

Department of Computer Science and Engineering
CS602 Computer Networks
Subject Notes: UNIT-II

Syllabus: Data Link Layer: Need, Services Provided, Framing, Flow Control, Error control. Data Link Layer Protocol: Elementary & Sliding Window protocol: 1-bit, Go-Back-N, Selective Repeat, Hybrid ARQ.

DATA LINK LAYER: NEED

Data Link Layer is second layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.

Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware.

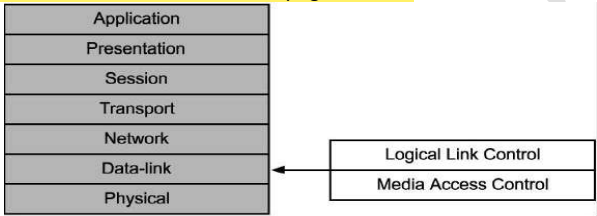


Fig. 2.1 Seven Layer Architecture

Data link layer has two sub-layers:

- Logical Link Control: It deals with protocols, flow-control, and error control
- Media Access Control: It deals with actual control of media

DATA LINK LAYER: SERVICE PROVIDED

- Encapsulation of network layer data packets into frames.
- Frame synchronization.
- Error Control
- Flow control, in addition to the one provided on the transport layer.
- LAN switching (packet switching) including MAC filtering and spanning tree protocol
- Data packet queuing or scheduling
- Store-and-forward switching or cut-through switching

DATA LINK LAYER: FRAMING

Since the physical layer merely accepts and transmits a stream of bits without any regard to meaning or structure, it is up to the data link layer to create and recognize frame boundaries. This can be accomplished by attaching special bit patterns to the beginning and end of the frame. If these bit patterns can accidentally occur in data, special care must be taken to make sure these patterns are not incorrectly interpreted as frame delimiters. The four framing methods that are widely used are

- Character count
- Starting and ending characters, with character stuffing
- Starting and ending flags, with bit stuffing

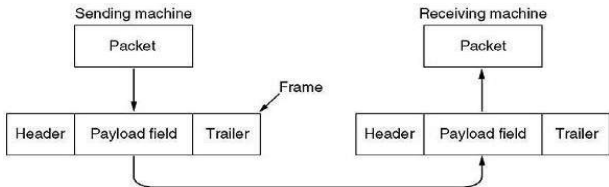


Fig. 2.2 Data Link Layer: Framing

Character Count

This method uses a field in the header to specify the number of characters in the frame. When the data link layer at the destination sees the character count, it knows how many characters follow, and hence where the end of the frame is. The disadvantage is that if the count is garbled by a transmission error, the destination will lose synchronization and will be unable to locate the start of the next frame. So, this method is rarely used.

Character stuffing

In the second method, each frame starts with the ASCII character sequence DLE STX and ends with the sequence DLE ETX. This method overcomes the drawbacks of the character count method. However, character stuffing is closely associated with 8-bit characters and this is a major hurdle in transmitting arbitrary sized characters.

Bit stuffing

The third method allows data frames to contain an arbitrary number of bits and allows character codes with an arbitrary number of bits per character. At the start and end of each frame is a flag byte consisting of the special bit pattern 01111110. Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a zero bit into the outgoing bit stream. This technique is called bit stuffing

Physical layer coding violations

The final framing method is physical layer coding violations and is applicable to networks in which the encoding on the physical medium contains some redundancy. In such cases normally, a 1 bit is a high-low pair and a 0 bit is a low-high pair. The combinations of low-low and high-high which are not used for data may be used for marking frame boundaries.

DATALINK LAYER: FLOW CONTROL

Flow control coordinates that amount of data that can be sent before receiving acknowledgement.

- It is one of the most important duties of the data link layer.
- Flow control tells the sender how much data to send.
- It makes the sender wait for some sort of an acknowledgment (ACK) before continuing to send more data.
- Flow Control Techniques: Stop-and-wait, and Sliding Window

DATA LINK LAYER: ERROR CONTROL

Error control in the data link layer is based on ARQ (automatic repeat request), which is the retransmission of data.

- The term error control refers to methods of error detection and retransmission.
- Anytime an error is detected in an exchange, specified frames are retransmitted. This process is called ARQ.

To ensure reliable communication, there needs to exist flow control (managing the amount of data the sender sends), and error control (that data arrives at the destination error free).

- Flow and error control needs to be done at several layers.
- For node-to-node links, flow and error control is carried out in the data-link layer.

- For end-point to end-point, flow and error control is carried out in the transport layer. There may be three types of errors:



Fig. 2.3 Single bit error

In a frame, there is only one bit, anywhere though, which is corrupt.



Fig. 2.4 Multiple bits error

Frame is received with more than one bit in corrupted state.



Fig. 2.5 Burst error

Frame contains more than 1 consecutive bits corrupted.

DATA LINK LAYER PROTOCOL

The basic function of the layer is to transmit frames over a physical communication link. Transmission may be half duplex or full duplex. To ensure that frames are delivered free of errors to the destination station (IMP) a number of requirements are placed on a data link protocol. The protocol (control mechanism) should be capable of performing:

- The identification of a frame (i.e. recognises the first and last bits of a frame).
- The transmission of frames of any length up to a given maximum. Any bit pattern is permitted in a frame.
- The detection of transmission errors.
- The retransmission of frames which were damaged by errors.
- The assurance that no frames were lost.
- In a multidrop configuration some mechanism must be used for preventing conflicts caused by simultaneous transmission by many stations.
- The detection of failure or abnormal situations for control and monitoring purposes.

It should be noted that as far as layer 2 is concerned a host message is pure data, every single bit of which is to be delivered to the other host. The frame header pertains to layer 2 and is never given to the host.

Elementary Data Link Protocols

- Data are transmitted in one direction only
- The transmitting (Tx) and receiving (Rx) hosts are always ready
- Processing time can be ignored
- Infinite buffer space is available
- No errors occur; i.e. no damaged frames and no lost frames (perfect channel)

Sliding Window protocol:

A sliding window protocol is a feature of packet-based data transmission protocols. Sliding window protocols are used where reliable in-order delivery of packets is required, such as in the Data Link Layer (OSI model) as well as in the Transmission Control Protocol (TCP).

