Q 1. What are roles of Data Link Layer

Ans:

Link layer makes datagram ready for transmission for a specific media. It receives datagram from Network layer. It produces frame for the specific media type. It decide when to transmit when multiple devices are sharing the media. It instruct Physical layer when to transmit. When it receives frames from physical layer destined for the specific device and provides datagram to network layer

Q2 . What are the services provided by the data link layer ?

Ans:

Data link layer provides the following services

Framing: Format is different for medium

Link access: Depends on the medium and network topology

Reliable delivery: May be offered on error prone links

Error detection and correction: Discard corrupt frames

Q3 . Why implementation of data link layer involves both software and hardware ?

Ans:

The software components of the link layer implement higher-level link layer functionality such as assembling link-layer information and activating the controller hardware.

On the receiving side, link-layer software responds to controller interrupts (e.g., due to the receipt of one or more frames), handling error conditions and passing a datagram up to the network layer.

Thus, the link layer is a combination of hardware and software—the place in the protocol stack where software meets hardware

Q4. Why Error detection and correction is important ?

Ans:

Complete error free link is not possible. Error can occur to any link anytime. Probability may be different for different kind of links. For wireless link probability is much high than other wired and optical links. There are few techniques that can be used to detect and, in some cases, correct such bit errors. If packet error detected it can be retrieved in Linked layer itself or can be stopped to flow to upper layers

Q5 . Show that two-dimensional parity checks can correct and detect a single bit error. Show (give an example of) a double-bit error that can be detected but not corrected.

Ans. Suppose following is the two dimensional data

1	0	1	0	1	1
1	1	1	1	0	0
0	1	1	1	0	1
0	0	1	0	1	0

Suppose 2nd row 3rd column data get corrupted and becomes 0.

1	0	1	0	1	1
1	1	0	1	0	0
0	1	1	1	0	1
0	0	1	0	1	0

When receiver receives this data it will try to check parity. It will find that second row parity and third column parity will not match. If there is only one error in data block then it is obvious that the location of the data that got corrupted is at 2nd row and 3rd column. As data is binary and know to be corrupted it can be corrected as 1.

Suppose two bits error occurs in data. Along with previous one row 3 and column 4 also get corrupted.

Parity of 2 rows and 2 columns will be violated. So there will be 2 possibilities of error.

i) Row 2 column 3 and row 3 column 4
ii) Row 2 column 4 and row 3 column 3

So we cannot tell deterministically which one actually occurred and cannot correct the error. But as we see violation of parity check we can say that there is some error in data which means error detection is possible.

Q6. What is multiple link access protocol and why is it required ?

Ans:

How to coordinate the access of multiple sending and receiving nodes to a shared broadcast channel is the multiple access problem. When more than two nodes transmit frames at the same time, the transmitted frames collide at all of the receivers. Clearly, if many nodes want to transmit frames frequently, and much of the bandwidth of the broadcast channel will be wasted. In order to ensure that the broadcast channel performs useful work when multiple nodes are active, we need multiple access protocols

Q7 . What are different types of guaranteed access methods ?

Ans:

Different types of guaranteed access methods are :

Time division multiplexing

Frequency division multiplexing

Code division multiplexing

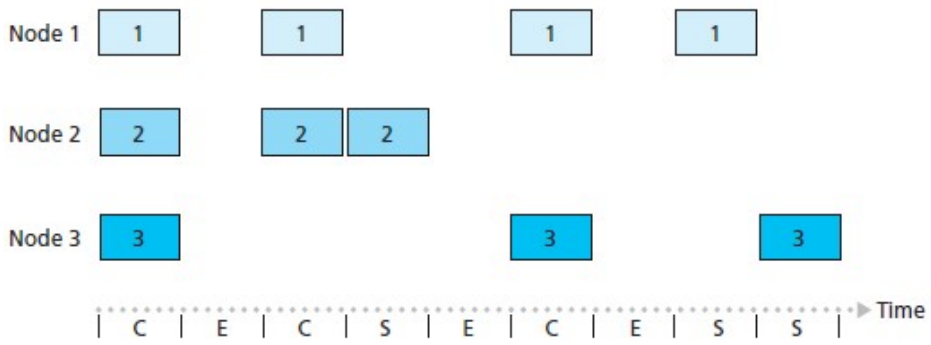
Space division multiplexing

Orthogonal frequency division multiplexing

Polling methods

Q8 . Explain slotted ALOHA protocol

Ans:



