exposed station problem*

7b. With neat diagram, explain the architecture of Piconet and Scatternet Bluetooth networks. (06 Marks)

Ans:

BLUETOOTH

• Bluetooth is a wireless-LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on.

• The devices

→ find each other and

→ make a network called a piconet (Usually, devices are called gadgets)

Architecture

• Bluetooth defines 2 types of networks: 1) Piconet and 2) Scatternet.

1) Piconets

• A Bluetooth network is called a piconet, or a small net. (Figure 15.17).

• A piconet can have up to 8 stations. Out of which

i) One of station is called the primary.

ii) The remaining stations are called secondaries.

• All the secondary-stations synchronize their clocks and hopping sequence with the primary station.

• A piconet can have only one primary station.

• The communication between the primary and the secondary can be one-to-one or one-to-many.

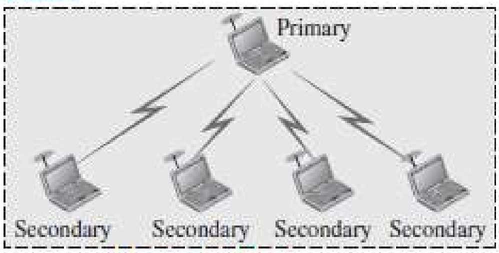


Figure 15.17 *Piconet*

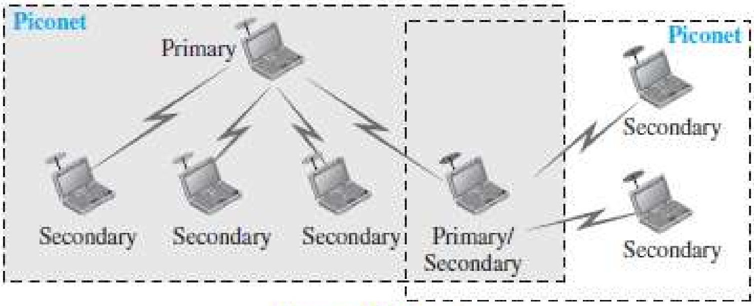


Figure 15.18 *Scatternet*

• Although a piconet can have a maximum of 7 secondaries, an additional 8 secondaries can be in the parked state.

• A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state.

• Because only 8 stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

2) Scatternet

• Piconets can be combined to form a scatternet (Figure 15.18).

• A station can be a member of 2 piconets.

• A secondary station in one piconet can be the primary in another piconet. This is called mediator station.

1) Acting as a secondary, mediator station can receive messages from the primary in the first piconet.

2) Acting as a primary, mediator station can deliver the message to secondaries in the second piconet.

7c. Explain the working of global system for mobile (GSM) in detail. (08 Marks)

Ans:

GSM

• Aim of GSM: to replace a number of incompatible 1G technologies.
• Here we discuss, two issues: 1) Bands 2) Transmission

1) Bands

➢ The system uses two bands for duplex communication (Figure 16.11).
➢ Each band is 25 MHz in width.
➢ Each band is divided into 124 channels of 200 kHz.

