BCA-1.13

1. Differentiate between OSI and TCP reference model in terms of layers. Functionality of each layer and important protocols at each layer.

Answer:

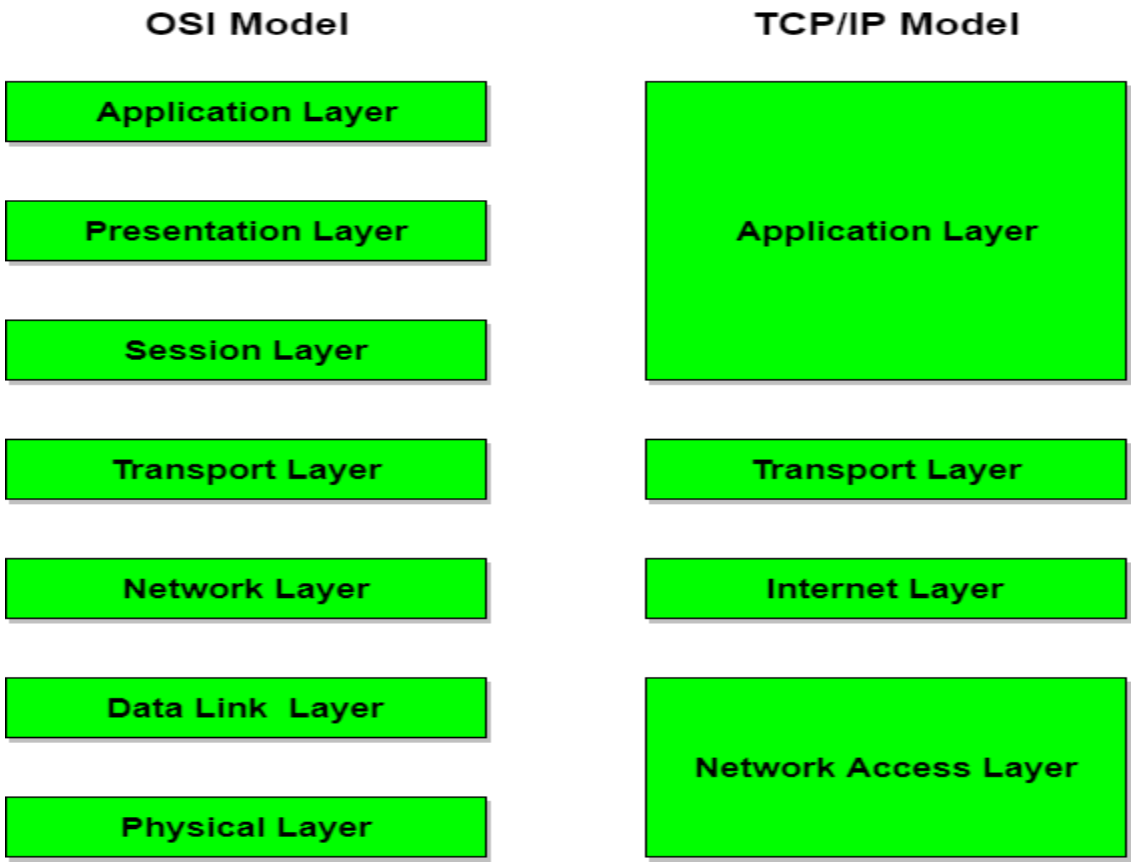
Difference between OSI and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model, with diagrammatic comparison below.

OSI(Open System Interconnection)	**TCP/IP(Transmission Control Protocol / Internet Protocol)**
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both	8. The Network layer in TCP/IP model provides

connection oriented and connectionless service.	connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers

Diagrammatic Comparison between OSI Reference Model and TCP/IP Reference Model



Here is a brief description of each of the layers of the OSI model.

