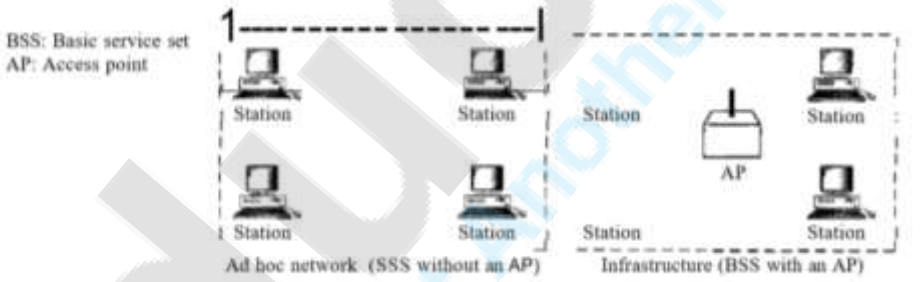
Unit-7

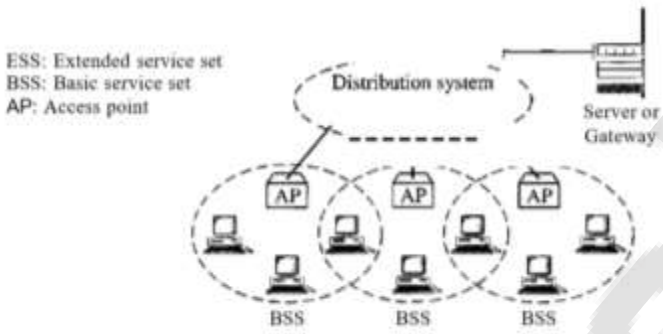
1) **Explain the IEEE 802.11 Protocol Architecture and its Services? (May 15)**
   Answer: -
   1) IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.
   2) Architecture: -The standard defines two kinds of services: the **basic service set (BSS) and the extended service set (ESS).**
   3) **Basic Service Set: -**
      a) IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). Figure 14.1 shows two sets in this standard.
      b) The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture. In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an infrastructure network.

Figure 14.1 *Basic service sets (BSSs)*



   4) **Extended Service Set**
      a) An extended service set (ESS) is made up of two or more BSSs with APs. In this case, 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; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN. Figure shows an ESS.
      b) When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. However, communication between two stations in two different BSSs usually occurs via two APs. The idea is similar to communication in a cellular network if we consider each BSS to be a cell and each AP to be a base station. Note that a mobile station can belong to more than one BSS at the same time.

Figure 14.2 *Extended service sets (ESSs)*



2) What are service provide by Data link layer?

Answer: -

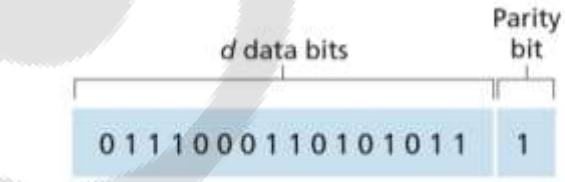
1) **Framing**. Almost all link-layer protocols encapsulate each network-layer datagram within a link-layer frame before transmission over the link. A frame consists of a data field, in which the network-layer datagram is inserted, and a number of header fields. The structure of the frame is specified by the link-layer protocol. We'll see several different frame formats when we examine specific link-layer protocols in the second half of this chapter.
2) **Link access**. A medium access control (MAC) protocol specifies the rules by which a frame is transmitted onto the link. For point-to-point links that have a single sender at one end of the link and a single receiver at the other end of the link, the MAC protocol is simple (or non-existent)—the sender can send a frame whenever the link is idle. The more interesting case is when multiple nodes share a single broadcast link—the so-called multiple access problem. Here, the MAC protocol serves to coordinate the frame transmissions of the many nodes.
3) **Reliable delivery**. When a link-layer protocol provides reliable delivery service, it guarantees to move each network-layer datagram across the link without error. Recall that certain transport-layer protocols (such as TCP) also provide a reliable delivery service. Similar to a transport-layer reliable delivery service, a link-layer reliable delivery service can be achieved with acknowledgments and retransmissions (see Section 3.4). A link-layer reliable delivery service is often used for links that are prone to high error rates, such as a wireless link, with the goal of correcting an error locally—on the link where the error occurs—rather than forcing an end-to end retransmission of the data by a transport- or application-layer protocol. However, link-layer reliable delivery can be considered an unnecessary overhead for low bit-error links, including fiber, coax, and many twisted-pair copper links. For this reason, many wired link-layer protocols do not provide a reliable delivery service.
4) **Error detection and correction**. The link-layer hardware in a receiving node can incorrectly decide that a bit in a frame is zero when it was transmitted as a one, and

vice versa. Such bit errors are introduced by signal attenuation and electromagnetic noise. Because there is no need to forward a datagram that has an error, many link-layer protocols provide a mechanism to detect such bit errors. This is done by having the transmitting node include error-detection bits in the frame, and having the receiving node perform an error check. Recall from Chapters 3 and 4 that the Internet's transport layer and network layer also provide a limited form of error detection—the Internet checksum. Error detection in the link layer is usually more sophisticated and is implemented in hardware. Error correction is similar to error detection, except that a receiver not only detects when bit errors have occurred in the frame but also determines exactly where in the frame the errors have occurred (and then corrects these errors).

3) Explain Different Error Detection and Correction Technique?