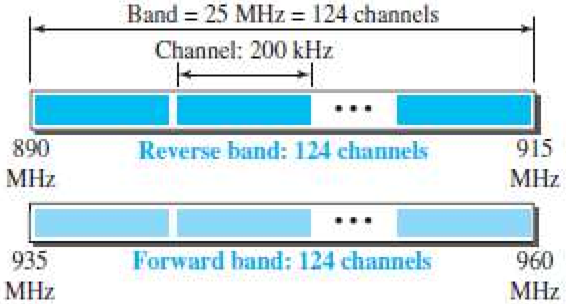


Figure 16.11 *GSM bands*

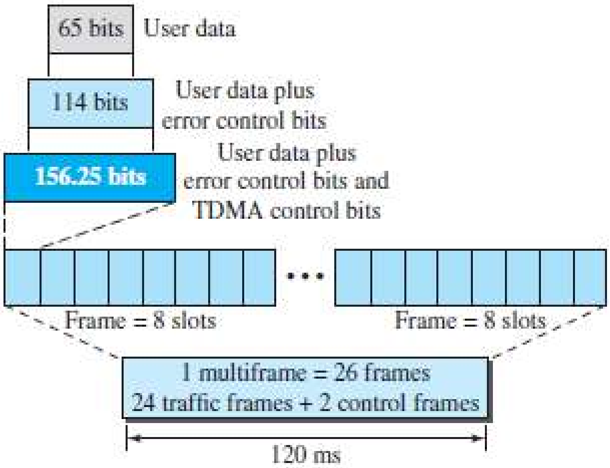


Figure 16.13 *Multiframe components*

2) Transmission

➢ Each voice channel is digitized and compressed to a 13-kbps digital signal (Fig 16.12).
➢ Each slot carries 156.25 bits.
➢ Eight slots share a frame (TDMA).
➢ 26 frames also share a multiframe (TDMA).
➢ We can calculate the bit rate of each channel as follows.

$$\text{Channel data rate} = (1/120 \text{ ms}) \times 26 \times 8 \times 156.25 = 270.8 \text{ kbps}$$

➢ Each 270.8-kbps digital channel modulates a carrier using GMSK (a form of FSK); the result is a 200-kHz analog signal.
➢ Finally, 124 analog channels of 200 kHz are combined using FDMA. The result is a 25-MHz band (Figure 16.13).

8a. Explain i) Header format & ii) Extension headers of IPV6 (10 Marks)

Ans (i): **For answer, refer Solved Paper Dec-2013 Q.No.8c.**

Ans (ii):

Extension Header

• An IP packet is made of
 → base-header &
 → some extension headers.

• To support extra functionalities, extension headers can be placed b/w base header and payload.

• There are Six types of extension headers (Figure 22.8).

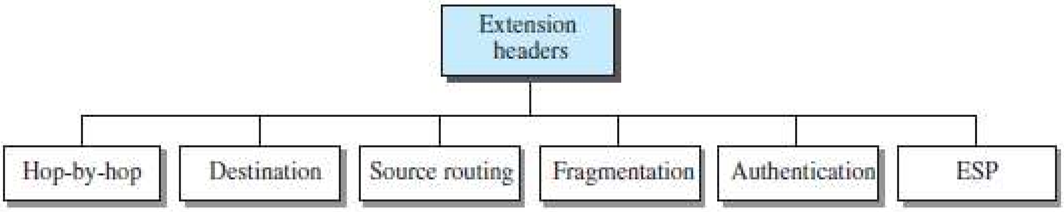


Figure 22.8 *Extension header types*

1) Hop-by-Hop Option

• This option is used when the source needs to pass information to all routers visited by the datagram.

• Three options are defined: i) Pad1, ii) PadN, and iii) Jumbo payload.

i) Pad1
- This option is designed for alignment purposes.
- Some options need to start at a specific bit of the 32-bit word.
- Pad1 is added, if one byte is needed for alignment.

ii) PadN
- PadN is similar in concept to Pad1.
- The difference is that PadN is used when 2 or more bytes are needed for alignment.

iii) Jumbo Payload
- This option is used when larger packet has to be sent. (> 65,535 bytes)
- Large packets are referred to as jumbo packets.
- Maximum length of payload = 65,535 bytes.

2) Destination Option

• This option is used when the source needs to pass information to the destination only.

• Intermediate routers are not allowed to access this information.

• Two options are defined: i) Pad1 & ii) PadN

3) Source Routing

• This option combines the concepts of
 → strict source routing and
 → loose source routing.

4) Fragmentation

• In IPv6, only the original source can fragment.

• A source must use a "Path MTU Discovery technique" to find the smallest MTU along the path from the source to the destination.

• Minimum size of MTU = 1280 bytes. This value is required for each network connected to the Internet.

• If a source does not use a Path MTU Discovery technique, the source fragments the datagram to a size of 1280 bytes.