- **Physical** – defines how to move bits from one device to another. It details how cables, connectors and network interface cards are supposed to work and how to send and receive bits.
- **Data Link** – encapsulates a packet in a frame. A frame contains a header and a trailer that enable devices to communicate. A header (most commonly) contains a source and destination MAC address. A trailer contains the Frame Check Sequence field, which is used to detect transmission errors. The data link layer has two sublayers:

    1. Logical Link Control – used for flow control and error detection.
    2. Media Access Control – used for hardware addressing and for controlling the access method.

- **Network** – defines device addressing, routing, and path determination. Device (logical) addressing is used to identify a host on a network (e.g. by its IP address).
- **Transport** – segments big chunks of data received from the upper layer protocols. Establishes and terminates connections between two computers. Used for flow control and data recovery.
- **Session** – defines how to establish and terminate a session between the two systems.
- **Presentation** – defines data formats. Compression and encryption are defined at this layer.
- **Application** – this layer is the closest to the user. It enables network applications to communicate with other network applications.

Here is a brief description of each layer:

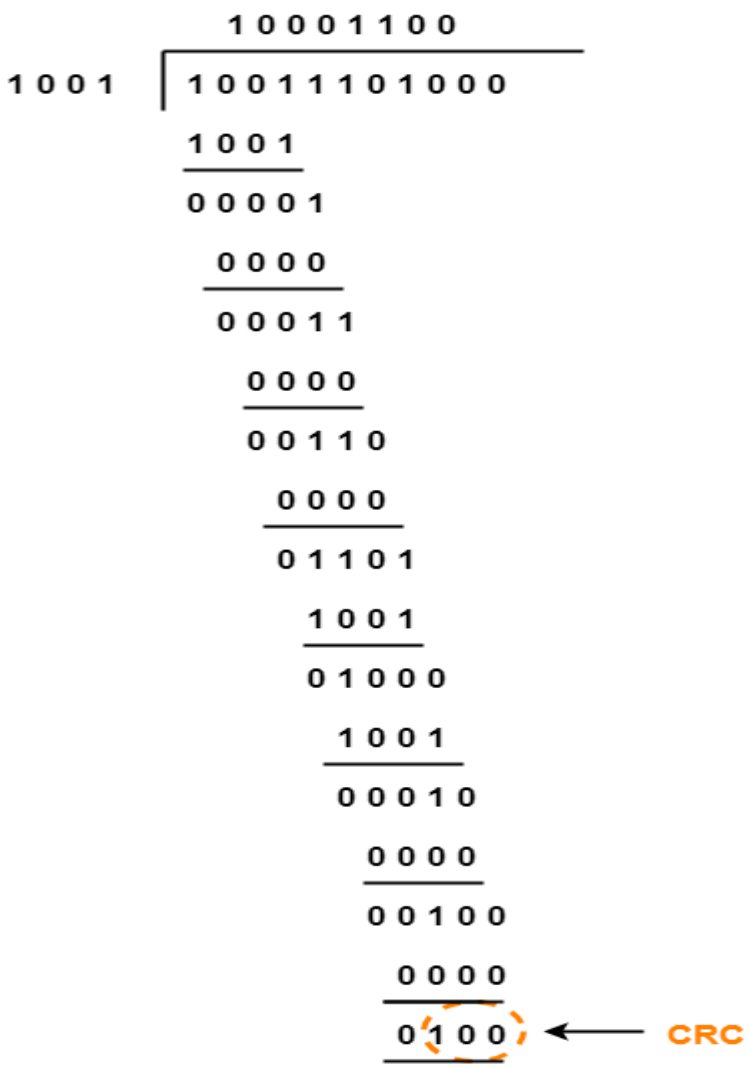
- **Link** – defines the protocols and hardware required to deliver data across a physical network.
- **Internet** – defines the protocols for the logical transmission of packets over the network.
- **Transport** – defines protocols for setting up the level of transmission service for applications. This layer is responsible for reliable transmission of data and the error-free delivery of packets.
- **Application** – defines protocols for node-to-node application communication and provide services to the application software running on a computer.

2. Assume message M: 1010101010 bits and generator G: 10001 bits. Explain how CRC is used for error detection using above message bits and generator bits.