The Sliding Window ARQ has three techniques

- 1-bit
- Go- Back N
- Selective Repeat

1-bit

One-bit sliding window protocol is also called Stop-And-Wait protocol. In this protocol, the sender sends out one frame, waits for acknowledgment before sending next frame, thus the name Stop-And-Wait.

Problem with Stop-And-Wait protocol is that it is very inefficient. At any one moment, only in frame is in transition. The sender will have to wait at least one round trip time before sending next. The waiting can be long for a slow network such as satellite link.

Stop and Wait Protocol

Characteristics

- Used in Connection-oriented communication.
- It offers error and flow control
- It is used in Data Link and Transport Layers
- Stop and Wait ARQ mainly implements Sliding Window Protocol concept with Window Size 1

Useful Terms:

- Propagation Delay:** Amount of time taken by a packet to make a physical journey from one router to another router.

$$\text{Propagation Delay} = (\text{Distance between routers}) / (\text{Velocity of propagation})$$

- $\text{RoundTripTime (RTT)} = 2 * \text{Propagation Delay}$
- $\text{TimeOut (TO)} = 2 * \text{RTT}$
- $\text{Time To Live (TTL)} = 2 * \text{TimeOut. (Maximum TTL is 180 seconds)}$

Simple Stop and Wait

Sender:

- Rule 1) Send one data packet at a time.
- Rule 2) Send next packet only after receiving acknowledgement for previous.

Receiver:

- Rule 1) Send acknowledgement after receiving and consuming of data packet.
- Rule 2) after consuming packet acknowledgement need to be sent (Flow Control)

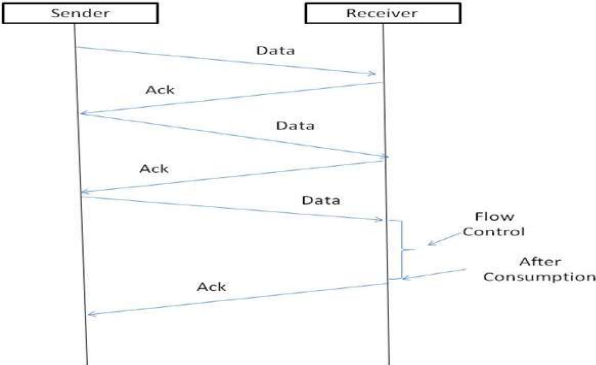
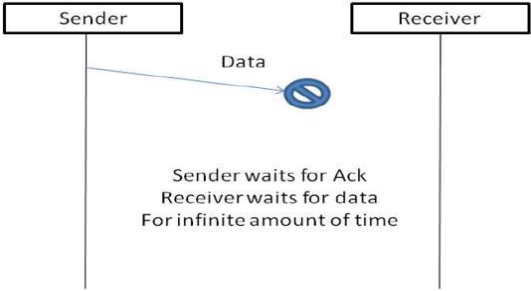


Fig. 2.6 Stop and Wait

Problems:

1. Lost Data



2. Lost Acknowledgement:

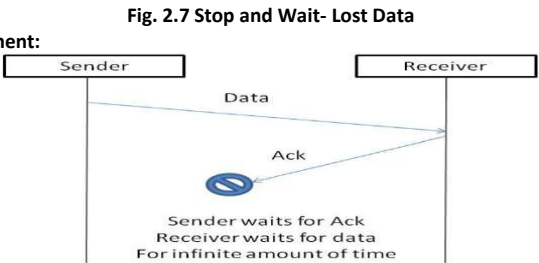


Fig. 2.8 Stop and Wait- Lost Acknowledgement

3. Delayed Acknowledgement/Data: After timeout on sender side, a long-delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

Stop and Wait ARQ (Automatic Repeat Request)

Above 3 problems are resolved by Stop and Wait ARQ (Automatic Repeat Request) that does both error control and flow control.

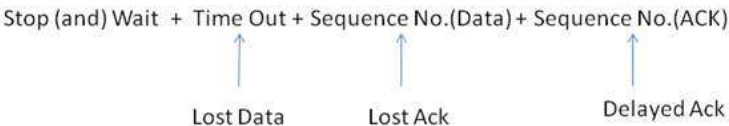


Fig. 2.9 Stop and Wait ARQ (Automatic Repeat Request)

1. Time Out:

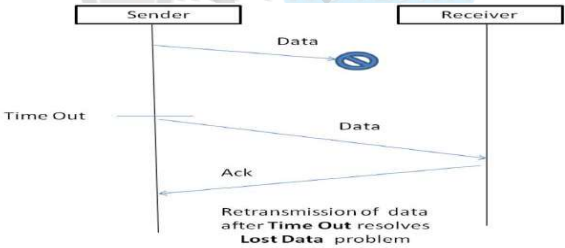


Fig. 2.10 Stop and Wait ARQ-Time Out

2. Sequence Number (Data)

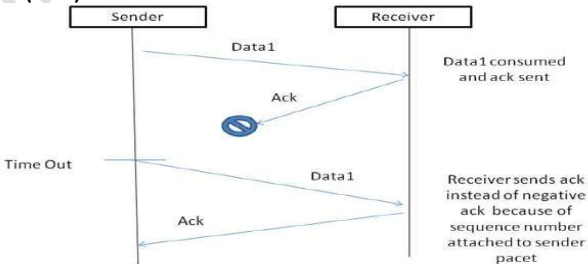


Fig. 2.11 Stop and Wait ARQ-ACK Lost

3. Delayed Acknowledgement:

This is resolved by introducing sequence number for acknowledgement also.

Working of Stop and Wait ARQ:

- 1) Sender A sends a data frame or packet with sequence number 0.
 - 2) Receiver B, after receiving data frame, sends and acknowledgement with sequence number 1 (sequence number of next expected data frame or packet)
- There is only one-bit sequence number that implies that both sender and receiver have buffer for one frame or packet only.