5) Authentication

• This option has a dual purpose:
 i) Validates the message sender: This is needed so the receiver can be sure that a message is from the genuine sender and not from an attacker.
 ii) Ensures the integrity of data: This is needed to check that the data is not altered in transition by some attacker.

6) Encrypted Security Payload (ESP)

• This option provides confidentiality and guards against attacker.

8b. Write short note for following: (10 Marks)
i) FHSS ii) Gigabit Ethernet
iii) Polling iv) Token passing

Ans (i): **For answer, refer Solved Paper June-2013 Q.No.3a.**

Ans (ii):

GIGABIT ETHERNET

Table 13.3 *Summary of Gigabit Ethernet implementations*

Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
1000Base-SX	Fiber S-W	550 m	2	8B/10B + NRZ
1000Base-LX	Fiber L-W	5000 m	2	8B/10B + NRZ
1000Base-CX	STP	25 m	2	8B/10B + NRZ
1000Base-T4	UTP	100 m	4	4D-PAM5

• Goals of Gigabit-Ethernet:
1) Upgrade the data-rate to 1 Gbps.
2) Make it compatible with Standard or Fast-Ethernet.
3) Use the same 48-bit address.
4) Use the same frame format.
5) Keep the same minimum and maximum frame-lengths.
6) To support auto-negotiation as defined in Fast-Ethernet.

MAC Sublayer

• Gigabit-Ethernet has 2 distinctive approaches for medium access: half-duplex and full-duplex.

1) Full-Duplex Mode

• There is a central switch connected to all computers or other switches.
• Each switch has buffers for each input-port in which data are stored until they are transmitted.
• There is no collision. This means that CSMA/CD is not used.

2) Half-Duplex Mode

• A switch is replaced by a hub, which acts as the common cable in which a collision might occur.
• CSMA/CD is used.
• The maximum length of the network is totally dependent on the minimum frame size.
• Three methods have been defined:

i) Traditional
➢ Like traditional Ethernet, the minimum length of a frame is 512 bits.
➢ The maximum length of the network is 25 m.

ii) Carrier Extension
➢ To allow for a longer network, we increase the minimum frame-length.
➢ Minimum length of frame is 512 bytes (4096 bits).
➢ The maximum length of the network is 200 m.

iii) Frame Bursting
➢ Instead of adding an extension to each frame, multiple frames are sent.

Ans (iii):

Polling

• In a network,
One device is designated as a primary station and
Other devices are designated as secondary stations.
• Functions of primary-device:
1) Primary-device controls the link.
2) Primary-device is always the initiator of a session.
3) Primary-device determines which device is allowed to use the channel at a given time.
4) All data exchanges must be made through the primary-device.
• The secondary devices follow instructions of primary-device.
• Disadvantage: If the primary station fails, the system goes down.
• Poll and select functions are used to prevent collisions (Figure 12.19).

1) Select
➢ If the primary wants to send data, it tells the secondary to get ready to receive; this is called select function.

2) Poll
➢ If the primary wants to receive data, it asks the secondaries if they have anything to send; this is called poll function.

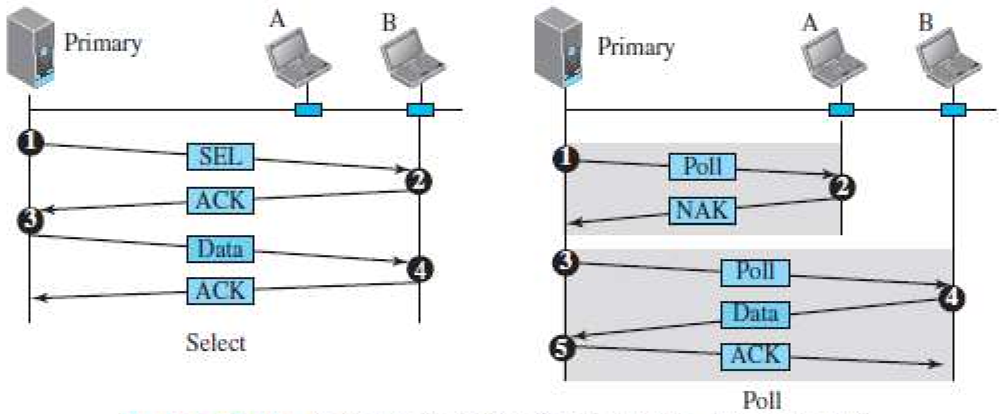


Figure 12.19 *Select and poll functions in polling-access method*

Ans (iv):