Answer: -

1) bit-level error detection and correction— detecting and correcting the corruption of bits in a link-layer frame sent from one node to another physically connected neighbouring node—are two services often provided by the link layer.
2) Error-detection and -correction techniques allow the receiver to sometimes, but not always, detect that bit errors have occurred. Even with the use of error-detection bits there still may be undetected bit errors; that is, the receiver may be unaware that the received information contains bit errors. As a consequence, the receiver might deliver a corrupted datagram to the network layer, or be unaware that the contents of a field in the frame's header have been corrupted.
3) **Parity Checks**: - The simplest form of error detection is the use of a single parity bit. Suppose that the information to be sent, D in Figure 5.4, has d bits. In an even parity scheme, the sender simply includes one additional bit and chooses its value such that the total number of 1s in the d + 1 bits (the original information plus a parity bit) is even. For odd parity schemes, the parity bit value is chosen such that there is an odd number of 1s. Figure 5.4 illustrates an even parity scheme, with the single parity bit being stored in a separate field. Receiver operation is also simple with a single parity bit. The receiver need only count the number of 1s in the received d + 1 bits. If an odd number of 1valued bits are found with an even parity scheme, the receiver knows that at least one bit error has occurred. More precisely, it knows that some odd number of bit errors has occurred.



One-bit even parity

4) **CRC: -** An error-detection technique used widely in today's computer networks is based on cyclic redundancy check (CRC) codes. CRC codes are also known as polynomial codes, since it is possible to view the bit string to be sent as a polynomial whose coefficients are the 0 and 1 values in the bit string, with operations on the bit string interpreted as polynomial arithmetic. Consider the d-bit piece of data, D, that the sending node wants to send to the receiving node. The sender and receiver must first agree on an r + 1 bit pattern, known as a generator, which we will denote as G. We will require that the most significant (leftmost) bit of G be a 1. The key idea behind CRC codes is shown in Figure 5.6. For a given piece of data, D, the sender will choose r additional bits, R, and append them to D such that the resulting d + r bit pattern (interpreted as a binary number) is exactly divisible by G (i.e., has no remainder) using modulo-2 arithmetic. The process of error checking with CRCs is thus simple: The receiver divides the d + r received bits by G. If the remainder is nonzero, the receiver knows that an error has occurred; otherwise the data is accepted as being correct. All CRC calculations are done in modulo-2 arithmetic without carries in addition or borrows in subtraction. This means that addition and subtraction are identical, and both are equivalent to the bitwise exclusive-or (XOR) of the operands. Thus, for example,

```
1011 XOR 0101 = 1110
1001 XOR 1101 = 0100
```

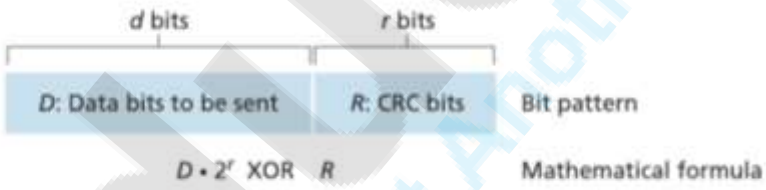


Figure 5.6 ♦ CRC

5) **Check Sum**: - In check summing techniques, the d bits of data in Figure 5.4 are treated as a sequence of k-bit integers. One simple check summing method is to simply sum these k-bit integers and use the resulting sum as the error-detection bits. The Internet checksum is based on this approach—bytes of data are treated as 16-bit integers and summed. The 1s complement of this sum then forms the Internet checksum that is carried in the segment header. The receiver checks the checksum by taking the 1s complement of the sum of the received data (including the checksum) and checking whether the result is all 1 bits. If any of the bits are 0, an error is indicated. In the TCP and UDP protocols, the Internet checksum is computed over all fields (header and data fields included). In IP the checksum is computed over the IP header (since the UDP or TCP segment has its own checksum). In other protocols, for example, XTP [Strayer 1992], one checksum is computed over the header and another checksum is computed over the entire packet. Check summing methods require

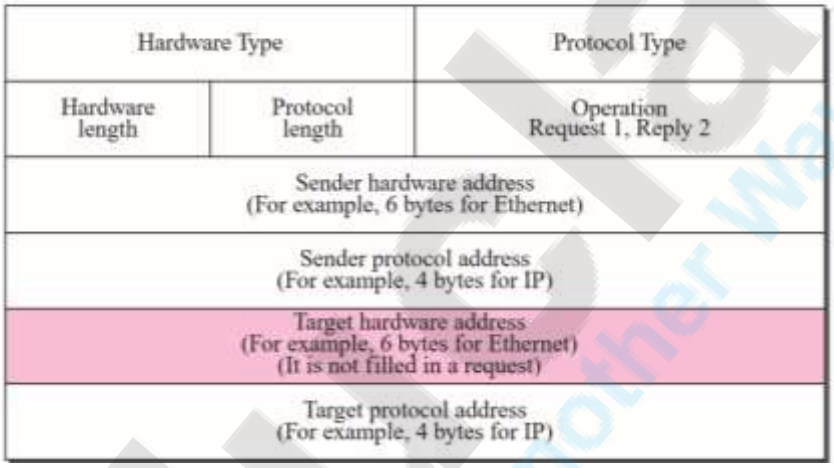
relatively little packet overhead. For example, the checksums in TCP and UDP use only 16 bits. However, they provide relatively weak protection against errors as compared with cyclic redundancy check, which is discussed below and which is often used in the link layer. Because transport-layer error detection is implemented in software, it is important to have a simple and fast error-detection scheme such as check summing. On the other hand, error detection at the link layer is implemented in dedicated hardware in adapters, which can rapidly perform the more complex CRC operations.

4) Short Note on ARP Packet Format?