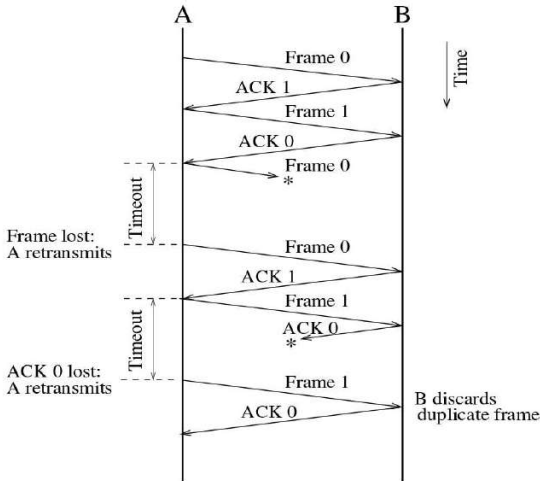


Fig. 2.12 Working of Stop and Wait ARQ

Characteristics of Stop and Wait ARQ:

- It uses link between sender and receiver as half duplex link
- Throughput = 1 Data packet/frame per RTT
- If Bandwidth*Delay product is very high, then stop and wait protocol is not so useful. The sender has to keep waiting for acknowledgements before sending the processed next packet.
- It is an example for "Closed Loop OR connection oriented" protocols
- It is a special category of SWP where its window size is 1
- Irrespective of number of packets sender is having stop and wait protocol requires only 2 sequences numbers 0 and 1

The Stop and Wait ARQ solves main three problems, but may cause big performance issues as sender always waits for acknowledgement even if it has next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high (you are connected to some server in some other country though a high-speed connection). To solve this problem, we can send more than one packet at a time with a larger sequence numbers. We will be discussing these protocols in next articles. So, Stop and Wait ARQ may work fine where propagation delay is very less for example LAN connections, but performs badly for distant connections like satellite connection.

Go- Back N protocol

Go-Back-N protocol is a sliding window protocol. It is a mechanism to detect and control the error in datalink layer. During transmission of frames between sender and receiver, if a frame is damaged, lost, or an acknowledgement is lost then the action performed by sender and receiver.

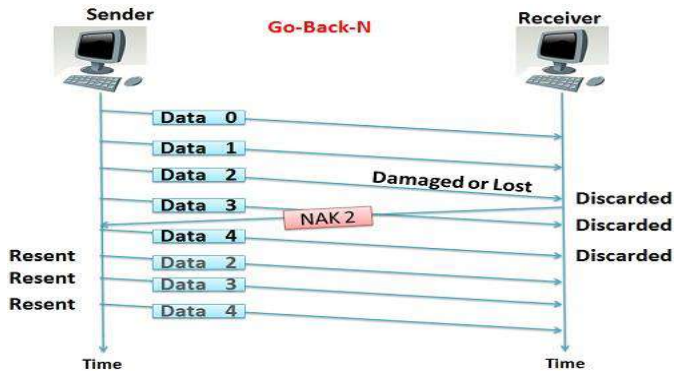


Fig. 2.13 Go-Back N protocol

Selective Repeat protocol

Selective repeat is also the sliding window protocol which detects or corrects the error occurred in datalink layer. The selective repeat protocol retransmits only that frame which is damaged or lost. In selective repeat protocol, the retransmitted frame is received out of sequence. The selective repeat protocol can perform following actions

- The receiver is capable of sorting the frame in a proper sequence, as it receives the retransmitted frame whose sequence is out of order of the receiving frame.
- The sender must be capable of searching the frame for which the NAK has been received.
- The receiver must contain the buffer to store all the previously received frame on hold till the retransmitted frame is sorted and placed in a proper sequence.
- The ACK number, like NAK number, refers to the frame which is lost or damaged.
- It requires the less window size as compared to go-back-n protocol.

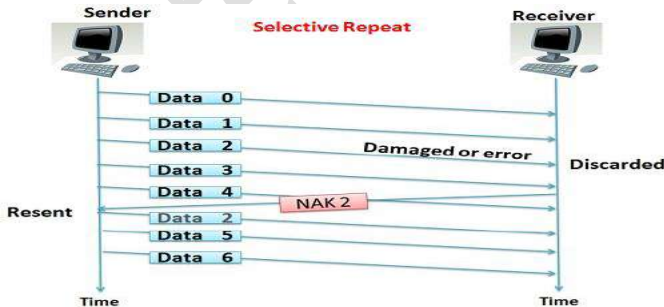


Fig. 2.14 Selective Repeat protocol

HYBRID ARQ

The HARQ is the use of conventional ARQ along with an Error Correction technique called 'Soft Combining', which no longer discards the received bad data (with error).

With the 'Soft Combining' data packets that are not properly decoded are not discarded anymore. The received signal is stored in a 'buffer', and will be combined with next retransmission.

That is, two or more packets received each one with insufficient SNR to allow individual decoding can be combined in such a way that the total signal can be decoded!

The following image explains this procedure. The transmitter sends a package [1]. The package [1] arrives, and is 'OK'. If the package [1] is 'OK' then the receiver sends an 'ACK'.



Fig. 2.15 Transmitter sends a packet-1

The transmission continues, and is sent a package [2]. The package [2] arrives, but let's consider now that it arrives with errors. If the package [2] arrives with errors, the receiver sends a 'NAK'.



Fig. 2.16 Transmitter sends a packet-2

Only now this package [2] (bad) is not thrown away, as it is done in conventional ARQ. Now it is stored in a 'buffer'.

buffer ?

Fig. 2.17 Receiver buffers a packet-2

Continuing, the transmitter sends another package [2.1] that also (let's consider) arrives with errors.



Fig. 2.18 Transmitter sends another packet-2

We have then in a buffer: bad package [2], and another package [2.1] which is also bad. Does by adding (combining) these two packages ([2] + [2.1]) we have the complete information? Yes. So, we send an 'ACK'.