Token Passing

• In a network, the stations are organized in a ring fashion i.e. for each station; there is a predecessor and a successor.

1) The predecessor is the station which is logically before the station in the ring.
2) The successor is the station which is after the station in the ring.

• The current station is the one that is accessing the channel now.

• A token is a special packet that circulates through the ring.

• Here is how it works:

- A station can send the data only if it has the token.
- When a station wants to send the data, it waits until it receives the token from its predecessor.
- Then, the station holds the token and sends its data.
- When the station finishes sending the data, the station
  → releases the token
  → passes the token to the successor.

• There are four physical topologies to create a logical ring (Figure 12.20).

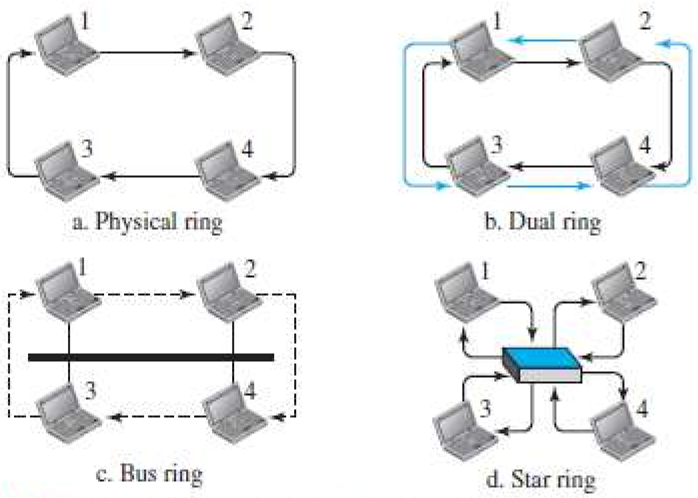


Figure 12.20 *Logical ring and physical topology in token-passing access method*

USN | | | | | | | | | | |

10CS55

Fifth Semester B.E. Degree Examination, June/July 2015
Computer Networks – I

Time: 3 hrs. Max. Marks:100

Note: ***Answer any FIVE full questions, selecting atleast TWO questions from each part.***

PART – A

1 a. What is data communication? What are the five components of data communication system? **(06 Marks)**
b. Explain the OSI reference model, listing the functions of each layer in brief. **(10 Marks)**
c. What are the four level of addresses used in internet employing TCP/IP. **(04 Marks)**

2 a. Using Shannon's theorem, compute the maximum bit rate for a channel having a band width of 3100 H_2 and signal to noise ratio of 20 db. **(06 Marks)**
b. Sketch the signal waveforms when 01001110 is transmit using following line coding schemes : i) R_2 ii) NRZ – L iii) Manchester coding. **(06 Marks)**
c. Explain different types of transmission modes. **(08 Marks)**

3 a. Four 1 – kbps connections are multiplexed together a unit is 1 bit. Find : i) the duration of 1–bit before multiplexing ii) the duration of a timeslot, iii) the duration a frame. **(06 Marks)**
b. Define direct sequence spread spectrum (DSSS) and explain how it achiever band with spread using relevant sketch. **(08 Marks)**
c. What is virtual circuit network? List the five characteristics of the same. **(06 Marks)**

4 a. Given the data word 1001 and divisor 1011 :
i) Show the generation code word at the sender site
ii) Show the checking of code word at receiver site (assume no error). **(10 Marks)**
b. Explain process of error detection and error detection using block coding. **(06 Marks)**
c. What is internet check sum? List the steps under taken by sender to calculate check sum.lss. **(04 Marks)**

