# 2020

# RANK Improvement WORKBOOK

## Answer key and Hint of Objective & Conventional *Questions*

## Electronics Engineering

Advanced Communication

MADE EASY Publications

# 1 Microwave Communication

## LEVEL 1 Objective Solutions

1. (b)
2. (b)
3. (c)
4. (a)
5. (c)
6. (a)
7. (d)
8. (c)
9. (b)
10. (c)
11. (b)
12. (d)

■■■■

## LEVEL 2 Conventional Solutions

**Solution: 1**

(i) $$\text{LOS distance} = 4.12\left(\sqrt{h_t} + \sqrt{h_r}\right) \text{ km} = 49.44 \text{ km}$$

(ii) Electric field strength received ($E_r$) at a distance "$d$" from the transmitter can be given by,

$$E_r = \frac{88\sqrt{P_t}}{\lambda d^2} h_t h_r$$

$d$ = LOS distance = 49.44 km

$E_r$ = 147 μV/m

**Solution: 2**

- In an ionized medium having free electrons and ions when the radio waves passes through it set these charged particles in motion. The radio wave passing through the ionosphere is influenced by the electrons only and the electric field of radio wave set electrons of the ionosphere in motion.
- These electrons then vibrate simultaneously along paths parallel to the electric field of the radio waves and the vibrating electrons present an AC current proportional to the velocity of vibration.
- Here the effect of earth's magnetic field on the vibrations of ionospheric electrons lags behind the electric field of wave, thus resulting electron current is inductive. The actual current flowing through a volume of space consist of the components e.g. the usual capacitive current which leads the voltage by 90° and the electron current which lags the voltage by 90° and hence subtracted from the capacitive current.
- Thus free electrons in the space decreases the current and dielectric constant of space is also reduced. **The reduction in the dielectric constant due to presence of the electrons in the ionosphere causes the path of radio waves to be bent towards earth i.e. from higher electron density to lower electron density.**

  Let the electric field of value, $E = E_m \sin\omega t$ volts/metre is acting across a cubic metre of space in the ionosphere, where ω is the angular velocity and $E_m$, the maximum amplitude.

  Force exerted by electric field on each electron is given by

  $$F = -eE \quad \text{Newton}$$

  Let us assume there is no collision, then the electron will have an instantaneous velocity $v$ meters/sec.

  $$\text{Force} = \text{Mass} \times \text{Acceleration}$$

  $$-Ee = m\frac{dV}{dt}$$

  where, $m$ = Mass of electrons (in kg) ; $\frac{dV}{dt}$ = Acceleration

  Integrating both sides, we have

  $$\int dV = -\int \frac{eE}{m} dt \; ; \; v = -\frac{e}{m}\int E_m \sin\omega t dt$$

  $$v = \frac{-eE_m \cos\omega t}{m\omega} = -\left(\frac{e}{m\omega}\right) E_m \cos\omega t \qquad \ldots(i)$$

- If $N$ be the number of electrons per cubic metre, then instantaneous electric current constituted by these $N$ electrons moving with instantaneous velocity $v$ is

$$i_e = -Nev \text{ amp/m}^2 = -Ne\left(\frac{e}{m\omega}\right)E_m \cos\omega t$$

From equation (i)

$$i_e = -\left(\frac{Ne^2}{m\omega}\right)E_m \cos\omega t \quad \text{...(ii)}$$

which shows current $i_e$ lags behind the electric field $E$ by 90°.

- Beside this inductive current, there is a capacitive current (**or displacement current exists in an unionized air**).

The capacitive or displacement current through the capacitance is

$$i_c = \frac{d}{dt}\vec{D} = \frac{d}{dt}(\epsilon_0 E) = \epsilon_0 \frac{d}{dt}(E_m \sin\omega t)$$

$$i_c = \epsilon_0 E_m \omega \cos\omega t \quad \text{...(iii)}$$

Thus, total current $i$ that flows through a cubic metre of ionized medium is

$$i = i_c + i_e = \epsilon_0 E_m \omega \cos\omega t - \frac{Ne^2}{m\omega}E_m \cos\omega t$$

$$i = E_m \omega \cos\omega t\left[\epsilon_0 - \frac{Ne^2}{m\omega^2}\right] \quad \text{...(iv)}$$

From equation (iii) and (iv), the effective dielectric constant of the ionosphere (i.e. ionized space).

$$\epsilon = \epsilon_0 - \frac{Ne^2}{m\omega^2} = \epsilon_0\left[1 - \frac{Ne^2}{m\omega^2 \epsilon_0}\right]$$

Hence, the relative dielectric constant w.r.t. air

$$\epsilon_r = \frac{\epsilon}{\epsilon_0} = 1 - \frac{Ne^2}{m\omega^2 \epsilon_0}$$

Thus, refractive index (μ) of the ionosphere w.r.t. vacuum or air is given by

$$\mu = \sqrt{\epsilon_r} = \sqrt{\frac{\epsilon}{\epsilon_0}} = \sqrt{1 - \frac{Ne^2}{m\omega^2 \epsilon_0}}$$

Putting, $m = 9.107 \times 10^{-31}$ kg

$e = 1.602 \times 10^{-19}$ Coulombs

$\epsilon_0 = 8.854 \times 10^{-12}$ F/m

So, we get, $\mu = \sqrt{1 - \frac{81N}{f^2}}$

When wave is refracted

$$\mu = 0$$

as $$\theta_i = 0,$$

$$\sin\theta_i = 0$$

and $$f = f_P$$

So $$\frac{1-81N}{f_p^2} = 0$$

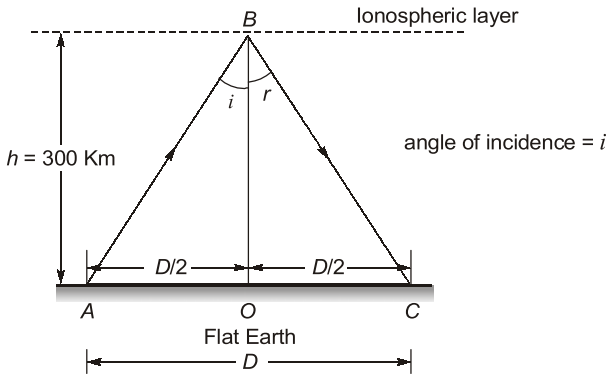
$$f_p = 9\sqrt{N_{max}}$$

Thus $f_p$ is of the from $f_P = 9\sqrt{N}$

For ionosphere with $N = 10^{12}$

$$f_P = 9\sqrt{10^{12}} = 9 \times 10^6 \text{ Hz} = 9 \text{ MHz}$$

**Solution: 3**




Ionization density (electrons per cubic meter) = $N_{max} = 5 \times 10^{11} / m^3$

$$\therefore \quad f_{cr} = 9\sqrt{N_{max}} = 6.36 \text{ MHz}$$

Maximum permissible frequency under flat earth assumptions is,

$$f_{muf} = f_c\sqrt{1+\left(\frac{D}{2h}\right)^2} = 6.36\sqrt{1+\left(\frac{1039.23}{600}\right)^2} \approx 12.72 \text{ MHz}$$