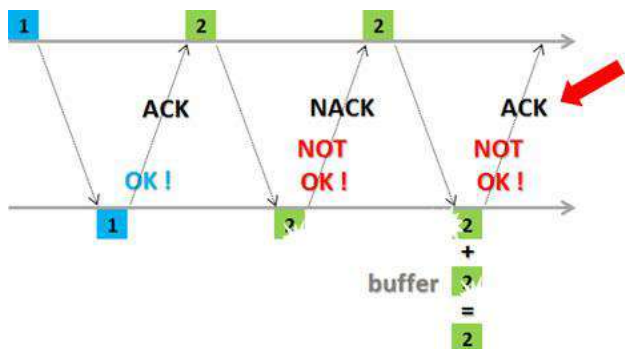


Fig. 2.19 Receiver combining buffers a packet-2 and another packet-2

But if the combination of these two packages still does not give us the complete information, the process must continue - and another 'NACK' is sent.

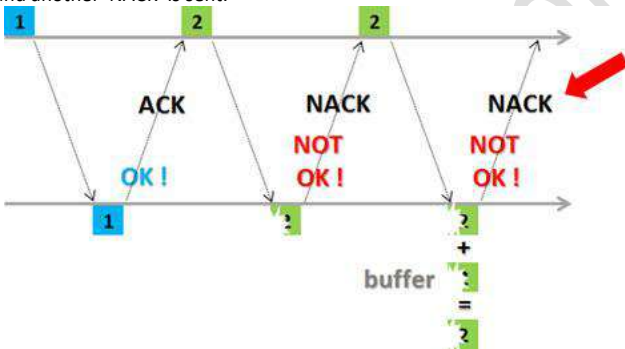


Fig. 2.20 Receiver sends NACK

And there we have another retransmission. Now the transmitter sends a third package [2.2]. Let's consider that now it is 'OK', and the receiver sends an 'ACK'.

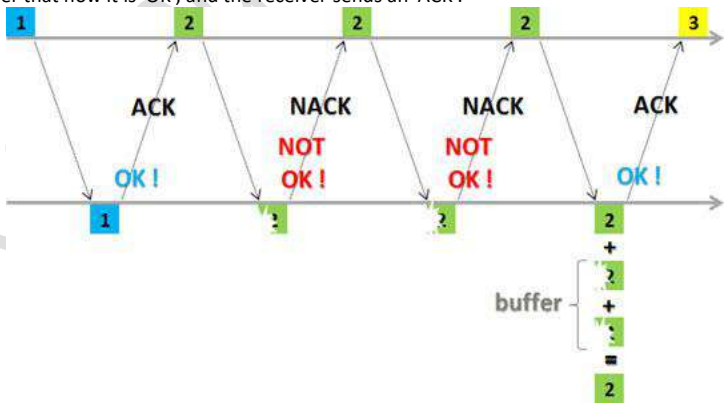


Fig. 2.21 Receiver sends ACK

Here we can see the following: along with the received package [2.2], the receiver also has packages [2] and [2.1] that have not been dropped and are stored in the buffer.

Department of Computer Science and Engineering
CS602 Computer Networks
Subject Notes: UNIT-III

Syllabus: MAC Sub layer: MAC Addressing, Binary Exponential Back-off (BEB) Algorithm, Distributed Random Access Schemes/Contention Schemes: for Data Services (ALOHA and Slotted-ALOHA), for Local-Area Networks (CSMA, CSMA/CD, CSMA/CA), IEEE

Standards 802 series & their variant.

MAC Sublayer

In the seven-layer OSI model of computer networking, media access control (MAC) data communication protocol is a sublayer of the data link layer (layer 2). The MAC sublayer provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, e.g. Ethernet. The hardware that implements the MAC is referred to as a media access controller.

The MAC sublayer acts as an interface between the logical link control (LLC) sublayer and the network's physical layer. The MAC layer emulates a full-duplex logical communication channel in a multi-point network. This channel may provide unicast, multicast or broadcast communication service.

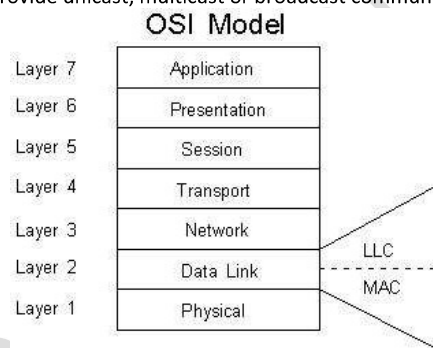


Fig.3.1 MAC Sub Layer

MAC Addressing (Media Access Control address)

In a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's unique hardware number.

In a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

What Is a MAC Address?

The MAC address is a unique value associated with a network adapter. MAC addresses are also known as hardware addresses or physical addresses. They uniquely identify an adapter on a LAN.

MAC addresses are 12-digit hexadecimal numbers (48 bits in length). By convention, MAC addresses are usually written in one of the following two formats:

MM:MM:MM:SS:SS:SS

MM-MM-MM-SS-SS-SS

The first half of a MAC address contains the ID number of the adapter manufacturer. These IDs are regulated by an Internet standards body. The second half of a MAC address represents the serial number assigned to the adapter by the manufacturer.

In the example, 00:A0:C9:14:C8:29 The prefix 00A0C9 indicates the manufacturer is Intel Corporation.

Why MAC Addresses?

Recall that TCP/IP and other mainstream networking architectures generally adopt the OSI model. In this model, network functionality is subdivided into layers. MAC addresses function at the data link layer (layer 2 in the OSI model). They allow computers to uniquely identify themselves on a network at this relatively low level.

MAC vs. IP Addressing

Whereas MAC addressing works at the data link layer, IP addressing functions at the network layer (layer 3). It's a slight oversimplification, but one can think of IP addressing as supporting the software implementation and MAC addresses as supporting the hardware implementation of the network stack. The MAC address generally remains fixed and follows the network device, but the IP address changes as the network device moves from one network to another.

IP networks maintain a mapping between the IP address of a device and its MAC address. This mapping is known as the ARP cache or ARP table. ARP, the Address Resolution Protocol, supports the logic for obtaining this mapping and keeping the cache up to date.