Answer: -

1) The format of an ARP packet. The fields are as follows:

Figure 8.3 *ARP packet*



2) **Hardware type**. This is a 16-bit field defining the type of the network on which ARP is running. Each LAN has been assigned an integer based on its type. For example, Ethernet is given the type 1. ARP can be used on any physical network.
3) **Protocol type**. This is a 16-bit field defining the protocol. For example, the value of this field for the IPv4 protocol is 080016. ARP can be used with any higher-level protocol.
4) **Hardware length**. This is an 8-bit field defining the length of the physical address in bytes. For example, for Ethernet the value is 6.
5) **Protocol length**. This is an 8-bit field defining the length of the logical address in bytes. For example, for the IPv4 protocol the value is 4.
6) **Operation: -** This is a 16-bit field defining the type of packet. Two packet types are defined: ARP request (1), ARP reply (2).
7) **Sender hardware address.** This is a variable-length field defining the physical address of the sender. For example, for Ethernet this field is 6 bytes long.
8) **Sender protocol address.** This is a variable-length field defining the logical (for example, IP) address of the sender. For the IP protocol, this field is 4 bytes long.

9) **Target hardware address.** This is a variable-length field defining the physical address of the target. For example, for Ethernet this field is 6 bytes long. For an ARP request message, this field is all 0s because the sender does not know the physical address of the target.
10) **Target protocol address**. This is a variable-length field defining the logical (for example, IP) address of the target. For the IPv4 protocol, this field is 4 bytes long.

5) In which layer PPP works? Explain PPP in detail? (May 14) (Dec 14)

Answer: -

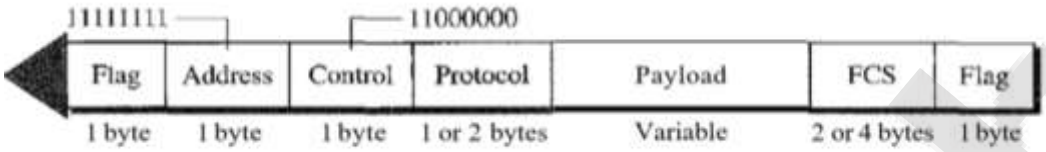
1) In the data link layer PPP works.
2) The most common protocols for point-to-point access are the Point-to-Point Protocol (PPP). Today, millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP. The majority of these users have a traditional modem; they are connected to the Internet through a telephone line, which provides the services of the physical layer. But to control and manage the transfer of data, there is a need for a point-to-point protocol at the data link layer. PPP is by far the most common.
3) PPP provides several services:
   a) PPP defines the format of the frame to be exchanged between devices.
   b) PPP defines how two devices can negotiate the establishment of the link and the exchange of data.
   c) PPP defines how network layer data are encapsulated in the data link frame.
   d) PPP defines how two devices can authenticate each other.
   e) PPP provides multiple network layer services supporting a variety of network layer protocols.
   f) PPP provides connections over multiple links.
   g) PPP provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.
4) On the other hand, to keep PPP simple, several services are missing:
   a) PPP does not provide flow control. A sender can send several frames one after another with no concern about overwhelming the receiver.
   b) PPP has a very simple mechanism for error control. A CRC field is used to detect errors. If the frame is corrupted, it is silently discarded; the upper-layer protocol needs to take care of the problem. Lack of error control and sequence numbering may cause a packet to be received out of order.
   c) PPP does not provide a sophisticated addressing mechanism to handle frames in a multipoint configuration.

6) Explain PPP frame format in detail?

Answer: -

1) PPP is a byte-oriented protocol. The format of a PPP frame. The description of each field follows:

32 *PPP frame format*



2) **Flag.** A PPP frame starts and ends with a I-byte flag with the bit pattern 01111110. Although this pattern is the same as that used in HDLC, there is a big difference. PPP is a byte-oriented protocol; HDLC is a bit-oriented protocol. The flag is treated as a byte, as we will explain later.
3) **Address.** The address field in this protocol is a constant value and set to 11111111 (broadcast address). During negotiation (discussed later), the two parties may agree to omit this byte.
4) **Control.** This field is set to the constant value 11000000 (imitating unnumbered frames in HDLC). As we will discuss later, PPP does not provide any flow control. Error control is also limited to error detection. This means that this field is not needed at all, and again, the two parties can agree, during negotiation, to omit this byte.
5) **Protocol.** The protocol field defines what is being carried in the data field: either user data or other information. We discuss this field in detail shortly. This field is by default 2 bytes long, but the two parties can agree to use only I byte.
6) **Payload field.** This field carries either the user data or other information that we will discuss shortly. The data field is a sequence of bytes with the default of a maximum of 1500 bytes; but this can be changed during negotiation. The data field is byte stuffed if the flag byte pattern appears in this field. Because there is no field defining the size of the data field, padding is needed if the size is less than the maximum default value or the maximum negotiated value.
7) **FCS.** The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRe.

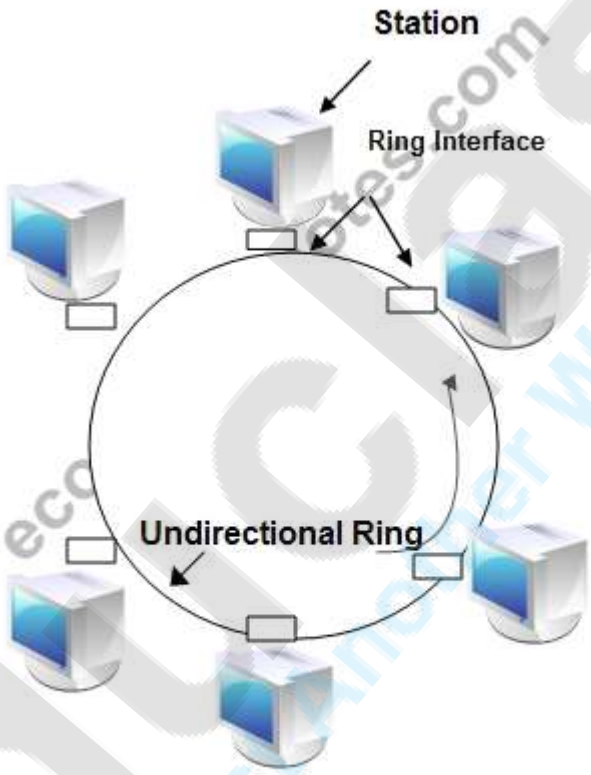
7) Explain IEEE 802.5 with frame format and specifications? Standard? (Dec 15)