Answer:

- The generator polynomial $G(x) = x^3 + 1$ is encoded as 1001.
- Clearly, the generator polynomial consists of 4 bits.
- So, a string of 3 zeroes is appended to the bit stream to be transmitted.
- The resulting bit stream is 10011101**000**.

Now, the binary division is performed as-



From here, CRC = 100.

Now,

- The code word to be transmitted is obtained by replacing the last 3 zeroes of 10011101**000** with the CRC.
- Thus, the code word transmitted to the receiver = 10011101**100**.

3. Explain the working of Link State Routing Algorithm using an example.

Answer:

Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

The three keys to understand the Link State Routing algorithm:

- **Knowledge about the neighborhood:** Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.
- **Flooding:** Each router sends the information to every other router on the internetwork except its neighbors. This process is known as Flooding. Every router that receives the packet sends the copies to all its neighbors. Finally, each and every router receives a copy of the same information.
- **Information sharing:** A router sends the information to every other router only when the change occurs in the information.

Link State Routing has two phases:

Reliable Flooding

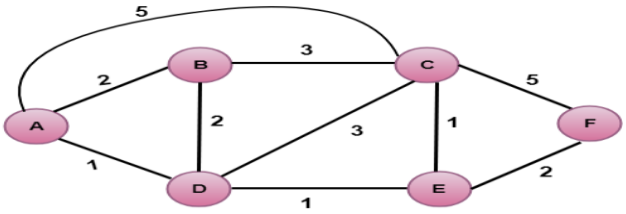
- **Initial state:** Each node knows the cost of its neighbors.
- **Final state:** Each node knows the entire graph.

Route Calculation

Each node uses Dijkstra's algorithm on the graph to calculate the optimal routes to all nodes.

- The Link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.
- The Dijkstra's algorithm is an iterative, and it has the property that after k^{th} iteration of the algorithm, the least cost paths are well known for k destination nodes.

Let's understand through an example:



In the above figure, source vertex is A.

Step 1:

The first step is an initialization step. The currently known least cost path from A to its directly attached neighbors, B, C, D are 2,5,1 respectively. The cost from A to B is set to 2, from A to D is set to 1 and from A to C is set to 5. The cost from A to E and F are set to infinity as they are not directly linked to A.

Step 2:

In the above table, we observe that vertex D contains the least cost path in step 1. Therefore, it is added in N. Now, we need to determine a least-cost path through D vertex.

a) Calculating shortest path from A to B

1. v = B, w = D
2. D(B) = min(D(B) , D(D) + c(D,B))
3. = min(2, 1+2)>
4. = min(2, 3)
5. The minimum value is 2. Therefore, the currently shortest path from A to B is 2.

b) Calculating shortest path from A to C

1. v = C, w = D
2. D(B) = min(D(C) , D(D) + c(D,C))
3. = min(5, 1+3)
4. = min(5, 4)
5. The minimum value is 4. Therefore, the currently shortest path from A to C is 4.</p>

c) Calculating shortest path from A to E

1. v = E, w = D
2. D(B) = min(D(E) , D(D) + c(D,E))
3. = min(∞, 1+1)
4. = min(∞, 2)
5. The minimum value is 2. Therefore, the currently shortest path from A to E is 2.

Step 3:

In the above table, we observe that both E and B have the least cost path in step 2. Let's consider the E vertex. Now, we determine the least cost path of remaining vertices through E.

a) Calculating the shortest path from A to B.

1. v = B, w = E
2. D(B) = min(D(B) , D(E) + c(E,B))
3. = min(2 , 2+ ∞)
4. = min(2, ∞)
5. The minimum value is 2. Therefore, the currently shortest path from A to B is 2.

b) Calculating the shortest path from A to C.

1. v = C, w = E
2. D(B) = min(D(C) , D(E) + c(E,C))
3. = min(4 , 2+1)
4. = min(4,3)
5. The minimum value is 3. Therefore, the currently shortest path from A to C is 3.

c) Calculating the shortest path from A to F.