Now, Skip distance $= D_{SKIP} = 2h\sqrt{\left(\frac{f_{muf}}{f_{cr}}\right)^2 - 1} = 1040$ km

■■■■

# 2 Satellite Communication

## LEVEL 1 Objective Solutions

1. (a)
2. (d)
3. (b)
4. (b)
5. (c)
6. (a)
7. (b)
8. (b)
9. (a)
10. (b)
11. (a)
12. (a)
13. (d)
14. (a)
15. (b)
16. (c)
17. (b)
18. (b)
19. (c)
20. (a)
21. (b)
22. (a)
23. (c)
24. (a)
25. (c)
26. (b)
27. (b)
28. (d)
29. (b)
30. (d)
31. (a)
32. (d)
33. (a)

## LEVEL 2 Conventional Solutions

**Solution : 1**

**(a)** $\text{EIRP} = P_t + G_t = P_t + 52 \text{ dBW}$

Flux density, $F = 20\log\left[\frac{\text{EIRP}}{(4\pi R^2)}\right] \text{dBW/m}^2$

By solving, $\text{EIRP} = 72.8 \text{ dBW}$

**(b)** $\text{EIRP} = P_t + G_t = 72.8 \text{ dBW}$

Hence, $P_t = 72.8 - 52.0 = 20.8 \text{ dBW}$

**Solution : 2**

Free space loss, $L_s(\text{dB}) = 32.45 + 20\log_{10} d + 20\log_{10} f$

where $d$ in km and $f$ in MHz.

$L_s(\text{dB}) = 199.105 \text{ dB}$

Carrier to noise ratio at satellite receiver input is

$$\frac{C}{N_0} = (\text{EIRP})_{\text{dBW}} + M(\text{dB}) - L_T(\text{dB}) - L_s(\text{dB}) + 228.6$$

$$= 80 + (-8) - 0.6 - 199.105 + 228.6 = 100.895 \text{ dB}$$

**Solution: 3**

**(a)** Flux density is given, $F = 20\log\left[\frac{P_t G_t}{(4\pi R^2)}\right] \text{dBW/m}^2$

By solving, $F = -122.7 \text{ dBW/m}^2$

**(b)**

Path loss, $L_p = 20\log\left(\frac{4\pi R}{\lambda}\right) = 196.2 \text{ dB}$

$P_r = P_t + G_t + G_r - L_p = -117.2 \text{ dBW}$

**(c)** Transponder $\text{EIRP} = P_t + G_t = 40 \text{ dBW}$

**Solution: 4**

$$\left[\frac{C}{N_0}\right] = [\text{EIPR}] + \left[\frac{G}{T}\right] - [\text{Losses}] - [k]$$

$[k]$ = Boltzmann constant in dB = –228.6 dB

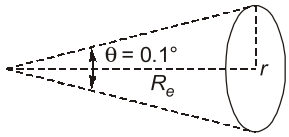
[Losses] = [FSL] + [APL] + [AA] + [RFL] = 210 dB

$$\left[\frac{C}{N_0}\right] = 86.10 \text{ dBHz}$$

**Solution: 5**

$$\text{Beam width} = \theta = 0.1^\circ$$

$$\text{Angle} = \frac{\text{Arc}}{\text{Radius}}$$




$$\Rightarrow \quad \frac{\theta}{2} = \frac{r}{R_e}$$

$$\Rightarrow \quad \frac{0.1\times\pi}{2\times 180} = \frac{r}{35860}$$

$$\Rightarrow \quad r = 31.294 \text{ km}$$

Area of spot, $A = \pi r^2 = \pi \times (31.294)^2 = 3076.61 \text{ km}^2$

■■■■

# 3 Optical Fibre

## LEVEL 1 Objective Solutions

1. (a)
2. (b)
3. (c)
4. (c)
5. (b)
6. (d)
7. (b)
8. (a)
9. (d)
10. (b)
11. (a)
12. (a)
13. (c)
14. (d)
15. (b)
16. (d)
17. (b)
18. (c)

■■■■

## LEVEL 2 Conventional Solutions

**Solution: 1**

(i) $$l_{max} = 12.5 \text{ km}$$

(ii) Minimum 7 repeaters are required to construct the link with a length of 100 km.

**Solution: 2**

(i) $$\text{Signal attenuation} = 10\log_{10}\frac{P_i}{P_o} = 16.0 \text{ dB}$$

(ii) $$\alpha_{dB} L = 16.0 \text{ dB}$$

Hence, $$\alpha_{dB} = \frac{16.0}{8} = 2.0 \text{ dB km}^{-1}$$

(iii) As $\alpha_{dB} = 2$ dB km$^{-1}$, the loss occurred along 10 km of the fiber is given by

$$\alpha_{dB} L = 2 \times 10 = 20 \text{ dB}$$

However, the link also has nine splices (at 1 km intervals) each with an attenuation of 1 dB. Therefore, the loss due to the splices is 9 dB.