Answer: -

1) IEEE 802.5 Token Ring: Token ring is the IEEE 802.5 standard for a token-passing ring in Communication networks. A ring consists of a collection of ring interfaces connected by point-to-point lines *i.e.* ring interface of one station is connected to the ring interfaces of its left station as well as right station. Internally, signals travel around the Communication network from one station to the next in a ring.
2) These point-to-point links can be created with twisted pair, coaxial cable or fiber optics. Each bit arriving at an interface is copied into a 1-bit buffer. In this buffer the bit is checked and may be modified and is then copied out to

the ring again. This copying of bit in the buffer introduces a 1-bit delay at each interface.

3) Token Ring is a LAN protocol defined in the IEEE 802.5 where all stations are connected in a ring and each station can directly hear transmissions only from its immediate neighbor. Permission to transmit is granted by a message (token) that circulates around the ring. A token is a special bit pattern (3 bytes long). There is only one token in the network.



A Ring Network

4) Token-passing networks move a small frame, called a token, around the network. Possession of the token grants the right to transmit. If a node receiving the token in order to transmit data, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. Since only one station can possess the token and transmit data at any given time, there are no collisions.

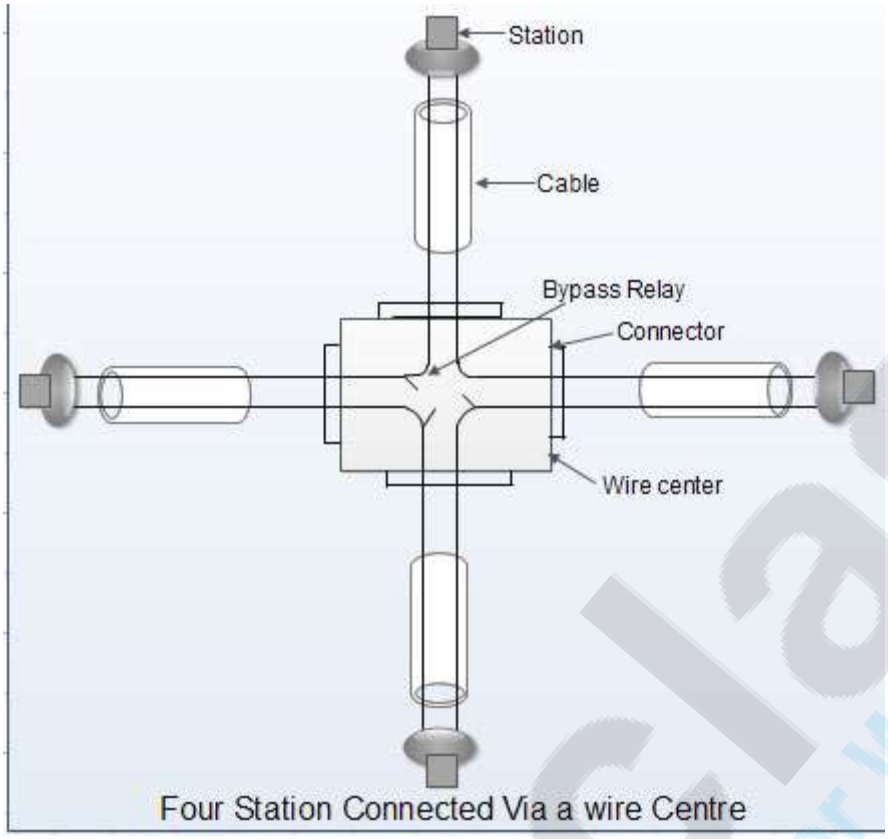
5) There are two operating modes of ring interfaces. There are listen and transmit. In listen mode, the input bits are simply copied to output with a delay of 1- bit time. In transmit mode the connection between input and output is broken by the interface so that is can insert its own data. The station comes in transmit mode when it captures the token.

6) The frames are acknowledged by the destination in a very simple manner. The sender sends frames to receiver with ACK bit 0. The receiver on receiving frames, copies data into its buffer, verifies the checksum and set the ACK bit to 1. The verified frames come back to sender, where they are removed from the ring.

7) The information frame circulates the ring until it reaches the intended destination station, which copies the information for further processing. The information frame continues to circle the ring and is finally removed when it reaches the sending station. The sending station can check the returning frame to see whether the frame was seen and subsequently copied by the destination.

8) A station can hold a token for a specific duration of time. During this time, it has to complete its transmission and regenerates the token in ring. Whenever a station finishes its transmissions, the other station grabs the token and starts its own transmission.

9) **Handling cable breakage in ring networks**



Four Station Connected Via a wire Centre

• If the cable breaks, the entire ring network goes down. This can completely stop the propagation of token in the ring.

• This problem can be solved by using wire centre as shown in fig.

• This wire centre bypasses the terminal that has gone down in following manner:

(a) Each station is connected to wire center by a cable containing two twisted pairs, one for data to station and one for data from the station.

(b) Inside the wire center are bypass relays that are energized by the current from the stations.

(c) If the ring breaks or a station goes down loss of drive current will release the relay and bypass the station.