1. v = F, w = E
2. D(B) = min(D(F) , D(E) + c(E,F))
3. = min(∞ , 2+2)
4. = min(∞ ,4)
5. The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

4. Explain the working of Distance Vector Routing using an example.

Answer:

A **distance-vector routing (DVR)** protocol requires that a router inform its neighbors of topology changes periodically. Historically known as the old ARPANET routing algorithm (or known as Bellman-Ford algorithm).
Bellman Ford Basics – Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes. Distances,based on a chosen metric, are computed using information from the neighbors' distance vectors.

Distance Vector Algorithm –

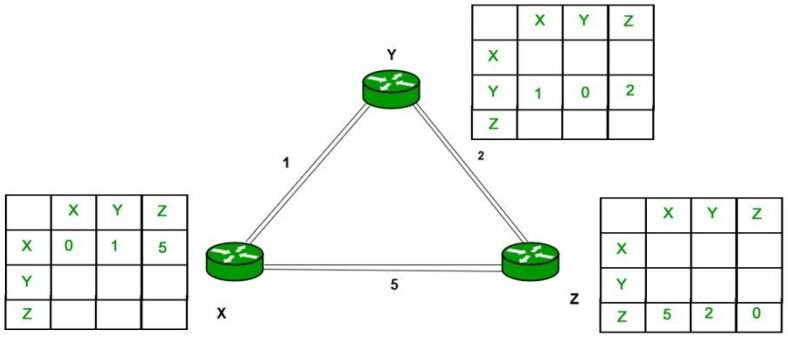
1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
   - It receives a distance vector from a neighbor containing different information than before.
   - It discovers that a link to a neighbor has gone down.

Note –

- From time-to-time, each node sends its own distance vector estimate to neighbors.

- When a node x receives new DV estimate from any neighbor v, it saves v's distance vector and it updates its own DV using B-F equation:
- `Dx(y) = min { C(x,v) + Dv(y), Dx(y) } for each node y ∈ N`

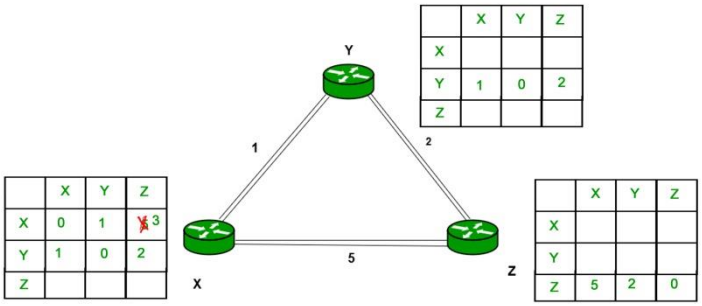
Example – Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.



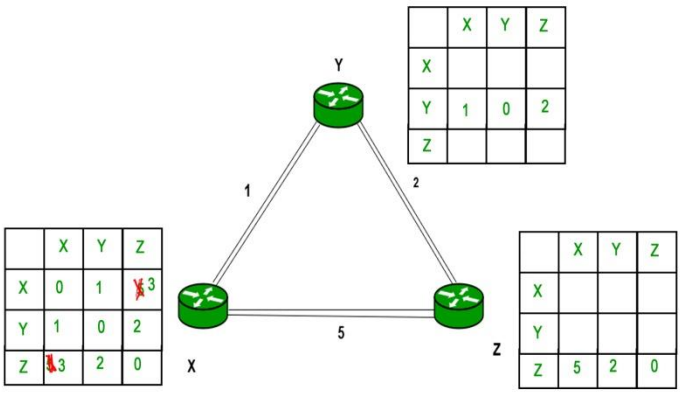
Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.