PART – B

5 a. With neat diagram of point – to point protocol (PPP) frame format, explain each of the fields. **(08 Marks)**
b. Explain stop and wait automatic repeat request protocol. **(06 Marks)**
c. What is framing? With necessary sketches explain bit stuffing and unstuffing. **(06 Marks)**

6 a. With neat diagram explain TDMA. **(06 Marks)**
b. Mention different categories of standard Ethernet and explain implementation of 10 base 5 – thick Ethernet. **(08 Marks)**
c. Mention the five goals of fast Ethernet. And give the importance of "AUTONEGOTIATION". **(06 Marks)**

7 a. What is blue tooth? Explain its architecture. **(06 Marks)**
b. Explain the following connecting devices :
i) Hub ii) Bridge iii) Router iv) Gateway. **(08 Marks)**
c. Discuss cellular telephone in brief. **(06 Marks)**

8 a. List the deficiencies of IPV4 and advantages of IPV6 over IPV4. **(10 Marks)**
b. Draw format of an IPV6 datagram and explain. **(10 Marks)**

* * * * *

1a. What is data communication? What are the five components of data communication system? (06 Marks)
Ans: For answer, refer Solved Paper Dec-2013 Q.No.1a.

1b. Explain OSI reference model, listing the functions of each layer in brief. (10 Marks)
Ans: For answer, refer Solved Paper June-2013 Q.No.1a.

1c. What are the four level of addresses used in internet employing TCP/IP. (04 Marks)
Ans:
Addressing
• Any communication that involves 2 parties needs 2 addresses: source address and destination address.
• We need 4 pairs of addresses (Figure 2.9):

1) At the application layer, we normally use names to define
→ site that provides services, such as vtunotesbysri.com, or
→ e-mail address, such as vtunotesbysree@gmail.com.

2) At the transport layer, addresses are called port numbers.
➢ Port numbers define the application-layer programs at the source and destination.
➢ Port numbers are local addresses that distinguish between several programs running at the same time.

3) At the network-layer, addresses are called IP addresses.
➢ IP address uniquely defines the connection of a device to the Internet.
➢ The IP addresses are global, with the whole Internet as the scope.

4) At the data link-layer, addresses are called MAC addresses
➢ The MAC addresses defines a specific host or router in a network (LAN or WAN).
➢ The MAC addresses are locally defined addresses.

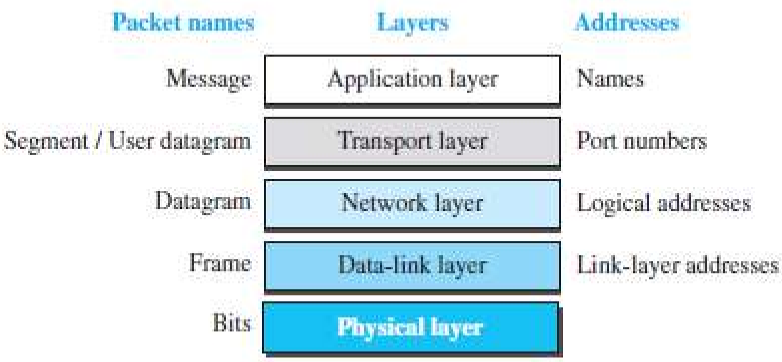


Figure 2.9 *Addressing in the TCP/IP protocol suite*

2a. Using Shannon's theorem, compute the maximum bit rate for a channal having a band width of 3100 Hz and signal to noise ratio of 20 db. (06 Marks)
Ans:

Solution:
$SNR_{dB} = 10 \log_{10} SNR \rightarrow SNR = 10^{SNR_{dB}/10} \rightarrow SNR = 10^2 = 100$
$C = B \log_2 (1 + SNR) = 3100 \log_2 (1 + 100) = 3100 \log_2 101 = 3100 \times 6.65 = 20615$ bps

2b. Sketch the signal waveform when 01001110 is transmit using following line coding schemes i) RZ ii) NRZ—L iii) Manchester coding. (06 Marks)
Ans: For answer, refer Solved Paper June-2013 Q.No.2a.