8) **Discuss various collision free protocols? (ALOHA ,CSMA/CD)**
9) **Difference between CSMA and CSMA/CD? (May 14)**

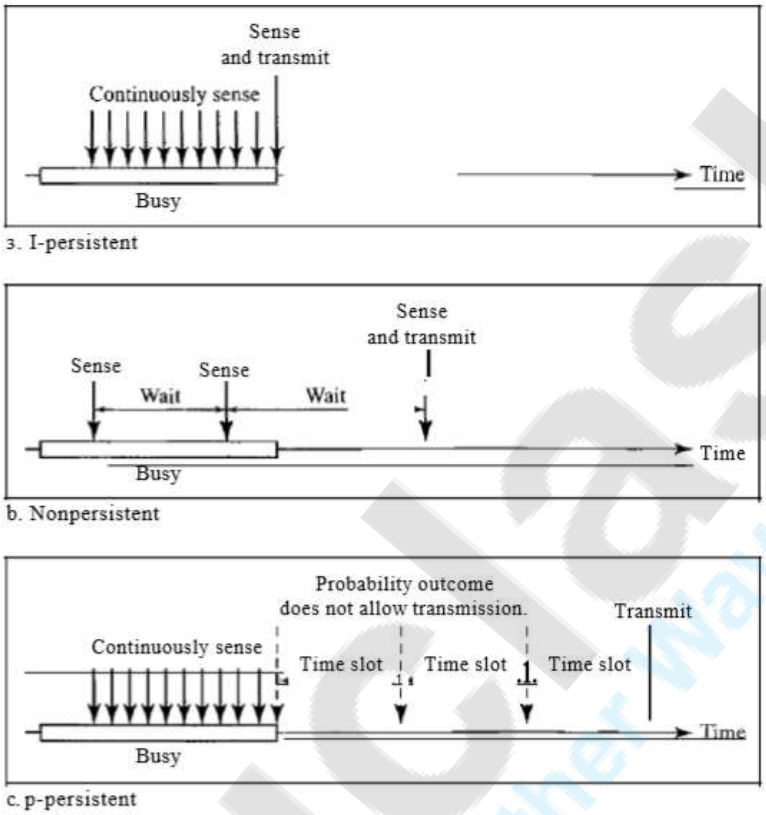
Sr.no.	CSMA-CD	CSMA-CS
1	Carrier sense multiple access with collision detection	Carrier sense multiple access with collision avoidance
2	CSMA/CD is standardized in IEEE 802.3	802.11b uses CSMA/CA MAC protocol
3	It act as interference between the logical link control sublayer and the network's physical layer.	It is protocol to implement the distributed coordination function(DCF) of the MAC sublayer.
4	Collisions detected within short time	RTS/CTS is used to avoid collisions.
5	If a collision is detected, the station aborts the transmission and sends a jamming signal to inform all other stations that a collision has occurred.	Use of RTS/CTS can be enabled or disabled depending on the traffic load(probablility of collisions).
6	This protocol is the basis of classical Ethernet LAN.	Used in a network where collision cannot be detected.,Eg. Wireless LAN

10) Short on CSMA and CSMA/CD? (Dec 14)

Answer: -

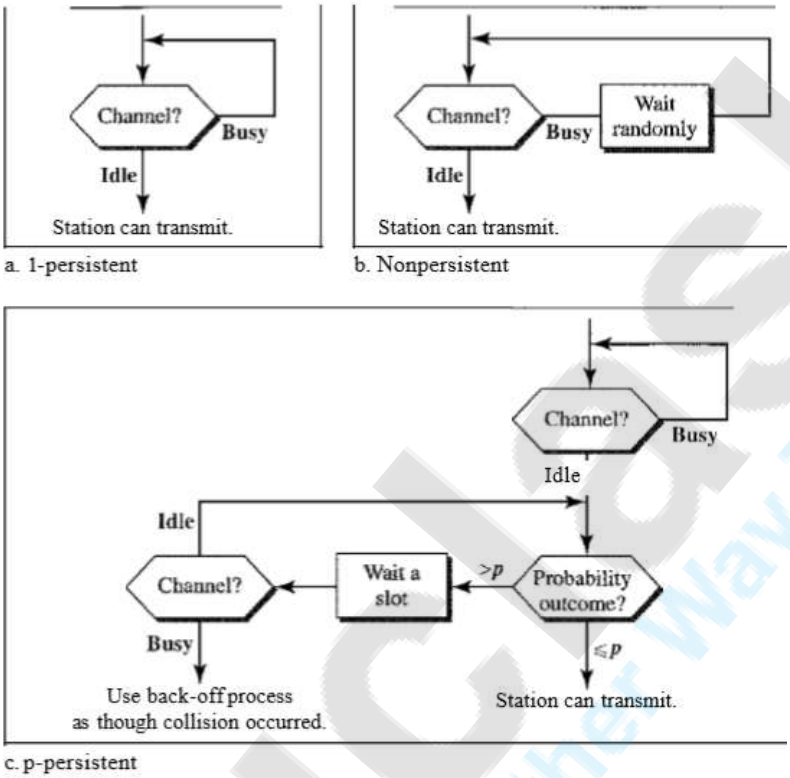
1) To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. Carrier-sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending. In other words, CSMA is based on the principle "sense before transmit" or "listen-before talk." CSMA can reduce the possibility of collision, but it cannot eliminate it. The reason for this is shown in Figure 12.8, a space and time model of a CSMA network. Stations are connected to a shared channel (usually a dedicated medium). The possibility of collision still exists because of propagation delay; when a station sends a frame, it still takes time (although very short) for the first bit to reach every station and for every station to sense it. In other words, a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received. At time tI' station B senses the medium and finds it idle, so it sends a frame. At time t2 (t2> tI)' station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C. Station C also sends a frame. The two signals collide and both frames are destroyed.
2) **Persistence Methods: -**

Figure 12.10 *Behavior of three persistence methods*



3) **I-Persistent: -** The I-persistent method is simple and straightforward. In this method, after the station finds the line idle, it sends its frame immediately (with probability I). This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately. We will see in Chapter 13 that Ethernet uses this method.
4) **Non-persistent: -** In the non-persistent method, a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again. The non-persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously. However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

Figure 12.11 *Flow diagram for three persistence methods*



5) **p-Persistent: -** The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time. The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency. In this method, after the station finds the line idle it follows these steps:

1. With probability p, the station sends its frame.
2. With probability q = 1 - p, the station waits for the beginning of the next time slot and checks the line again.
   a. If the line is idle, it goes to step 1.
   b. If the line is busy, it acts as though a collision has occurred and uses the back off procedure.