Hence, the overall signal attenuation for the link is

$$\text{Signal attenuation} = 20 + 9 = 29 \text{ dB}$$

**Solution : 3**

Given

(i)

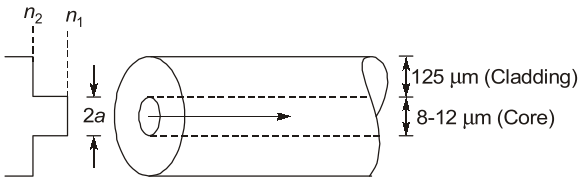



Fig. Step index single-mode fibre

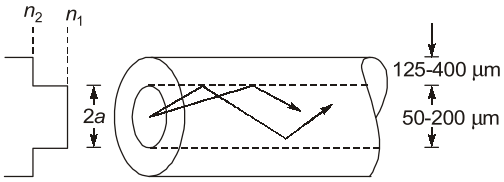



Fig. Step index multi-mode fibre

(ii)

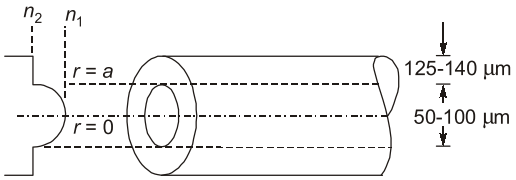



Fig. Graded index multi-mode fibre

Core refractive index $n_1 = 1.46$

Core radius $a = 4.5$ μm

Relative index $\Delta = 0.25\%$

So $$\lambda_c = \frac{2\pi a}{V_c}(NA) = \frac{2\pi a n_1}{V_c}(2\Delta)^{1/2}$$

$[NA = n_1(2\Delta)^{1/2}]$

$$= \frac{2\pi \times 4.5 \times 10^{-6} \times 1.46}{2.405}\left(2 \times \frac{0.25}{100}\right)^{1/2} = 1.214\ \mu m$$

**Solution: 4**

The SNR is, $$\frac{S}{N} = \frac{\eta P_o}{2\pi fB}$$

Hence, $$P_o = \left(\frac{S}{N}\right)\frac{2\pi fB}{\eta}$$

For $\frac{S}{N}$ = 50 dB, when considering signal and noise powers:

$$10\log_{10}\left(\frac{S}{N}\right) = 50$$

and therefore, $$\frac{S}{N} = 10^5$$

At 1 μm, $f = 2.998 \times 10^{14}$ Hz. For an ideal detector $\eta = 1$ and, thus incident optical power.

$$P_o = \frac{10^5 \times 2 \times 6.626 \times 10^{-34} \times 2.998 \times 10^{14} \times 5 \times 10^6}{1} = 198.6\ nW$$

In dBm, $P_o = 10\log_{10} 198.6 \times 10^{-6} = -40 + 2.98 = -37.0$ dBm

Therefore, the incident optical power required to achieve an SNR of 50 dB at the receiver is 198.6 nW which is equivalent to –37.0 dBm.

**Solution: 5**

**(i)** Radius of core = 33.82 μm

Core area $A$ = 3.59 $nm^2$

**(ii)** Cut-off $V$ for single mode $V_c$ = 2.405

$$2.405 = \frac{2\pi a}{1.3 \times 10^{-6}} \times 0.173$$

$$a = 2.876\ \mu m$$

So, Core area = $\pi \times (2.876 \times 10^{-6})^2 = 25.98\ pm^2$

■■■■

# 4 Cellular Communication

## LEVEL 1 Objective Solutions

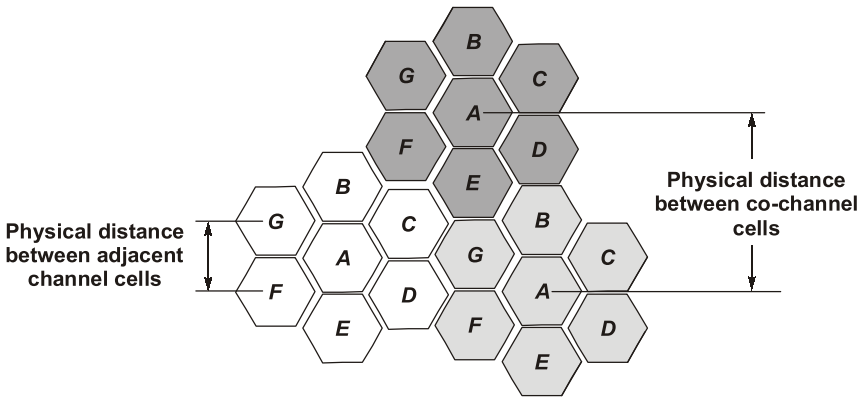
1. (c)
2. (b)
3. (b)
4. (b)
5. (b)
6. (b)
7. (b)
8. (c)
9. (d)
10. (c)
11. (a)

## LEVEL 2 Conventional Solutions

**Solution : 1**

### Co-channel Interference:

For the efficient use of available spectrum, it is necessary to reuse frequency bandwidth over relatively small geographical areas. However, increasing frequency reuse also increases interference, which decreases system capacity and service quality. The cells, which are using same set of frequencies, are called co-channel cells.




Co-channel interference is the cross talk between two different radio transmitters using the same radio frequency, i.e. the interference between co-channel cells. The reasons of co-channel interference can be because of either adverse weather conditions or poor frequency planning or overly crowded radio spectrum.

If the cell size and the power transmitted at the base stations of co-channel cells are same then the co-channel interference will become independent of the transmitted power and will depend on radius of the cell ($R$) and the distance between the interfering co-channel cells ($D$). If $D/R$ ratio is increased, then the effective distance between the co-channel cells will increase and interference will decrease.

The parameter $Q$ is called the frequency reuse ratio and is related to the cluster size. For hexagonal geometry,

$$Q = \frac{D}{R} = \sqrt{3N}$$

From the above equation, it is clear that, as the frequency reuse ratio increases, the co-channel interference will be reduced.

### Adjacent Channel Interference:

This is a different type of interference which is caused by adjacent channels i.e. channels in adjacent cells. It is the signal impairment which occurs to one frequency due to presence of another signal on a nearby frequency. This occurs when imperfect receiver filters allow nearby frequencies to leak into the passband. This problem is enhanced if the adjacent channel user is transmitting in a close range compared to the subscriber's receiver while the receiver attempts to receive a base station on the channel. This is called near-far effect.

This effect can also occur if a mobile close to a base station transmits on a channel close to one being used by a weak mobile. This problem might occur if the base station has problem in discriminating the mobile user from the "bleed over" caused by the close adjacent channel mobile.