2c. Explain different types of transmission modes. (08Marks)
Ans: For answer, refer Solved Paper Dec-2013 Q.No.2b.

3 a. Four 1-kbps connections are muhiplexed together a unit is 1 bit. Find :
i) the duration of 1-bit before multiplexing
ii) the duration of a timeslot
iii) the duration a frame. (06 Marks)
Ans: For answer, refer Solved Paper June-2013 Q.No.3b.

3b. Define direct sequence spread spectrum (DSSS) and explain how it achieves bandwith spread using relevant sketch. (08 Marks)

Ans: **For answer, refer Solved Paper June-2014 Q.No.3b.**

3c. What is virtual circuit network? List the five characteristics of the same. (06 Marks)

Ans:

Virtual Circuit Network (VCN)

- This is similar to telephone system.
- A virtual-circuit network is a combination of circuit-switched-network and datagram-network.
- Five characteristics of VCN:
  1) As in a circuit-switched-network, there are setup & teardown phases in addition to the data transfer phase.
  2) As in a circuit-switched-network, resources can be allocated during the setup phase. As in a datagram-network, resources can also be allocated on-demand.
  3) As in a datagram-network, data is divided into packets. Each packet carries an address in the header. However, the address in the header has local jurisdiction, not end-to-end jurisdiction.
  4) As in a circuit-switched-network, all packets follow the same path established during the connection.
  5) A virtual-circuit network is implemented in the data link layer. A circuit-switched-network is implemented in the physical layer. A datagram-network is implemented in the network layer.

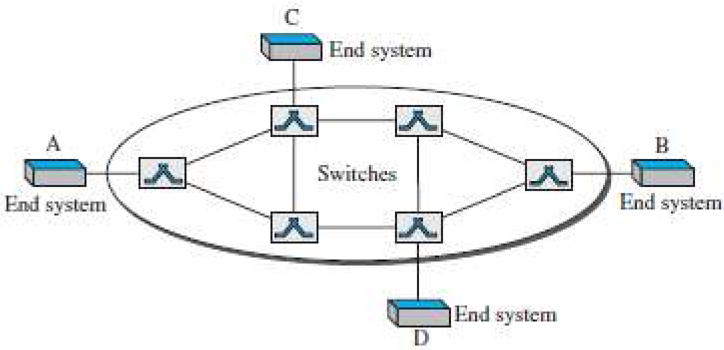


Figure 8.10 *Virtual-circuit network*

- ➢ The Figure 8.10 is an example of a virtual-circuit network.
- ➢ The network has switches that allow traffic from sources to destinations.
- ➢ A source or destination can be a computer, packet switch, bridge, or any other device that connects other networks.

4a. Given the data word 1001 and divisor 1011 : (10 Marks)

i) Show the generation code word at the sender site

ii) Show the checking of code word at receiver site (assume no error).

Ans: **For answer, refer Solved Paper June-2013 Q.No.4b.**

4b. Explain process of error detection using block coding. (06 Marks)

Ans: **For answer, refer Solved Paper Dec-2013 Q.No.4b.**

4c. What is internet checksum? List the steps under taken by sender to calculate check sum. (04 Marks)

Ans: **For answer, refer Solved Paper June-2013 Q.No.4c.**

5a. With neat diagram of point-to-point protocol (PPP) frame format, explain each of the fields. (08 Marks)

Ans: **For answer, refer Solved Paper Dec-2013 Q.No.5b.**

5b. Explain stop and wait automatic repeat request protocol. (06 Marks)

Ans: **For answer, refer Solved Paper June-2013 Q.No.5a.**

5c. What is framing? With sketches explain bit stuffing and unstuffing. (06 Marks)
Ans: **For answer, refer Solved Paper June-2013 Q.No.5b.**

6a. With neat diagram explain TDMA. (06 Marks)
Ans: **For answer, refer Solved Paper Dec-2014 Q.No.6b.(ii)**

6b. Mention different categories of standard Ethernet and explain implementation of 10 base 5-thick Ethernet. (08 Marks)
Ans:
Implementation
• The Standard-Ethernet defines several physical-layer implementations (Table 13.1).