Instead of transmitting packet at any time, time is divided into equal length slots and any sers can transmit at the start of a slot. Slot length is decided by transmission delay. So packets will be successful in transmission of will collide completely. If collision occurs then each node decide whether to retransmit or not in the subsequent solt with probability p.

Q9 . Explain CSMA/CD.

Ans:

All nodes listen before talking. It increases efficiency than ALOHA. A sender listens to channel for busy/idle status. Node sends the frame if channel is sensed idle. If collisions are heard during transmission, then the transmission is aborted. A retransmission occurs after channel is sensed idle and a random waiting time elapsed. The waiting time is chosen by first picking a random value (say x) from $\{0,...,2^n-1\}$ and then multiplying the random number x with W. Here n is the collision round.

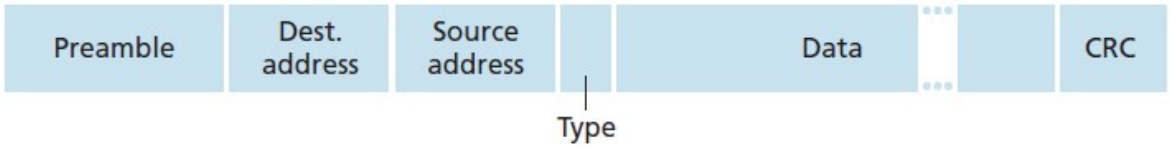
Q 10 . What is MAC address ?

Ans:

In a LAN, transmissions can happen via switches. We need some way to uniquely identify the interfaces of sender and receiver. MAC address aka LAN address or physical address serve this purpose. MAC addresses are 6-byte numbers. Each byte is expressed using two hexadecimal numbers. IEEE manages the MAC address space to provide unique address to each interface card across the world. A sender must know the destination MAC address in order to send a unicast packet. Upon knowing the destination MAC address, the sender broadcasts the packet

Q 11 . Describe role of preamble and address in Ethernet frame format.

Ans:



Preamble : It is of 8 bytes. First 7 bytes of the preamble has a value of 10101010 serve to “wake up” the receiving adapters and to synchronize their clocks to that of the sender’s clock. The last byte is 10101011 - The last 2 bits (the first two consecutive 1s) alert adapter as end of preamble

Address : It is of 6 bytes. Destination address contains the MAC address of the destination adapter. When adapter receives an Ethernet frame whose destination address is either its MAC or the MAC broadcast address, it passes the contents of the frame’s data to the network layer. If it receives a frame with any other MAC address, it discards the frame. Source address contains the MAC address of the adapter that transmits the frame onto the LAN.

Q 12 . How forwarding table is built in switch ?

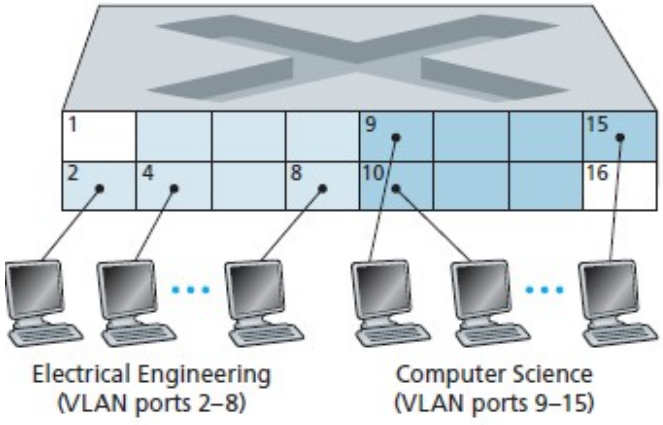
Ans:

When a frame from source reaches switch it comes to know which port (physical) the source MAC is available. First time it does not know which port the destination is available. So it sends packet to all ports. When response reaches it knows destination port.