Adjacent channel interference occurs more frequently in small cell clusters and heavily used cells. If the frequency separation between the channels is kept large, then this interference can be reduced to some extent. Thus assignment of channels is given such that they do not form a contiguous band of frequencies within a particular cell and frequency separation is maximized. Efficient assignment strategies are very much important in making the interference as less as possible.

**Solution : 2**

(i) Total number of duplex channels for voice = $\frac{50\times10^6}{50\times10^3} = 1000$

(ii) Total number of duplex channels for control = $\frac{1\times10^6}{50\times10^3} = 20$

(iii) Total number of cells within a cluster = 5

Voice channels per cell = $\frac{1000}{5} = 200$

Control channels per cell = $\frac{20}{5} = 4$

Total number of channels per cell = 200 + 4 = 204.

**Solution : 3**

Fixed Channel Assignment (FCA) :

In fixed channel assignment strategy each cell is allocated a fixed number of voice channels. Any communication within the cell can only be made with the designated unused channels of that particular cell. Suppose if all the channels are occupied, then the call is blocked and subscriber has to wait.

This is the simplest way of the channel assignment strategies, as it requires very simple circuitry but provides worst channel utilization.

Later there was another approach in which the channels were borrowed from adjacent cell if all of its own designated channels were occupied. This was named as borrowing strategy. In such cases the MSC supervises the borrowing process and ensures that none of the calls in progress are interrupted.

Dynamic Channel Assignment (DCA) :

In dynamic channel assignment strategy channels are temporarily assigned for use in cells for the duration of the call. Each time a call attempt is made from a cell, the corresponding BS requests a channel from MSC. The MSC then allocates a channel to the requesting BS. After the call is over the channel is returned and kept in a central pool.

To avoid co-channel interference any channel that in use in one cell can only be reassigned simultaneously to another cell in the system if the distance between the two cells is larger than the minimum reuse distance.

When compared to FCA, DCA has reduced the likelihood of blocking and even increased the trunking capacity of the network, as all of the channels are available to all cells, i.e., good quality of service.

But this type of assignment strategy results in heavy load on switching center at heavy traffic condition.

**Solution : 4**

Given:

Total bandwidth = 30 MHz, Channel bandwidth = 25 kHz × 2 simplex channels = 50 kHz/duplex channel

Total available channels = 30,000/50 = 600 channels.

**(a)** For $N = 4$, total number of channels available per cell = 600/4 ≈ 150 channels.

**(b)** For $N = 7$, total number of channels available per cell = 600/7 ≈ 85 channels.

**(c)** For $N = 12$, total number of channels available per cell = 600/12 ≈ 50 channels.

A 1 MHz spectrum to control channels implies that there are 1000/50 = 20 control channels out of the 600 channels available. To evenly distribute the control and voice channels, simply allocate the same number of voice channels in each cell wherever possible.

**(a)** For $N = 4$, we can have 5 control channels and 145 voice channels per cell. In practice, however, each cell only needs a single control channel (the control channels have a greater reuse distance than the voice channels). Thus, 1 control channel and 145 voice channels would be assigned to each cell.

**(b)** Total number of voice channels for $N = 7$, (600 – 20)/7 = 82 voice channels are to be assigned to each cell approximately, 4 cells with 3 control channels and 82 voice channels, and 3 cells with 2 control channels are to be assigned along with 83 voice channels.

**(c)** For $N = 12$, we can have eight cells with two control channels and 48 voice channels, and four cells with one control channel and 49 voice channels each. In an actual system, each cell would have 1 control channel, 8 cells would have 48 voice channels, and 4 cells would have 49 voice channels.

■■■■

# 5 Network Basics and Models

## LEVEL 1 Objective Solutions

1. (d)
2. (b)
3. (a)
4. (a)
5. (d)
6. (a)
7. (a)
8. (d)
9. (b)
10. (c)
11. (b)
12. (c)

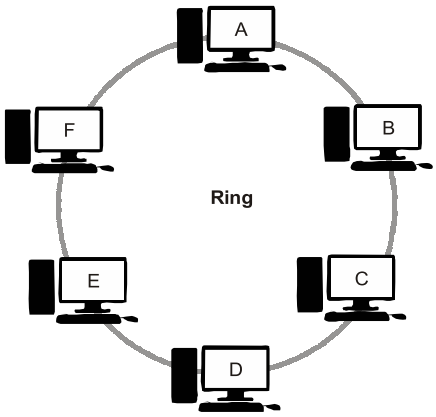
■■■■

## LEVEL 2 Conventional Solutions

**Solution : 1**

In ring topology, each computer is connected to the next computer, with the last one connected to the first. Rings are used in high performance network where large bandwidth is necessary.

- Computer is connected to next peer on the ring and each retransmits and receives from the previous computer.




- The message flow around the ring is in one direction. There is no termination of the ring because there is no end. Some rings do token passing. A short message called token, is passed around the computers in the ring from one to another. The computer, which transmits the data keeps the token with it otherwise passes the token to the computer, which is next to it in the ring. After transmitting the data, the token is sent to next computer in the ring. Thus, the token circulates until a station is ready to send and capture the token.

### Advantages of Ring Topology

(i) No computer can monopolise the network because every computer is given equal access to the token.

(ii) The sharing of the network allows the network to continue function in a useful manner.

### Disadvantages of Ring Topology

(i) Failure of one computer on the ring can affect the whole network.

(ii) Initial installation cost is high and hence not preferable for low density traffic.

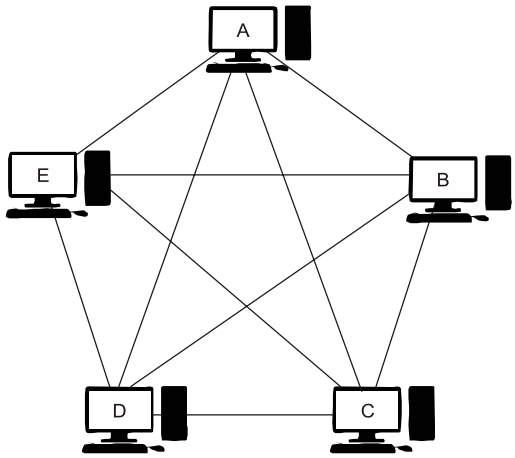
(iii) If any link breaks or if any repeater fails, then the entire network will be disabled.

(iv) To install a new repeater for supporting a new device, it is necessary to have the identification of two nearby network.