DHCP also usually relies on MAC addresses to manage the unique assignment of IP addresses to devices.

Link MAC Address: <https://www.youtube.com/watch?v=W52Wt1LDweQ>

Binary Exponential Back-off (BEB) Algorithm

In a variety of computer networks, binary exponential back off or truncated binary exponential back off refers to an algorithm used to space out repeated retransmissions of the same block of data, often as part of network congestion avoidance.

Examples are the retransmission of frames in carrier sense multiple access with collision avoidance (CSMA/CA) and carrier sense multiple access with collision detection (CSMA/CD) networks, where this algorithm is part of the channel access method used to send data on these networks. In Ethernet networks, the algorithm is commonly used to schedule retransmissions after collisions. The retransmission is delayed by an amount of time derived from the slot time and the number of attempts to retransmit.

After c collisions, a random number of slot times between 0 and $2^c - 1$ is chosen. For the first collision, each sender will wait 0 or 1 slot times. After the second collision, the senders will wait anywhere from 0 to 3 slot times (inclusive). After the third collision, the senders will wait anywhere from 0 to 7 slot times (inclusive), and so forth. As the number of retransmission attempts increases, the number of possibilities for delay increases exponentially.

Link: <https://www.youtube.com/watch?v=WeGNeUHYv5g>

Distributed Random Access Schemes/Contention Schemes: for Data Services (ALOHA and Slotted ALOHA)

ALOHA: ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. The original system used for ground-based radio broadcasting, but the system has been implemented in satellite communication systems.

A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.

Aloha means "Hello". Aloha is a multiple access protocol at the datalink layer and proposes how multiple terminals access the medium without interference or collision. A scientist developed a protocol that would increase the capacity of aloha two-fold. The Slotted Aloha protocol involves dividing the time interval into discrete slots and each slot interval corresponds to the time period of one frame. This method requires synchronization between the sending nodes to prevent collisions.

There are two different versions

Types of ALOHA:

- (i) Pure ALOHA
- (ii) Slotted ALOHA

(i) Pure ALOHA

- In pure ALOHA, the stations transmit frames whenever they have data to send.
- When two or more stations transmit simultaneously, there is collision and the frames are destroyed.
- In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.
- If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.
- If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.
- Therefore, pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.

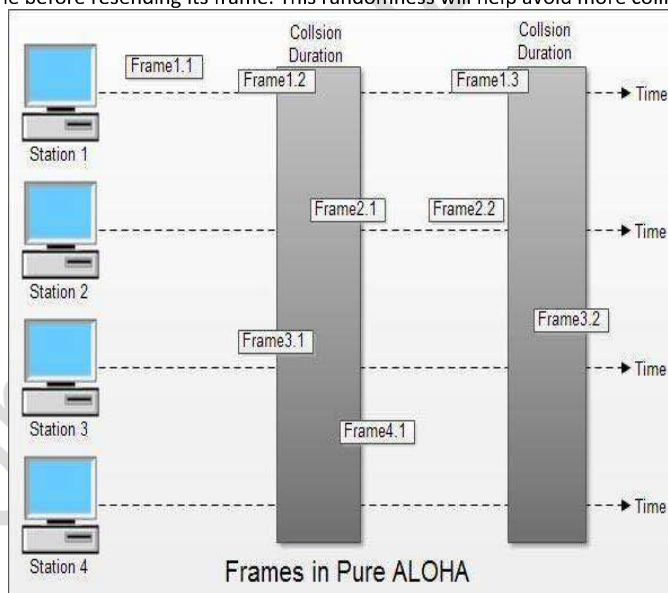


Fig 3.2 Pure ALOHA

(ii) Slotted ALOHA

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
- In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.
- The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.
- In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot i.e. it misses the time slot then the station has to wait until the beginning of the next time slot.

- In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot.
- Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.

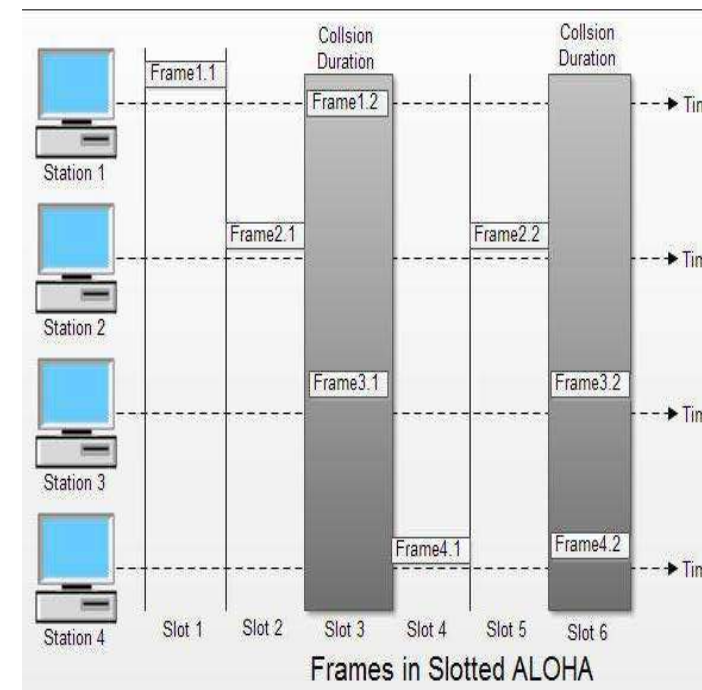


Fig 3.3 Slotted ALOHA

Link ALOHA: <https://www.youtube.com/watch?v=c39k2clZU74>

For Local-Area Networks (CSMA, CSMA/CD, CSMA/CA)

Carrier sense multiple access (CSMA) is a probabilistic media access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium, such as an electrical bus, or a band of the electromagnetic spectrum.