Q 13 . Why do we need Virtual Lan ? Explain operation of port based VLAN.

Ans:

Each workgroup (department) having its own switched LAN connected to the switched LANs of other groups. Such a configuration often does not works well in real world. Departmental LANs can be done using separate switches which makes LAN location specific. But due to space optimisation or due to project requirement people of different departments might have to seat together which break LAN separation architecture. These difficulties can be handled by a switch that supports virtual local area networks (VLANs).



A switch that supports VLANs allows multiple virtual local area networks to be defined over a single physical local area network infrastructure. In a port-based VLAN, the switch's ports (interfaces) are divided into groups by the network manage. Each group constitutes a VLAN, with the ports in each VLAN forming a broadcast domain. If the user at switch port 8 joins the CS Department, the network operator simply reconfigures the VLAN software so that port 8 is now associated with the CS VLAN. A table of port-to-VLAN mappings is maintained within the switch and switch hardware only delivers frames between ports belonging to the same VLAN.

Q 14 . How wireless communication is different from wired communication ?

Ans :

There are a number of important differences between a wired link and a wireless link.

Decreasing signal strength: Electromagnetic radiation attenuates as it passes through matter (through a wall, even in free space) resulting in decreased signal strength as the distance between sender and receiver increases. Also referred as path loss.

Interference from other sources: Sources transmitting in the same frequency band will interfere with each other. In addition electromagnetic noise within the environment (e.g., a nearby motor, a microwave) can result in interference.

Multipath propagation : Multipath propagation occurs when portions of the electromagnetic wave reflect off objects and the ground, taking paths of different lengths between a sender and receiver.

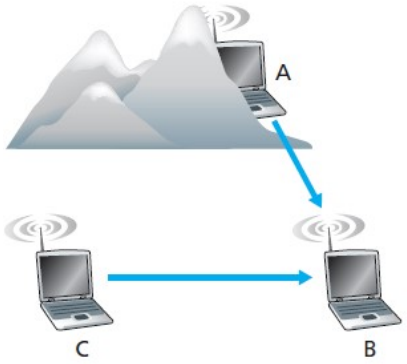
Moving objects between the sender and receiver can cause multipath propagation to change over time.

As signal decreases quickly with distance signal to noise ration (SNR) becomes important point for consideration

So in wireless scenario probability of occurrence of error (bit error rate / packet error rate) is very high.

Q 15 . What is hidden terminal problem ?

Ans:



Suppose that Station A is transmitting to Station B. Suppose also that Station C is transmitting to Station B. Physical obstructions in the environment may prevent A and C from hearing each other's transmissions. A's and C's transmissions are interfering at B. Even they wish A and C can not coordinate to transmit to B. This is called hidden terminal problem. This problem make multiple access in a wireless network considerably more complex and need to address in associated protocols.

Q 16 . How a node get associated with an AP ?

Ans:

AP periodically send beacon frames, each of which includes the AP's SSID and MAC address. Wireless station, scans the 11 channels, seeking beacon frames from any APs that may be out there. User of device or the wireless station itself select one of the APs for association. 802.11 standard does not specify any algorithm for selecting which of the available APs to associate with. It is possible to selected AP with a strong signal or servicing load of an AP. It is known as passive scanning.

Q 17. How RTS and CTS works for CSMA/CA ?

Ans:

802.11 protocol introduce two short frames Request to Send (RTS) and Clear to Send (CTS) to reserve access to the channel. When sender wants to send DATA frame, it first send an RTS frame to the AP, indicating the total time required to transmit the DATA frame and the ACK frame. When the AP receives the RTS frame, it responds by broadcasting a CTS frame. This CTS frame gives the sender explicit permission to send and instructs the other stations not to send for the reserved duration.