(v) Closed nature of ring topology makes it necessary to remove the circulating packets.

**Solution : 2**

In case of mesh topology, there is a dedicated point to point link from one device to another as shown below:




If there are N-devices, then a fully connected network will have $N(N-1)$ physical channels to link devices. The link between the devices in this case are dedicated link i.e. traffic is carried on it between two devices.

### Advantages of mesh topology

(i) The use of dedicated link guarantees that each connection can carry its own data load, thus eliminates traffic problem.

(ii) In case of mesh topology, failure of one node/computer does not bring down the entire network.

(iii) It provides security and privacy because every message is sent along dedicated line.

(iv) In case of failure, troubleshooting is easy.

### Disadvantages of mesh topology

(i) Installation and reconfiguration of mesh topology is difficult, since all node/computers are connected to each other node/computer.

(ii) Cabling cost is more

(iii) The hardware require to connect each link input/output and cable is expensive.

**Solution : 3**

| Sl. No. | Circuit switching | Packet switching |
|---|---|---|
| 1. | There is physical connection between transmitter and receiver. | No physical path is established between transmitter and receiver. |
| 2. | All the packets use same path. | Packet travels independently. |
| 3. | Needs an end to end path before the data transmission. | No requirement of end to end path before data transmission. |
| 4. | Reserves the entire bandwidth in advance. | Does not reserve the bandwidth in advance. |
| 5. | Charge is based on distance and time, but not on traffic. | Charge is based on both number of bytes and connect time. |
| 6. | Wastage of bandwidth. | No Wastage of bandwidth. |
| 7. | It cannot support store and forward transmission. | It supports store and forward transmission. |
| 8. | Not suitable for handling interactive traffic. | Suitable for handling interactive traffic. |

**Solution : 4**

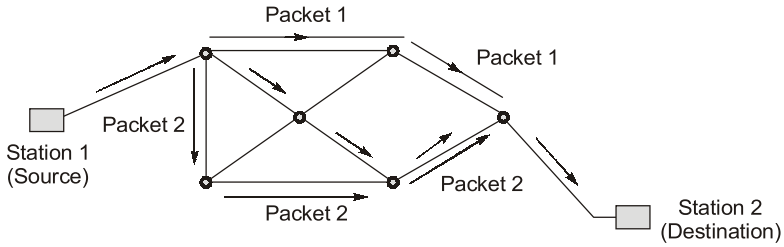
Packet Switching:

- Packet switching is often used in computer networks where individual users have need of the channel intermittently. While using the channel the application requires high bandwidth, but most of the time, each user does not require that channel at all. Such applications, characterized by a high peak to average requirement for capacity, are called **bursty** and are ideal for: packet switching.
- In packet switching, messages are broken into short blocks and interleaved with other messages. Thus, users queue for the channel and share it with one another efficiently. Data is sent in individual packets and each packet is forwarded from switch to switch, eventually reaching its destination. Each switching node has a small amount of buffer space to temporarily hold packets. If the outgoing line is busy, the packet stays in queue until the line becomes available. Packet switching handles burstly traffic well.
- Packet switching method uses two approaches :

  (i) Datagram packet switching (ii) Virtual circuit packet switching.

**1. Datagram Packet Switching**

- In **datagram** each packet is routed independently through the network. Header is attached to each packet. It provides the information required to route the packet to its destination. While routing the packet, the destination address in the header are examined to determine the next hop in the path to the destination. If the required line is busy then the packet is placed in the queue until the line becomes free. Packet shares the transmission line with other packets and then it delivers to the destination. Datagram approach is also called connectionless.
- Disadvantage of datagram approach is size of overhead is large and packet may not arrive in, the order at destination in which they were sent.
- Since each packet is routed independently, packets from the same source to the same destination may traverse through different paths. This is shown in figure below.




*Connectionless packet switching*

- The packets at station 2 or destination may arrive out of order, and resequencing may be required at the destination. At each node a routing table is maintained which specifies the next hops that is to be taken by packets for the given destination.

**2. Virtual Circuit Packet Switching**

- In virtual circuit packet switching a fixed path between a source and a destination is established prior to transfer of packets.
- Connection-oriented network is also known as virtual circuit, which is similar to telephone system. A route, which consists of a logical connection is first established between two users. The connection that is established is not a dedicated path between stations.

- The process is completed in three phases:
  (i) Establishment phase (ii) Data transfer phase (iii) Connection release phase.

**(i) Establishment phase**

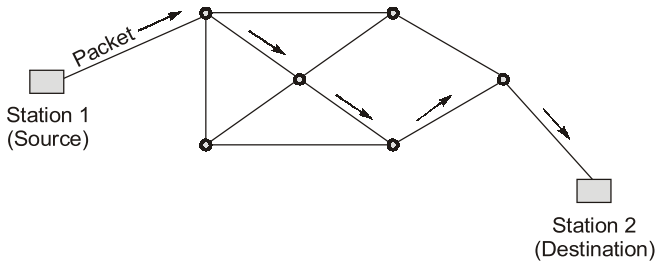
During setting up of logical connection, the two users not only agree to setup a connection between them but also decide upon the quality of service associated with the connection. After this the sequences of packetized information are transmitted bidirectionally between the nodes. The information is delivered to the receiver in the same order as transmitted by sender.

**(ii) Data transfer phase**

- During this phase it performs **flow control** and **error control services.**
- **The error control service** ensures correct sequencing of packets and correct arrival of packets.
- **Flow control service** ensures a slow receiver from being overwhelming with data from a faster transmitter.

**(iii) Connection release**

When the station wishes to close down the virtual circuit, one station can terminate the connection with a clear request packet. Figure shown below the virtual circuit packet switching.