`Dx(y) = min { C(x,v) + Dv(y)} for each node y ∈ N`

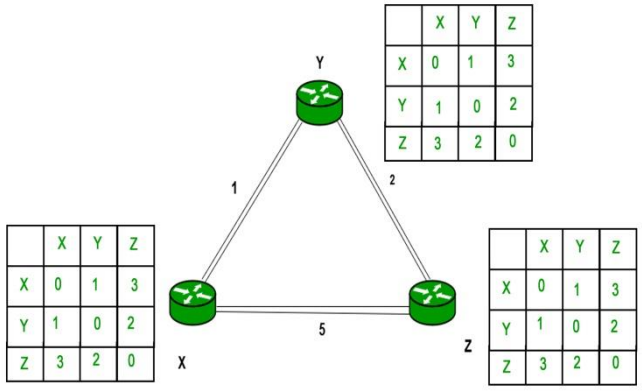
As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.



Similarly for Z also –



Finally the routing table for all –



4. Differentiate between mutlicast addressing and Unicast addressing.

Answer:

Unicast - Unicast is the term used to describe communication where a piece of information is sent from one point to another point. In this case there is just one sender, and one receiver.

Unicast transmission, in which a packet is sent from a single source to a specified destination, is still the predominant form of transmission on LANs and within the Internet. All LANs (e.g. Ethernet) and IP networks support the unicast transfer mode, and most users are familiar with the standard unicast applications (e.g. http, smtp, ftp and telnet) which employ the TCP transport protocol.

Multicast - Multicast is the term used to describe communication where a piece of information is sent from one or more points to a set of other points. In this case there is may be one or more senders, and the information is distributed to a set of receivers (their may be no receivers, or any other number of receivers).

One example of an application which may use multicast is a video server sending out networked TV channels. Simultaneous delivery of high quality video to each of a large number of delivery platforms will exhaust the capability of even a high bandwidth network with a powerful video clip server. This poses a major salability issue for applications which required sustained high bandwidth. One way to significantly ease scaling to larger groups of clients is to employ multicast networking.

Multicasting is the networking technique of delivering the same packet simultaneously to a group of clients. IP multicast provides dynamic many-to-many connectivity between a set of senders (at least 1) and a group of receivers. The format of IP multicast packets is identical to that of unicast packets and is distinguished only by the use of a special class of destination address (class D IPv4 address) which denotes a specific multicast group. Since TCP supports only the unicast mode, multicast applications must use the UDP transport protocol.

Unlike broadcast transmission (which is used on some local area networks), multicast clients receive a stream of packets only if they have previously elect to do so (by joining the specific multicast group address). Membership of a group is dynamic and controlled by the receivers (in turn informed by the local client applications). The routers in a multicast network learn which sub-networks have active clients for each multicast group and attempt to minimise the transmission of packets across parts of the network for which there are no active clients.

The multicast mode is useful if a group of clients require a common set of data at the same time, or when the clients are able to receive and store (cache) common data until needed. Where there is a common need for the same data required by a group of clients, multicast transmission may provide significant bandwidth savings (up to 1/N of the bandwidth compared to N separate unicast clients).

The majority of installed LANs (e.g. Ethernet) are able to support the multicast transmission mode. Shared LANs (using hubs/repeaters) inherently support multicast, since all packets reach all network interface cards connected to the LAN. The earliest LAN network interface cards had no specific support for multicast and introduced a big performance penalty by forcing the adaptor to receive all packets (promiscuous mode) and perform software filtering to remove all unwanted packets. Most modern network interface cards implement a set of multicast filters, relieving the host of the burden of performing excessive software filtering.

6. What do we mean by class addressing and class-less addressing? Give the range of IP addresses used in different classes in class addressing mode.

Answer:

Address Classes

In the original Internet routing scheme developed in the 1970s, sites were assigned addresses from one of three *classes*: Class A, Class B and Class C. The address classes differ in size and number. Class A addresses are the largest, but there are few of them. Class Cs are the smallest, but they are numerous. Classes D and E are also defined, but not used in normal operation.

To say that class-based IP addressing in still used would be true only in the loosest sense. Many addressing designs are still class-based, but an increasing number can only be explained using the more general concept of CIDR, which is backwards compatible with address classes.