Table 13.1 *Summary of Standard Ethernet implementations*

Implementation	*Medium*	*Medium Length*	*Encoding*
10Base5	Thick coax	500 m	Manchester
10Base2	Thin coax	185 m	Manchester
10Base-T	2 UTP	100 m	Manchester
10Base-F	2 Fiber	2000 m	Manchester

Encoding and Decoding
• All standard implementations use digital-signaling (baseband) at 10 Mbps (Figure 13.6).
1) At the sender, data are converted to a digital-signal using the Manchester scheme.
2) At the receiver, the received-signal is
→ interpreted as Manchester and
→ decoded into data.

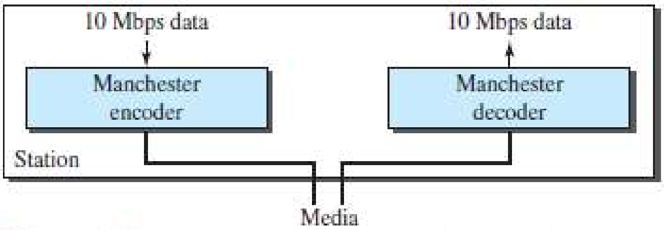


Figure 13.6 *Encoding in a Standard Ethernet implementation*

10Base5: Thick Ethernet
➢ 10Base5 uses a bus topology (Figure 13.7).
➢ A external transceiver is connected to a thick coaxial-cable.
(transceiver → transmitter/receiver)
➢ The transceiver is responsible for
→ transmitting
→ receiving and
→ detecting collisions.
➢ The transceiver is connected to the station via a coaxial-cable.
The cable provides separate paths for sending and receiving.
The collision can only happen in the coaxial cable.

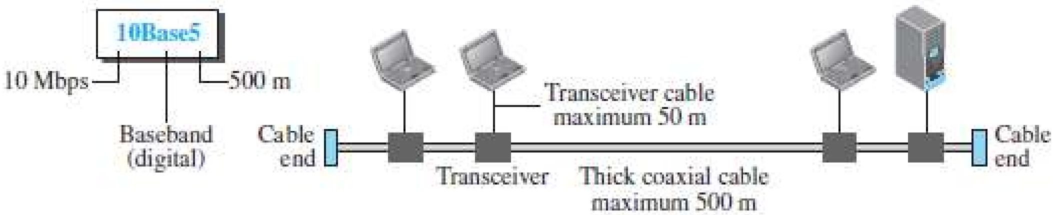


Figure 13.7 *10Base5 implementation*

➢ The maximum-length of the cable must not exceed 500m.
If maximum-length is exceeded, then there will be excessive degradation of the signal.
➢ If a cable-length of more than 500 m is needed, the total cable-length can be divided into up to 5 segments.
➢ Each segment of maximum length 500-meter, can be connected using repeaters.

6c. Mention the five goals of fast Ethernet. And give the importance of "AUTONEGOTIATION". (06 Marks)

Ans:

FAST ETHERNET (100 MBPS)

- IEEE created Fast-Ethernet under the name 802.3u.
- Goals of Fast-Ethernet:
  1) Upgrade the data-rate to 100 Mbps.
  2) Make it compatible with Standard-Ethernet.
  3) Keep the same 48-bit address.
  4) Keep the same frame format.
  5) Keep the same minimum and maximum frame-lengths.

Access Method

- Only the star topology is used.
- For the star topology, there are 2 choices:
  1) In half-duplex approach, the stations are connected via a hub.
     CSMA/CD was used as access-method.
  2) In full-duplex approach, the connection is made via a switch with buffers at each port.
     There is no need for CSMA/CD.