*Virtual circuit packet switching*

**Solution : 5**

| Connection Oriented Network | Connection Less Network |
|---|---|
| 1. It provides dedicated link for entire message. | 1. It provides dedicated link for a packet. |
| 2. The entire message is transmitted over a single channel. | 2. Different packets are transmitted over different channels. |
| 3. No reordering of data is required at the receiver end. | 3. Reordering of data is required at receiver end. |
| 4. If the connection broke, entire message has to be sent again. | 4. If the connection is broke, particular packet is re-transmitted. |
| 5. It has simplex circuitry. | 5. It has complex circuitry. |
| 6. It relies heavily on error control coding for providing data protection. | 6. Here, no such equipment is required. |
| 7. Less overhead information is required for transmission. | 7. More overhead information is required for transmission. |

■■■■

# 6 Layers and Purpose

## LEVEL 1 Objective Solutions

1. (a)
2. (a)
3. (a)
4. (c)
5. (c)
6. (a)
7. (c)
8. (a)
9. (d)
10. (c)
11. (a)
12. (d)
13. (d)
14. (c)
15. (c)
16. (c)
17. (b)
18. (c)
19. (c)
20. (a)
21. (a)

## LEVEL 2 Conventional Solutions

**Solution : 1**

The sketch of OSI model is as under:

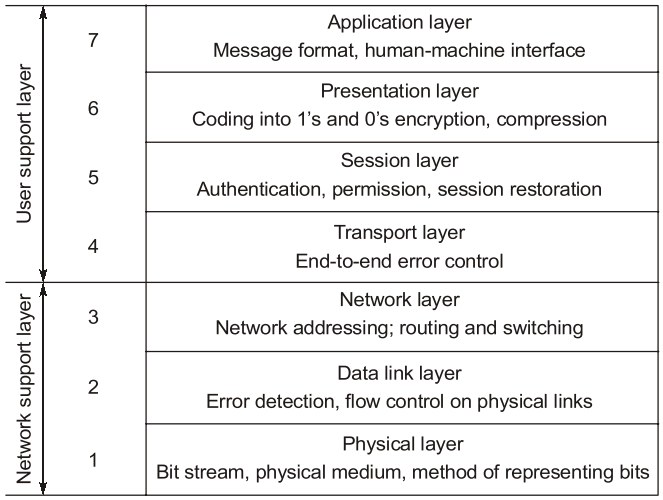



***Fig:** 7 layer OSI model*

**Significance of data link layer:** It provides error-free transfer of data frames from one link to another over physical layer, allowing layer above it to assume virtually error-free transmission over the link. To do this, data link layer provides:

1. Link establishment and termination.
2. Frame sequencing.
3. **Frame acknowledgment:** Provide/expect frame acknowledgment. Detects and recovers data from error that occur in the physical layer by retransmitting non-acknowledge frame and handling duplicate frame receipt.
4. Frame delimiting
5. Frame error checking

**Flow control and error control mechanism:** In case of data communication between a sender and receiver, it may so happen that rate at which data is transmitted by a fast sender is not acceptable by a slow receiver. In such a situation, there is a need of flow control so that a fast transmitter does not overwhelm a slow receiver.

These are basically two types of error, (a) damaged frame, (b) lost frame. The key functions for error control techniques are as follows:

- Error detection.
- Sending of positive acknowledgment by the receiver for no error.
- Sending for negative acknowledgment by the receiver for error.
- Setting the receiver for error times for lost frame.
- Numbering of frames.

**Solution : 2**

There are broadly five class of address used in classful IP addresses. They are:

- Class A networks:
  (a) First octet value ranges from 0 through 127.
  (b) First octet starts with bit 0.
  (c) Network mask is 8 bits, written /8 or 255.0.0.0.
  (d) 1.0.0.0 through 127.255.255.255 are class A networks with 16777214 hosts each.
  (e) Number of networks: $2^7 - 2$.
- Class B networks:
  (a) First octet values range from 128 through 191.
  (b) First octet starts with binary pattern 10.
  (c) Network mask is 16 bits, written /16 or 255.255.0.0.
  (d) 128.0.0.0 through 191.255.255.255 are class B networks, with 65534 hosts each.
  (e) Number of networks: $2^{14} - 2$.
- Class C networks:
  (a) First octet values range from 192 through 223.
  (b) First octet starts with binary pattern 110.
  (c) Network mask is 24 bits, written /24 or 255.255.255.0.
  (d) 192.0.0.0 through 223.255.255.255 are class C networks, with 254 hosts each.
  (e) Number of networks: $2^{21} - 2$.
- Class D addresses:
  (a) First octet values range from 224 through 239.
  (b) First octet starts with binary pattern 1110.
  (c) Class D addresses are multicast addresses.
- Class E addresses:
  (a) First octet starts with binary pattern of 1111 and ranges from 240-255.
  (b) Experimental class.
- Reserved addresses:
  (a) 0.0.0.0 is the default IP address, and it is used to specify a default route.
  (b) Addresses beginning with 127(127.x.y.z) are reserved for internal loopback addresses.
    - It is common to see 127.0.0.1 used as the internal loopback address on many devices.

**Solution : 3**

The data link layer concerned with reliable, error-free and efficient communication between adjacent machines in the network through the following functions:

**Data Framing**

The term "frame" refers to a small block of data used in a specific network. The data link layer groups raw data bits to/from the physical layer into discrete frames with error detection/correction code bits added.

Framing methods:

- Character count.
- Starting and ending characters, with character stuffing.
- Starting and ending flags with bit-stuffing.
- Physical layer coding violations.

**Error Detection/Correction**

Error detection:

- Include enough redundant information in each frame to allow the receiver to deduce that an error has occurred, and to request a retransmission.
- Uses error-detecting codes.

Error correction:

- Include redundant information in the transmitted frame to enable the receiver not only to deduce that an error has occurred but also correct the error.
- Uses error-correcting codes.

**Flow Control**

There are several protocols to control the rate at which sender transmits frames and at a rate acceptable to the receiver, and the ability to retransmit lost or damaged frames. This ensures that slow receivers are not swamped by fast senders and further aids error detection/correction.

Several flow control protocol exist, but all essentially require a form of feedback to make the sender aware of whether the receiver can keep up.

Stop-and-wait protocols:

- A positive acknowledgment frame is send by the receiver to indicate that the frame has been received and to indicate being ready for the next frame.
- Positive Acknowledgment with Retransmission (PAR); uses timeouts

Sliding window protocols:

- Data frames and acknowledgment frames are mixed in both directions.
- Frames sent contain sequence numbers
- Timeouts used to initiate retransmission of lost frames.