Carrier sense means that a transmitter uses feedback from a receiver to determine whether another transmission is in progress before initiating a transmission. That is, it tries to detect the presence of a carrier wave from another station before attempting to transmit. If a carrier is sensed, the station waits for the transmission in progress to finish before initiating its own transmission. In other words, CSMA is based on the principle "sense before transmit" or "listen before talk".

Multiple access means that multiple stations send and receive on the medium. Transmissions by one node are generally received by all other stations connected to the medium.

CSMA protocol was developed to overcome the problem found in ALOHA i.e. to minimize the chances of collision, so as to improve the performance. CSMA protocol is based on the principle of 'carrier sense'. The station senses the carrier or channel before transmitting a frame. It means the station checks the state of channel, whether it is idle or busy.

Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it.

The chances of collision still exist because of propagation delay. The frame transmitted by one station takes some time to reach other stations. In the meantime, other stations may sense the channel to be idle and transmit their frames. This results in the collision.

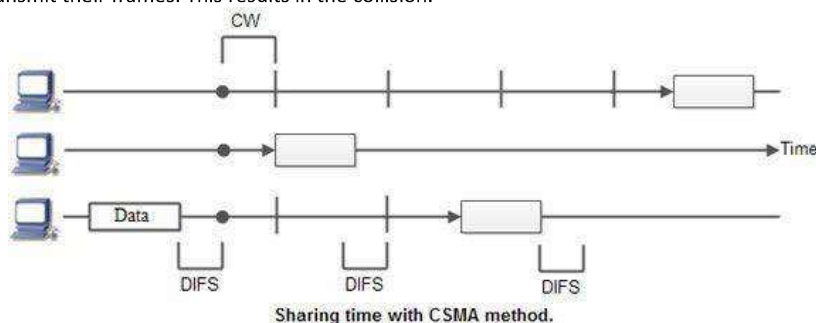


Fig 3.4 CSMA

There Are Three Different Type of CSMA Protocols

- (i) 1-persistent CSMA
- (ii) Non- Persistent CSMA
- (iii) p-persistent CSMA

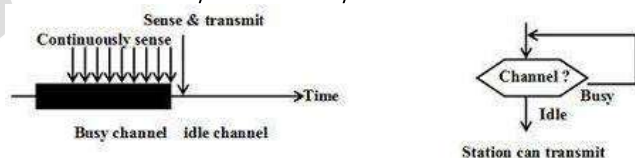
(i) 1-persistent CSMA

- In this method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy.
- If the channel is busy, the station waits until it becomes idle.
- When the station detects an idle-channel, it immediately transmits the frame with probability 1. Hence it is called 1-persistent CSMA.
- This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.
- When the collision occurs, the stations wait a random amount of time and start all over again.

Drawback of 1-persistent

The propagation delay time greatly affects this protocol. Let us suppose, just after the station 1 begins its transmission, station 2 also became ready to send its data and senses the channel. If the station 1 signal has not yet reached station 2, station 2 will sense the channel to be idle and will begin its transmission. This will result in collision.

Even if propagation delay time is zero, collision will still occur. If two stations became ready in the middle of third station's transmission, both stations will wait until the transmission of first station ends and then both will begin their transmission exactly simultaneously. This will also result in collision.



1-persistent CSMA

Fig 3.5 1-persistent CSMA

(ii) Non-persistent CSMA

- In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval of time.

- After this time, it again checks the status of the channel and if the channel is free it will transmit.
- A station that has a frame to send senses the channel.
- If the channel is idle, it sends immediately.
- If the channel is busy, it waits a random amount of time and then senses the channel again.
- In non-persistent CSMA the station does not continuously sense the channel for the purpose of capturing it when it detects the end of previous transmission.

Advantage of non-persistent

- It reduces the chance of collision because the stations wait a random amount of time. It is unlikely that two or more stations will wait for same amount of time and will retransmit at the same time.

Disadvantage of non-persistent

- It reduces the efficiency of network because the channel remains idle when there may be stations with frames to send. This is due to the fact that the stations wait a random amount of time after the collision.

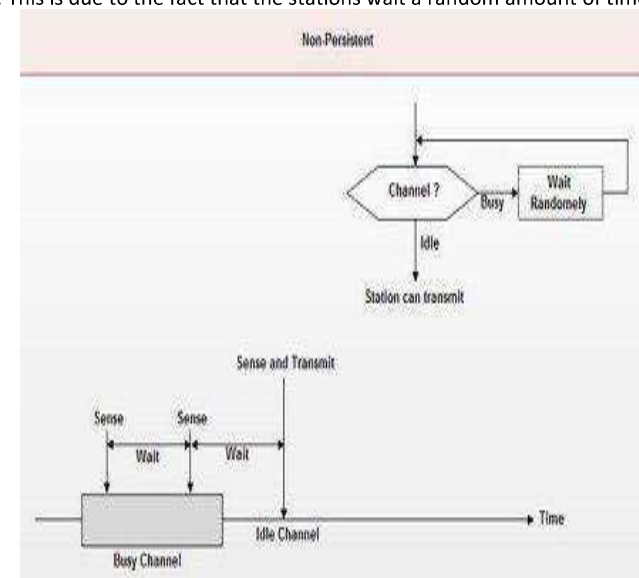


Fig 3.6 Non-persistent CSMA

(iii) p-persistent CSMA

- This method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.
- Whenever a station becomes ready to send, it senses the channel.
- If channel is busy, station waits until next slot.
- If channel is idle, it transmits with a probability p .
- With the probability $q=1-p$, the station then waits for the beginning of the next time slot.
- If the next slot is also idle, it either transmits or waits again with probabilities p and q .
- This process is repeated till either frame has been transmitted or another station has begun transmitting.

- In case of the transmission by another station, the station acts as though a collision has occurred and it waits a random amount of time and starts again.

Advantage of p-persistent

- It reduces the chance of collision and improves the efficiency of the network.