6) **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**

A) The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

B) In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again. To better understand CSMA/CD, let us look at

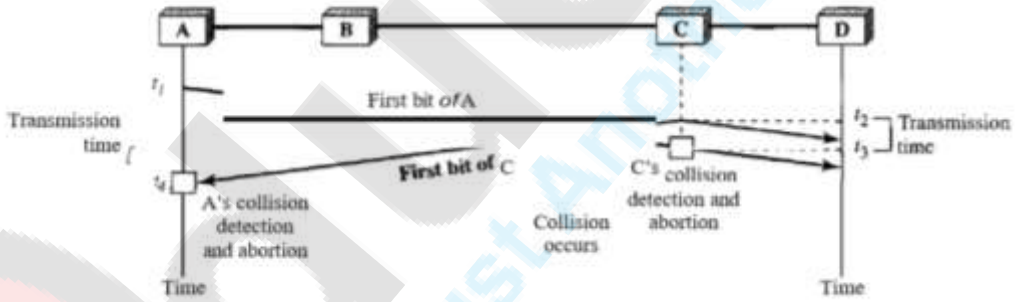
the first bits transmitted by the two stations involved in the collision. Although each station continues to send bits in the frame until it detects the collision, we show what happens as the first bits collide.

C) In Figure 12.12, stations A and C are involved in the collision. At time t1, station A has executed its persistence procedure and starts sending the bits of its frame. At time t2, station C has not yet sensed the first bit sent by A. Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right.

D) The collision occurs sometime after time t2' Station C detects a collision at time t3 when it receives the first bit of A's frame. Station C immediately (or after a short time, but we assume immediately) aborts transmission. Station A detects collision at time t4 when it receives the first bit of C's frame; it also immediately aborts transmission.

E) Looking at the figure, we see that A transmits for the duration t4 - tl; C transmits for the duration t3 - t2' Later we show that, for the protocol to work, the length of any frame divided by the bit rate in this protocol must be more than either of these durations. At time t4, the transmission of A:s frame, though incomplete, is aborted; at time t3, the transmission of B's frame, though incomplete, is aborted.

Figure 12.12 *Collision of the first bit in CSMA/CD*

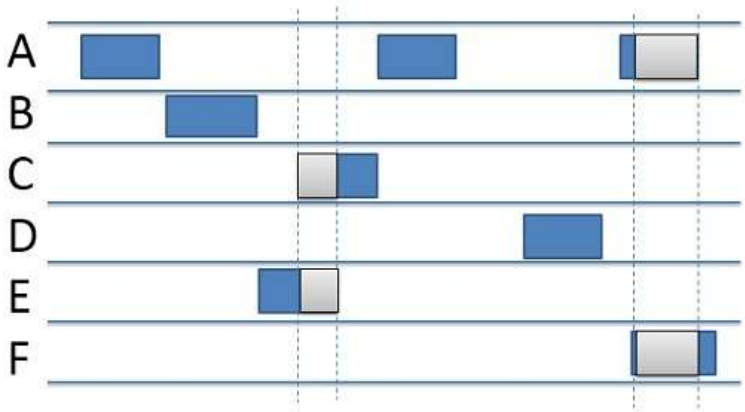


11) Describe ALOHA multiple access techniques and its different forms with performance?

Answer: -

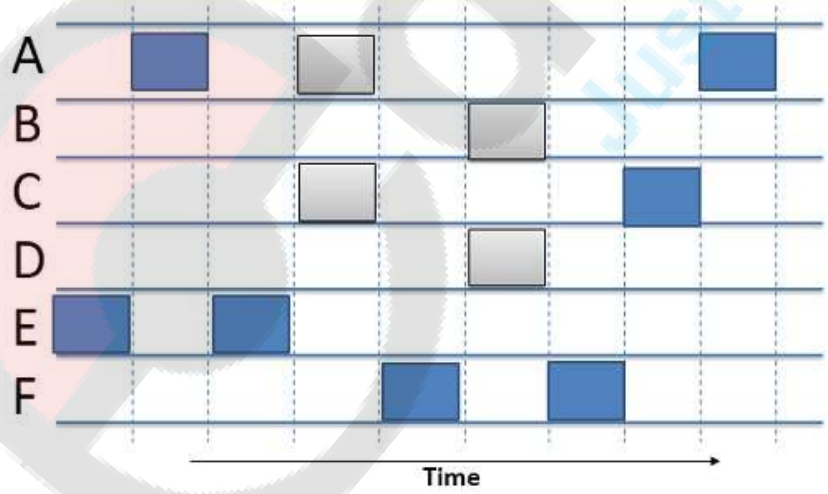
1) Definition Of Pure ALOHA

Pure ALOHA is introduced by Norman Abramson and his associates at the University of Hawaii in early 1970. The Pure ALOHA just allows every station to transmit the data whenever they have the data to be sent. When every station transmits the data without checking whether the channel is free or not there is always the possibility of the collision of data frames. If the acknowledgment arrived for the received frame, then it is ok or else if the two frames collide (Overlap), they are damaged.