Suffice it to say that at one point in time, you could request the Internet NIC to assign you a class A, B or C address. To get the larger class B addresses, you might have to supply some justification, but only the class A was really tough to get. In any case, NIC would set the network bits, or n-bits, to some unique value and inform the local network engineer. It would then be up to the engineer to assign each of his hosts an IP address starting with the assigned n-bits, followed by host bits, or h-bits, to make the address unique.

Internet routing used to work like this: A router receiving an IP packet extracted its Destination Address, which was classified (literally) by examining its first one to four bits. Once the address's class had been determined, it was broken down into network and host bits. Routers ignored the host bits, and only needed to match the network bits to find a route to the network. Once a packet reached its target network, its host field was examined for final delivery.

Summary of IP Address Classes

Class A - `0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh`

- First bit 0; 7 network bits; 24 host bits
- Initial byte: 0 - 127
- 126 Class As exist (0 and 127 are reserved)
- 16,777,214 hosts on each Class A

Class B - `10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh`

- First two bits 10; 14 network bits; 16 host bits
- Initial byte: 128 - 191
- 16,384 Class Bs exist
- 65,532 hosts on each Class B

Class C - `110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh`

- First three bits 110; 21 network bits; 8 host bits
- Initial byte: 192 - 223
- 2,097,152 Class Cs exist
- 254 hosts on each Class C

Class D - `1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm`

- First four bits 1110; 28 multicast address bits
- Initial byte: 224 - 247
- Class Ds are multicast addresses - see RFC 1112

Class E - `1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr`

- First four bits 1111; 28 reserved address bits
- Initial byte: 248 - 255
- Reserved for experimental use

7. Write short notes on the following:
a. Hub b. Repeater

Answer:

a.Hub - There are two primary types of hubs in the computing world: 1) network hubs and 2) USB hubs.

1. Network hub

A network hub is a device that allows multiple computers to communicate with each other over a network. It has several Ethernet ports that are used to connect two or more network devices together. Each computer or device connected to the hub can communicate with any other device connected to one of the hub's Ethernet ports.
Hubs are similar to switches, but are not as "smart." While switches send incoming data to a specific port, hubs broadcast all incoming data to all active ports. For example, if five devices are connected to an 8-port hub, all data received by the hub is relayed to the five active ports. While this ensures the data gets to the right port, it also leads to inefficient use of the network bandwidth. For this reason, switches are much more commonly used than hubs.

2. USB hub

A USB hub is a device that allows multiple peripherals to connect through a single USB port. It is designed to increase the number of USB devices you can connect to a computer. For example, if your computer has two USB ports, but you want to connect five USB devices, you can connect a 4-port USB hub to one of the ports. The hub will create four ports out of one, giving you five total ports. The USB interface allows you to daisy chain USB hubs together and connect up to 127 devices to a single computer.
Some USB hubs include a power supply, while others do not. If you're connecting basic devices like a mouse, keyboard, and USB flash drive, an unpowered or "passive" USB hub should work fine. However, some peripherals, like external hard drives and backlit keyboards, require additional

electrical power. In order for these types of devices to function through a USB hub, you may need use a powered or "active" hub that provides 5 volts of power to connected devices.

b. Repeater –

A repeater is an electronic device that relays a transmitted signal. It receives a signal on a specific frequency, then amplifies and rebroadcasts it. By amplifying the signal, a repeater increases the transmission range of the original signal.

Repeaters have many applications, but in computing they are most commonly used in wireless networks. For example, a Wi-Fi network in a large home may benefit from using one or more repeaters to relay the signal to different areas of the house. Homes that have brick walls or cement floors may also benefit from having a repeater relay the signal around the obstacle. Businesses often use a series of repeaters to create a single wireless network within a large building.

While repeaters all serve the same purpose, they come in many forms. Some wireless devices, often called "range extenders" are designed to be used specifically as repeaters. Other devices, such as hubs, switches, and routers can all be configured as repeaters using a software utility or web interface that controls the wireless device.

NOTE: Since repeaters only relay an incoming signal, using a router as a repeater does not make use of its signal routing capability. Therefore, it make more sense to use a range extender as a repeater if possible.