**Solution : 4**

1. Reliable message delivery:
   (*i*) Byte stream broken into small chunks called segments.
   (*ii*) Receiver sends Ack's for segments.
   (*iii*) TCP maintains a timer. If ACK is not received in time then it is retransmitted.
2. Byte stream service:
   (*i*) To the lower layers, TCP handles data in blocks, the Segments.
   (*ii*) To the higher layers TCP handles data as a sequence of bytes and does not identify boundaries between bytes. So higher layers do not know about the beginning and end of segments.
   (*iii*) If a sender process sends a stream of bytes, the receiver process will be getting exactly the same stream of bytes.
3. Synchronization between sender and receiver through flow control:
   (*i*) Flow control is also sometimes necessary between two users for speed matching, that is, for ensuring that a fast transmitter does not overwhelm a slow receiver with more packets than the latter can handle.
   (*ii*) TCP allows the receiver to apply flow control to the sender and Prevents sender from overrunning the receiver.

4. Support for multiple application processes on each host:
   (*i*) Unique port assigned for each process both at sender and receiver (the range of port numbers is 0 to 65535).
   (*ii*) Ports can provide multiple endpoints on a single node.

**Solution : 5**

Application layer **uses protocols that are implemented within applications and services.**

Applications provide people with a way to create messages and application layer services establish an interface to the network, protocols provide the rules and formats that govern how data is treated.

All three components may be used by a single executable program and may even use the same name.The Application layer, protocols specify what messages are exchanged between the source and destination hosts, the syntax of the control commands, the type and format of the data being transmitted, and the appropriate methods for error notification and recovery.

### Application Layer Protocol Functions

Application layer ISO OSI protocols are used by both the source and destination devices during a communication session.

Protocols specify how data inside the messages is structured and the types of messages that are sent between source and destination. Protocols establish consistent rules for exchanging data between applications and services loaded on the participating devices.

In order for the communications to be successful, the application layer protocols implemented on the source and destination host must match. The messages exchanged can be requests for services, acknowledgments, data messages, status messages, or error messages. Protocols also define message dialogues, ensuring that a message being sent is met by the expected response and the correct services are invoked when data transfer occurs.

Applications and services may also use multiple protocols in the course of a single conversation. One protocol may specify how to establish the network connection and another describe the process for the data transfer when the message is passed to the next lower layer. Application layer protocols define:

1. Types of messages
2. Syntax of messages
3. Meaning of any informational fields
4. How messages are sent and the expected response
5. Interaction with next lower layer

**Solution : 6**

TCP/IP Reference Model:

- **TCP/IP Protocol** is a name of two most important protocols: **Transmission Control Protocol (TCP) and Internet Protocol (IP)**. The main goal of TCP/IP model was to build an interconnection of network, referred as internet, that provides universal communication over heterogenous physical networks.
- Like most networking software, TCP/IP is modeled in layers. This layered representation leads to the term **protocol stack**, which refers to stack of layers of protocols. The various layers in TCP/IP can be represented as

| Application Layer |
|---|
| Transport Layer |
| Internet / Network Layer |
| Host to Network / Link Layer |

*Various layer of TCP/IP reference model*

1. **Application Layer:** An application are user process as cooperating with another process usually on a different host. The interface between application and transport layers is defined by port numbers.
2. **Transport Layer:** This layer provides end to end data transfer by delivering data from an application to its remote peer. Multiple applications can be supported simultaneously. The **most used transport layer protocol is Transmission Control Protocol (TCP),** which provides connection oriented reliable data delivery, duplicate data suppression, congestion control, error control and flow control.

   Another transport layer protocol is the **User Datagram Protocol (UDP)**. It provides connectionless, unreliable best effort service.
3. **Internet Layer:** This layer is also known as **network layer**. It provides "Virtual Network" an image of the network. Internet protocol is defined at internet layer.

   IP does not provide reliability, flow control or error recovery. These functions must be provided by higher layer. IP provides a routing function that attempts to deliver transmitted message to their destination.
4. **Host to Network Layer:** This is the lowest layer in the TCP/IP reference model. The host has to connect to the network using some protocol, so that it can send the IP Packets over it. This protocol varies from host to host and network to network.

■■■■

# 7 Security and Routing

## LEVEL 1 Objective Solutions

1. (c)
2. (c)
3. (d)
4. (c)
5. (d)
6. (d)
7. (b)
8. (b)
9. (b)
10. (d)
11. (26)

## LEVEL 2 Conventional Solutions

**Solution : 1**

Network layer is connected with getting data packets from the source way to the destination. The packets may require to make many hops at the intermediate router while reaching destination. This is the lowest layer that deals with end to end transmission. In order to achieve its goals, network layer must knows about the topology of the network. It must also take care to choose routes to avoid overloading of the lines while leaving other idle. The function of the layer includes:

(i) Routing of packets through network.

(ii) Flow control or congestion control of packets. It is also called traffic control.

(i) Routing of packets is a process of transferring packets received from data link layer of source network to data link layer of the correct destination network. Involves decision making at each intermediate node on where to send the packet next so that it eventually reaches its destination.

These are two parts of routing problems:

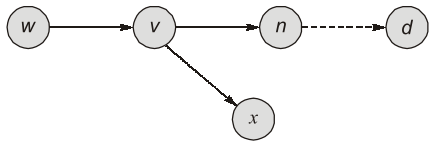
1. How to pass a packet from an input interface to the output interface of a router i.e. forwarding of packets.
2. How to calculate the most efficient route Packet forwarding is done differently in datagram and virtual circuit packet network. The calculation of route is done in similar fashion.

1. **Packet forwarding:**

**(a) Through datagram:** In datagram network, each packet carrier the full destination address. Each router maintains a routing table which has one row for each possible destination address.

Routing table of node V

| To | Via (next hop) |
|---|---|
| | |
| ⋮ | |
| *d* | *n* |
| | |




When a packet with destination node arrives at an incoming link:

- The router looks up the routing table.
- The routing table look up yields the address of the next node (next hop).
- The packet is transmitted onto the outgoing link that goes to the next hop.

Advantage of datagram is the router doesn't need to know about end-to-end flow but in the process size of routing table can grow very large.

**(b) Through virtual circuits:** In VC networks, the route is setup in the connection establishment phase. During the setup, each router assigns a VC number (VC #) to virtual circuit. The VC # can be different for each hop and it is written in the packet headers. When a packet $VC_{in}$ in header arrives from router.

- The router looks up the routing table for an entry.
- The routing table look up yields.
- The router update the header.