Pure ALOHA

2) If a frame is damaged, then the stations wait for a random amount of type and retransmits the frame till it transmits successfully. The waiting time of the each station must be random and it must not be same just to avoid the collision of the frames again and again. The throughput of the Pure ALOHA is maximized when the frames are of uniform length. The formula to calculate the throughput of the Pure ALOHA is S-=G*e^-2G, the throughput is maximum when G=1/2 which is 18% of the total transmitted data frames.
3) **Definition Of Slotted ALOHA**
After the pure ALOHA in 1970, Roberts introduced an another method to improve the capacity of the Pure ALOHA which is called Slotted ALOHA. He proposed to divide the time into discrete intervals called time slots. Each time slot corresponds to the length of the frame. In contrast to the Pure ALOHA, Slotted ALOHA does not allow to transmit the data whenever the station has the data to be send. The Slotted ALOHA makes the station to wait till the next time slot begins and allow each data frame to be transmitted in the new time slot.



Slotted ALOHA

4) Synchronization can be achieved in Slotted ALOHA with the help of a special station that emits a pip at the beginning of every time slot as a clock does. The formula to calculate the throughput of the Slotted ALOHA is S=G*e^-G, the throughput is maximum when G=1 which is 37% of the total transmitted data frames. In Slotted ALOHA, 37% of the time slot is empty, 37% successes and 26% collision.

5) Key Differences Between Pure ALOHA and Slotted ALOHA

a) Pure ALOHA was introduced by Norman and his associates at the university of Hawaii in 1970. On the other hand, Slotted ALOHA was introduced by Roberts in 1972.

b) In pure ALOHA, whenever a station has data to send it transmits it without waiting whereas, in slotted ALOHA a user wait till the next time slot beings to transmit the data.

c) In pure ALOHA the time is continuous whereas, in Slotted ALOHA the time is discrete and divided into slots.

d) In pure ALOHA the probability of successful transmission is S=G*e^-2G. On the other hand, in slotted ALOHA the probability of successful transmission is S=G*e^-G.

e) The time of sender and receiver in pure ALOHA is not globally synchronized whereas, the time of sender and receiver in slotted ALOHA is globally synchronized.

f) The maximum throughput occurs at G=1/2 which is 18 % whereas, the maximum throughput occurs at G=1 which is 37%.

6) Conclusion:

The Slotted ALOHA is somewhat better than the Pure ALOHA. As the probability of collision is less in Slotted ALOHA as compared to Pure ALOHA because the station waits for the next time slot to begin which let the frame in a previous time slot to pass and avoids the collision between the frames.

12) What do you mean by ARP and PPP over the Internet Standard? Explain its features in detail? (May 15)

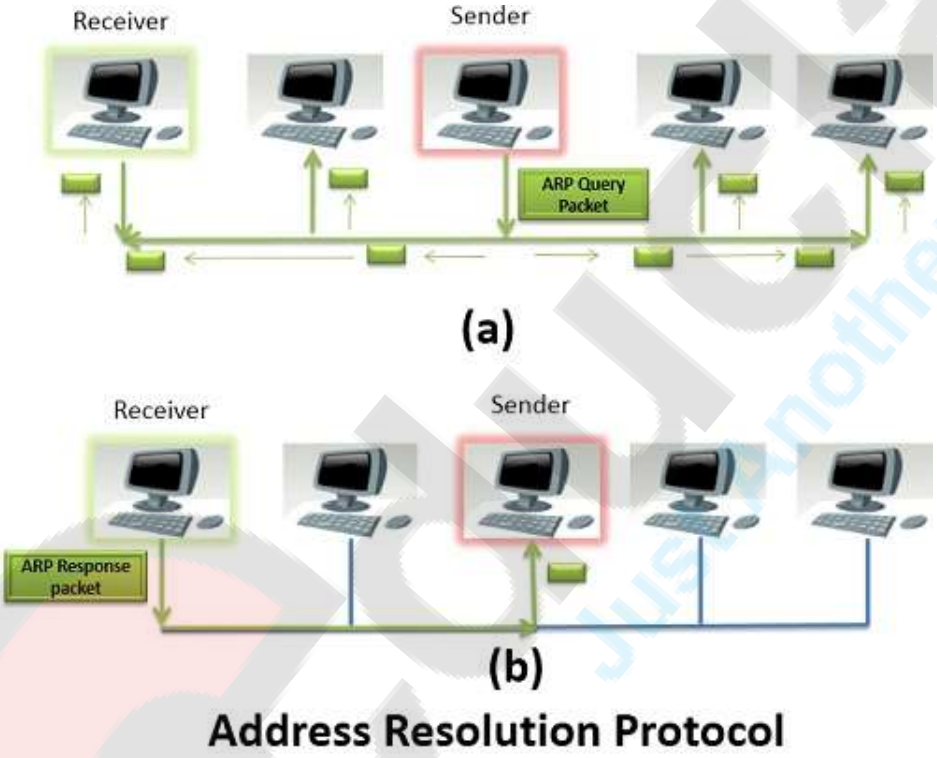
Answer: -

1) ARP and RARP both are the Network layer protocol. Whenever a host needs to send an IP datagram to another host, the sender requires both the logical address and physical address of the receiver. The dynamic mapping provides two protocols ARP and RARP. The basic difference between ARP and RARP is that ARP when provided with the logical address of the receiver it obtains the physical address of the receiver whereas in RARP when provided with the physical address of the host, it obtains the logical address of the host from the server.

2) **Definition of ARP**

3) ARP (Address Resolution Protocol) is a network layer protocol. As ARP is a dynamic mapping protocol, each host in the network knows the Logical address of another host. Now, suppose a host needs to send the IP datagram to another host. But, the IP datagram must be encapsulated in a frame so that it can pass through the physical network between sender and receiver. Here, the sender needs the physical address of the receiver so that it is being identified that to which receiver the packet belong to when the packet travel in the physical network.