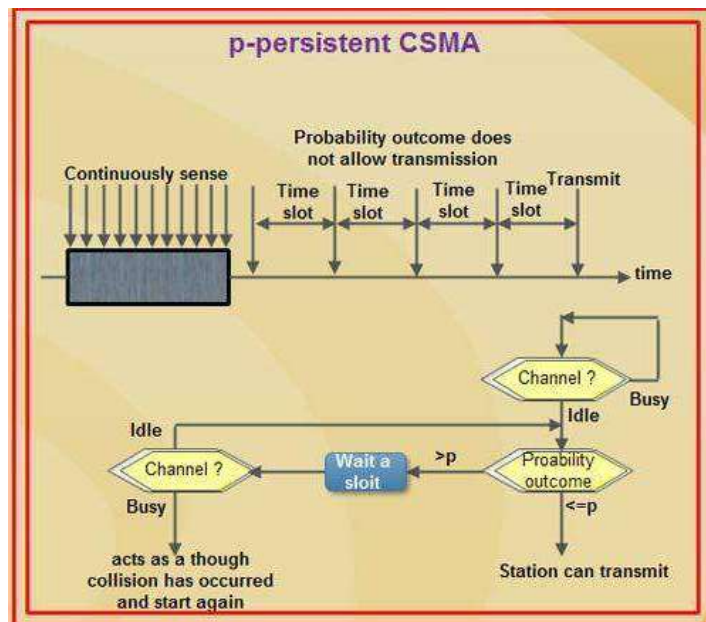


Fig 3.7 p-persistent CSMA

CSMA/CD - Carrier Sense Multiple Access / Collision Detection

To reduce the impact of collisions on the network performance, Ethernet uses an algorithm called CSMA with Collision Detection (CSMA / CD): CSMA/CD is a protocol in which the station senses the carrier or channel before transmitting frame just as in persistent and non-persistent CSMA. If the channel is busy, the station waits. It listens at the same time on communication media to ensure that there is no collision with a packet sent by another station. In a collision, the issuer immediately cancel the sending of the package. This allows to limit the duration of collisions: we do not waste time to send a packet complete if it detects a collision. After a collision, the transmitter waits again silence and again, he continued his hold for a random number; but this time the random number is nearly double the previous one: it is this called back-off (that is to say, the "decline") exponential. In fact, the window collision is simply doubled (unless it has already reached a maximum). From a packet is transmitted successfully, the window will return to its original size.

Again, this is what we do naturally in a meeting room if many people speak exactly the same time, they are realizing account immediately (as they listen at the same time they speak), and they interrupt without completing their sentence. After a while, one of them speaks again. If a new collision occurs, the two are interrupted again and tend to wait a little longer before speaking again.

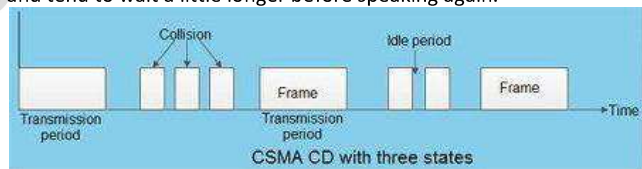


Fig 3.8 CSMA/CD

CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance

CSMA/CA protocol is used in wireless networks because they cannot detect the collision so the only solution is collision avoidance.

- CSMA/CA avoids the collisions using three basic techniques.

- Interframe space
- Contention window
- Acknowledgements

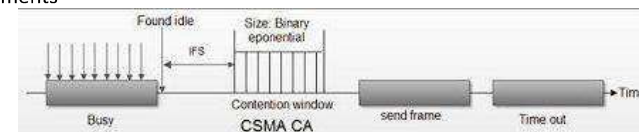


Fig 3.9 CSMA/CA

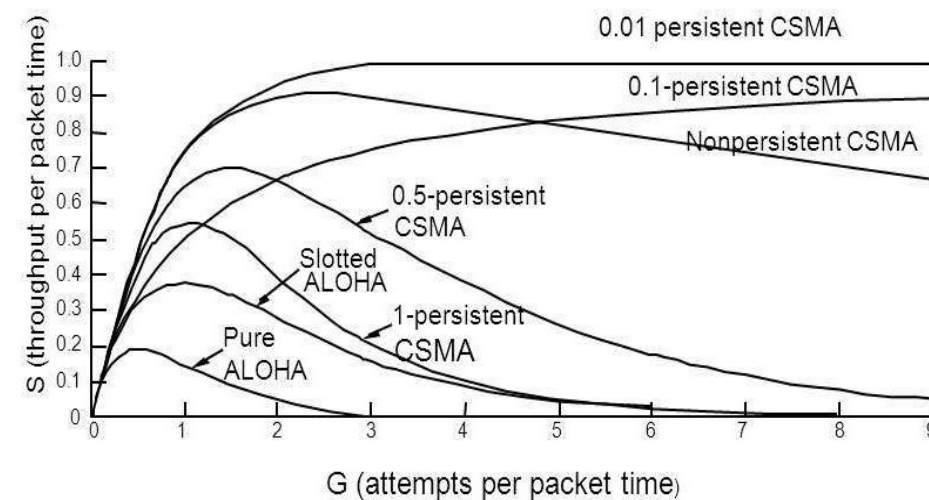
Comparison between all with an BAR Chart

Fig 3.10 Comparison between all with an BAR Chart

1. Interframe Space (IFS)

- Whenever the channel is found idle, the station does not transmit immediately. It waits for a period of time called interframe space (IFS).
- When channel is sensed to be idle, it may be possible that same distant station may have already started transmitting and the signal of that distant station has not yet reached other stations.
- Therefore the purpose of IFS time is to allow this transmitted signal to reach other stations.
- If after this IFS time, the channel is still idle, the station can send, but it still needs to wait a time equal to contention time.
- IFS variable can also be used to define the priority of a station or a frame.

2. Contention Window

- Contention window is an amount of time divided into slots.
- A station that is ready to send chooses a random number of slots as its wait time.
- The number of slots in the window changes according to the binary exponential back-off strategy. It means that it is set of one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.
- This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station.
- In contention window the station needs to sense the channel after each time slot.

- If the station finds the channel busy, it does not restart the process. It just stops the timer & restarts it when the channel is sensed as idle.