Its advantage is that routing table is small but changing the route is complicated.

2. **How to calculate most efficient routing:** For this we have routing algorithms. Routing algorithms for both datagram and virtual circuit should satisfy the following:
   - Correctness
   - Simplicity
   - Robustness
   - Stability
   - Optimality
   - Fairness

   Elements of routing algorithms:
   - Optimization criteria covers numbers of hops, cost, time delay and throughput.
   - **Decision time involves time:** It is taken once per session in VC and one per packet in datagram.
   - Decision place may be:
     (a) At each node
     (b) Central node
     (c) Sending node

Classification of routing algorithms:

1. **Adaptive routing algorithm:** These algorithm change their routing decisions to reflect changes in topology and in traffic as well. These get their routing information from adjacent routers or from all routers. This can be further classified as
   **(a) Centralised:** Some central node gets entire information.
   **(b) Isolated:** Node decides the routing within seeking information from other nodes. Some the examples are:
   - **Hot potato:** Tries to get rid of it as fast as it can.
   - **Backward learning:** Routing table at each node gets modified by information from incoming packets.

   **(c) Distributed:** Receives information from neighbouring nodes and then decides about which way to send packet.
2. **Non-adaptive routing algorithms:** In this route is computed in advance, off-line and downloaded to the routers when network is booted.
   **(a) Flooding:** Every incoming packet is sent to every outgoing line except the one from which it has arrived. In this packet may go in loop.
   - **Sequence numbers:** Packet is forwarded based on predecided sequence number.
   - **Hop count:** Every packet has a hop count associated with it. When hop count become zero the packet is dropped.
   - **Spanning tree:** Packet is sent only on those links that lead to the destination by constructing a spanning tree routed at the source.

   **(b) Random walk:** Packet is forwarded to neighbour randomly. This algorithm is highly robust.
3. **Delta routing:** It is hybrid of centralised and isolated algorithm.
4. **Multipath routing:** It has been assumed that there is a single best path between any pair of nodes and that all traffic between them should use it.
5. **Hierarchical routing:** Nodes are divided based on hierarchy. A particular node can communicate with node at the same hierarchial levels or the nodes at lower level and directly under it.

(ii) Flow control at network layers attempts to control the numbers of packets that are in network at a time. It prevents the network from becoming a bottleneck.

Techniques of Flow control:

- Packet discarding
- Choke packets
- Sliding window flow control
- Leaky bucket
- **Preallocation of buffers:** Reserve sufficient buffer at each node for each virtual circuit. If sufficient buffer not available, reject the virtual circuit.
- **Packet discarding:** Drop packets if they arrive at a node with almost full buffer. Heuristics should be used to decide when to drop a packet.
- **Choke packets:** If a packet enters a node and queue length of the outgoing buffer exceeds a threshold, the node sends a choke packet to the source node. If source node receiver choke packet it reduces the traffic by certain amount.
- **Sliding window flow control:** Can be used at the hop-by-hop and the entry-to-exit level.
- **Leaky bucket:** Used to control the maximum rate at which sender can transmit traffic.

**Solution : 2**

The most popular public-key algorithm is the RSA (named after their inventors Rivest, Shamir and Adleman). Key features of the RSA algorithm are given below:

- Public key algorithm that performs encryption as well as decryption based on number theory.
- Variable key length; long for enhanced security and short for efficiency (typical 512 bytes).
- Variable block size, smaller than the key length.
- The private key is a pair of numbers ($d$, $n$) and the public key is also a pair of numbers ($e$, $n$).
- Choose two large primes p and q (typically around 256 bits).
- Compute $n = p \times q$ and $z = (p - 1) \times (q - 1)$.
- Choose a number d relatively prime to $z$.
- Find e such that $e \times d \bmod (p - 1) \times (q - 1) = 1$.
- For encryption: $C = P^e \pmod n$ For decryption: $P = C^d \pmod n$.

**Solution : 3**

### Features

The successor of IPv4 is not designed to be backward compatible. Trying to keep the basic functionalities of IP addressing, IPv6 is redesigned entirely. It offers the following features:

#### Larger Address Space

In contrast to IPv4, IPv6 uses 4 times more bits to address a device on the Internet i.e., 128 bits IP address. Hence number of address = $2^{128}$.

#### End-to-end Connectivity

Every system now has unique IP address and can traverse through the Internet without using Network Address Translation (NAT) or other translating components. After IPv6 is fully implemented, every host can directly reach other hosts on the Internet, with some limitations involved like Firewall, organization policies, etc.

#### Auto-configuration

IPv6 supports both stateful and stateless auto-configuration mode of its host devices. So, the absence of a DHCP server does not create trouble.

**Faster Forwarding/Routing**

Simplified header puts all unnecessary information to extention header. The information contained in the first part of the header is adequate for a Router to take routing decisions, thus making routing decision very fast.

**IPSec**

IPv6 have IPSec security i.e., inbuilt security making it more secure than IPv4.

**No Broadcast**

Though Ethernet/Token Ring are considered as broadcast network because they support Broadcasting, IPv6 does not have any broadcast support anymore. It uses multicast to communicate with multiple hosts.

**Anycast Support**

This is another characteristic of IPv6. IPv6 has introduced Anycast mode of packet routing. In this mode, multiple interfaces over the Internet are assigned same Anycast IP address. Routers, while routing, send the packet to the nearest destination.

**Mobility**

IPv6 was designed keeping mobility in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with the same IP address. The mobility feature of IPv6 takes advantage of auto IP configuration and Extension headers.

**Enhanced Priority Support**

IPv4 used 6 bits DSCP (Differential Service Code Point) and 2 bits ECN (Explicit Congestion Notification) to provide Quality of Service but it could only be used if the end-to-end devices support it, that is, the source and destination device and underlying network must support it whereas, in IPv6, Traffic class and Flow label are used to tell the underlying routers how to efficiently process the packet and route it.

**Smooth Transition**

Large IP address scheme in IPv6 enables to allocate devices with globally unique IP addresses. This mechanism saves IP addresses and NAT is not required. So devices can send/receive data among each other, for example, VoIP and/or any streaming media can be used much efficiently.

Other fact is, the header is less loaded, so routers can take forwarding decisions and forward them as quickly as they arrive.

■■■■