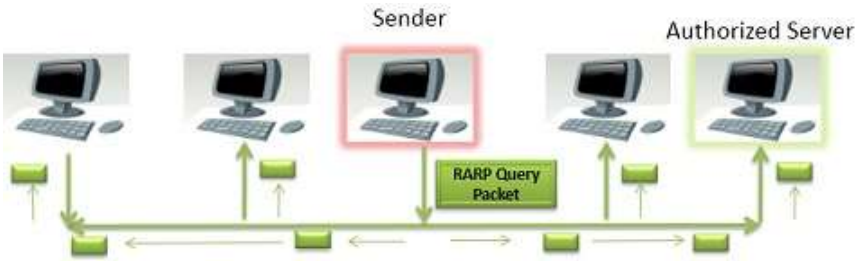
4) For retrieving the physical address of the receiver the sender performs the following action.
    a) The sender sends the ARP query packet on the network which is broadcasted to all the other host or router present in the network.
    b) The ARP query packet contains the logical and physical address of the sender and the logical address of the receiver.
    c) All the host and router receiving the ARP query packet process it but, only the intended receiver identifies its logical address present in the ARP query packet.
    d) The receiver then sends ARP response packet which contains the logical (IP) address and physical address of the receiver.
    e) The ARP response packet is unicast directly to the sender whose physical address is present in the ARP query packet.



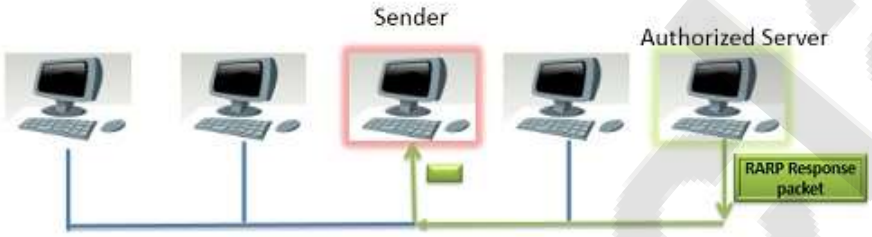
Address Resolution Protocol

5) **Definition of RARP**
6) RARP (Reverse Address Resolution Protocol) is also a network layer protocol. RARP is a TCP/IP protocol that allows any host to obtain its IP address from the server. RARP is adapted from the ARP protocol and it is just reverse of ARP. RARP perform following steps to obtain an IP address from the server.
    a) The sender broadcast the RARP request to all the other host present in the network.
    b) The RARP request packet contains the physical address of the sender.

c) All the host receiving the RARP request packet process it but, the authorized host only which can serve RARP service, responds to the RARP request packet such host are known as RARP Server.
d) The authorized RARP server replies directly to requesting host with the RARP response packet which contains IP address for the sender.



(a)



(b)

Reverse Address Resolution Protocol

7) RARP is outdated now because of two reasons. First, the RARP is using the broadcast service of the data-link layer; that means the RARP must be present at each network. Second, RARP only provides IP address but today the computer also need other information.
8) **Key Differences Between ARP and RARP**
   a) The full form of ARP is Address Resolution Protocol whereas, the full form of RARP is Reverse Address Resolution Protocol.
   b) ARP protocol retrieves the physical address of the receiver. On the other hand, the RARP protocol retrieves logical (IP) address of the protocol.
   c) ARP maps 32 bit logical (IPv4) address to a 48-bit physical address of the receiver. On the other hand, RARP maps 48-bit physical address to 32-bit logical address of the receiver.
9) **Conclusion: -**RARP has been replaced by BOOTP and DHCP.

13) Difference between ARP and RARP?

BASIS FOR COMPARISON	ARP	RARP
Full Form	Address Resolution Protocol.	Reverse Address Resolution Protocol.
Basic	Retrieves the physical address of the receiver.	Retrieves the logical address for a computer from the server.
Mapping	ARP maps 32-bit logical (IP) address to 48-bit physical address.	RARP maps 48-bit physical address to 32-bit logical (IP) address.

14) Difference between Point-to-Point and Multipoint?

BASIS FOR COMPARISON	POINT-TO-POINT	MULTIPOINT
Link	There is dedicated link between two devices.	The link is shared between more than two devices.
Channel Capacity	The channel's entire capacity is reserved for the two connected devices.	The channel's capacity is shared temporarily among the devices connected to the link.
Transmitter and Receiver	There is a single transmitter and a single receiver.	There is a single transmitter and multiple receivers.
Example	Frame relay, T-carrier, X.25, etc.	Frame relay, token ring, Ethernet, ATM, etc.

15) Difference between Pure ALOHA vs Slotted ALOHA?

Answer: -

BASIS FOR COMPARISON	PURE ALOHA	SLOTTED ALOHA
Introduced	Introduced by Norman Abramson and his associates at the University of Hawaii in 1970.	Introduced by Roberts in 1972.
Frame Transmission	The user can transmit the data frame whenever the station has the data to be transmitted.	The user has to wait till the next time slot start, to transmit the data frame.
Time	In Pure ALOHA the time is continuous.	In Slotted ALOHA the time is discrete.
Successful Transmission	The probability of successful transmission of the data frame is: S= G* e^-2G	The probability of successful transmission of the data frame is: S= G*e^-G
Synchronization	The time is not globally synchronized.	The time here is globally synchronized.
Throughput	The maximum throughput occurs at G = 1/2 which is 18%.	The maximum throughput occurs at G = 1 which is 37%.

16) Difference between ARP and DHCP? (May 14)