3. Acknowledgement

- Despite all the precautions, collisions may occur and destroy the data.
- The positive acknowledgment and the time-out timer can help guarantee that receiver has received the frame.

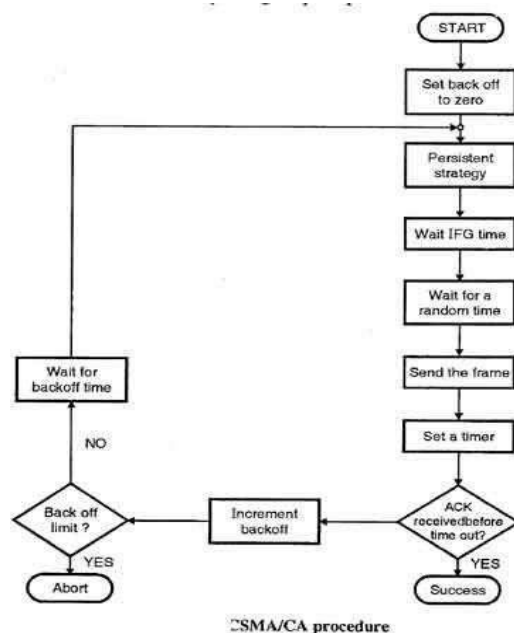


Fig 3.11 Flow Chart of CSMA/CA

LINK: <https://www.youtube.com/watch?v=74zIRH-bj2c>

Hidden Node Problem

In the case of wireless network it is possible that A is sending a message to B, but C is out of its range and hence while "listening" on the network it will find the network to be free and might try to send packets to B at the same time as A. So, there will be a collision at B. The problem can be looked upon as if A and C are hidden from each other. Hence it is called the "hidden node problem".

Exposed Node Problem

If C is transmitting a message to D and B wants to transmit a message to A, B will find the network to be busy as B hears C transmitting. Even if B would have transmitted to A, it would not have been a problem at A or D. CSMA/CD would not allow it to transmit message to A, while the two transmissions could have gone in parallel.

IEEE Standards 802 series & their variant

802.2 Logical Link Control

The technical definition for 802.2 is "the standard for the upper Data Link Layer sublayer also known as the Logical Link Control layer. It is used with the 802.3, 802.4, and 802.5 standards (lower DL sublayers)."

802.2 "specifies the general interface between the network layer (IP, IPX, etc) and the data link layer (Ethernet, Token Ring, etc).

Basically, think of the 802.2 as the "translator" for the Data Link Layer. 802.2 is concerned with managing traffic over the physical network. It is responsible for flow and error control. The Data Link Layer wants to send some data over the network, 802.2 Logical Link Control helps make this possible. It also helps by identifying the line protocol, like NetBIOS, or Netware.

The LLC acts like a software bus allowing multiple higher layer protocols to access one or more lower layer networks. For example, if you have a server with multiple network interface cards, the LLC will forward packets from those upper layer protocols to the appropriate network interface. This allows the upper layer protocols to not need specific knowledge of the lower layer networks in use.

802.3 Ethernet

802.3 is the standard which Ethernet operates by. It is the standard for CSMA/CD (Carrier Sense Multiple Access with Collision Detection). This standard encompasses both the MAC and Physical Layer standards.

CSMA/CD is what Ethernet uses to control access to the network medium (network cable). If there is no data, any node may attempt to transmit, if the nodes detect a collision, both stop transmitting and wait a random amount of time before retransmitting the data.

The original 802.3 standard is 10 Mbps (Megabits per second). 802.3u defined the 100 Mbps (Fast Ethernet) standard, 802.3z/802.3ab defined 1000 Mbps Gigabit Ethernet, and 802.3ae define 10 Gigabit Ethernet.

Commonly, Ethernet networks transmit data in packets, or small bits of information. A packet can be a minimum size of 72 bytes or a maximum of 1518 bytes.

The most common topology for Ethernet is the star topology.

802.5 Token Ring

Token ring is designed to use the ring topology and utilizes a token to control the transmission of data on the network.

The token is a special frame which is designed to travel from node to node around the ring. When it does not have any data attached to it, a node on the network can modify the frame, attach its data and transmit. Each node on the network checks the token as it passes to see if the data is intended for that node, if it is; it accepts the data and transmits a new token. If it is not intended for that node, it retransmits the token on to the next node.

The token ring network is designed in such a way that each node on the network is guaranteed access to the token at some point. This equalizes the data transfer on the network. This is different from an Ethernet network where each workstation has equal access to grab the available bandwidth, with the possible of a node using more bandwidth than other nodes.

Originally, token ring operated at a speed of about 4 Mbps and 16 Mbps. 802.5t allows for 100 Mbps speeds and 802.5v provides for 1 Gbps over fiber.

Token ring can be run over a star topology as well as the ring topology.

There are three major cable types for token ring: Unshielded twisted pair (UTP), Shielded twisted pair (STP), and fiber.

Token ring utilizes a Multi-station Access Unit (MAU) as a central wiring hub. This is also sometimes called a MSAU when referring to token ring networks.

802.11 Wireless Network Standards

802.11 is the collection of standards setup for wireless networking. You are probably familiar with the three popular standards: 802.11a, 802.11b, 802.11g and latest one is 802.11n. Each standard uses a frequency to connect to the network and has a defined upper limit for data transfer speeds.

802.11a was one of the first wireless standards. 802.11a operates in the 5GHz radio band and can achieve a maximum of 54Mbps. Wasn't as popular as the 802.11b standard due to higher prices and lower range.

802.11b operates in the 2.4GHz band and supports up to 11 Mbps. Range of up to several hundred feet in theory. The first real consumer option for wireless and very popular.

802.11g is a standard in the 2.4GHz band operating at 54Mbps. Since it operates in the same band as 802.11b, 802.11g is compatible with 802.11b equipment. 802.11a is not directly compatible with 802.11b or 802.11g since it operates in a different band.

Wireless LANs primarily use CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance. It has a "listen before talk" method of minimizing collisions on the wireless network. This results in less need for retransmitting data.

Wireless standards operate within a wireless topology.