Autonegotiation

- A new feature added to Fast-Ethernet is called autonegotiation.
- It provides a station/hub with a range of capabilities.
- It was used for the following purposes:
  1) To allow 2 devices to negotiate the mode or data-rate of operation.
  2) To allow incompatible devices to connect to one another.
     For example: a device with a maximum capacity of 10 Mbps can communicate with a device with a 100 Mbps capacity.
  3) To allow one device to have multiple capabilities.
  4) To allow a station to check a hub's capabilities.

7a. What is blue tooth? Explain its architecture. (06 Marks)

Ans: **For answer, refer Solved Paper Dec-2014 Q.No.7b.**

7b. Explain the following connecting devices (08 Marks)

i) Hub ii) Bridge iii) Router iv) Gateway.

Ans: **For answer, refer Solved Paper June-2013 Q.No.7b.**

7c. Discuss cellular telephone in brief. (06 Marks)

Ans:

CELLULAR TELEPHONY

• Cellular telephony is designed to provide communications
→ between two moving units called mobile-stations (MSs) or
→ between one mobile-station and one stationary unit called a land unit (Figure 16.6).

• A service-provider is responsible for
→ locating & tracking a caller
→ assigning a channel to the call and
→ transferring channel from base-station to base-station as caller moves out-of-range.

• Each cellular service-area is divided into small regions called cells.
• Each cell contains an antenna.
• Each cell is controlled by AC powered network-station called the base-station (BS).
• Each base-station is controlled by a switching office called a mobile-switching-center (MSC).
• MSC coordinates communication between all the base-stations and the telephone central office.
• MSC is a computerized center that is responsible for
→ connecting calls
→ recording call information and
→ billing.

• Cell-size is not fixed; Cell-size can be increased or decreased depending on population of the area.
• Cell-radius = 1 to 12 mi.
• Compared to low-density areas, high-density areas require many smaller cells to meet traffic demands.
• Cell-size is optimized to prevent the interference of adjacent cell-signals.

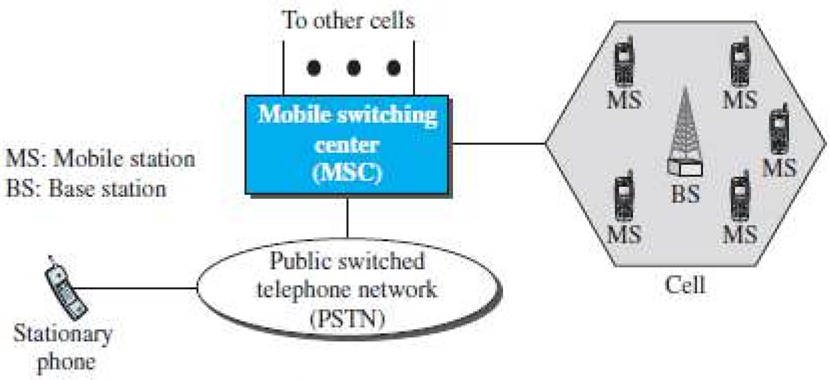


Figure 16.6 *Cellular system*

8a. List i) deficiencies of IPV4 and ii) advantages of IPV6 over IPV4. (10 Marks)

Ans(i):

Deficiencies of IPV4

1) Scarcity of IPv4 Addresses: The recent exponential growth of the Internet and the exhaustion of the IPv4 address space
2) Security Related Issues: The requirement for security at the Internet layer
3) Absence of support of QoS: The need for better support for prioritized and real-time delivery of data.
4) Absence of the autoconfiguration addresses mechanism: Internet is expanding and many new devices are using IP. The configuration of IP addresses should be simple.
5) The problems related to fragmentation: The size of the maximal block of data transmission on each concrete way is not defined;

Ans(ii): **For answer, refer Solved Paper June-2014 Q.No.8c.(i)**

8b. Draw format of an IPV6 datagram and explain. (10 Marks)

Ans: **For answer, refer Solved Paper Dec-2013 Q.No.8b.**