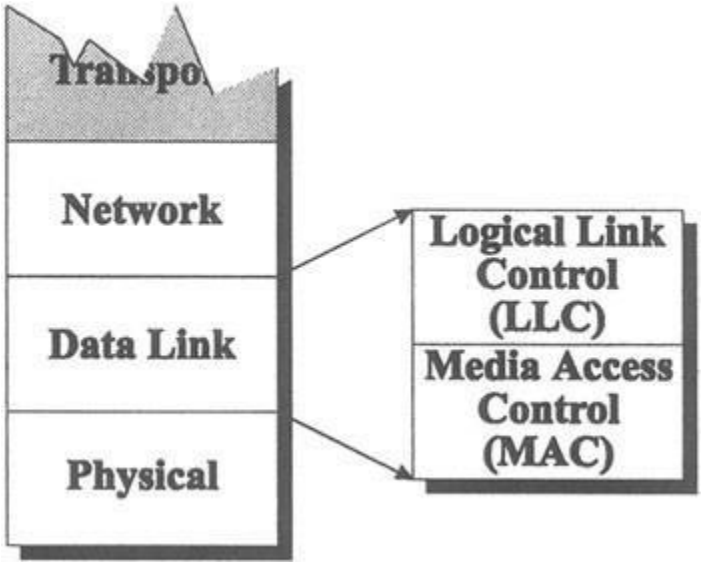
Unit 3: Data Link Layer

Functions of Data Link Layer:

The data link layer transforms the physical layer, a raw transmission facility, to a link responsible for node-to-node (hop-to-hop) communication. Specific responsibilities of the data link layer include framing, addressing, flow control, error control, and media access control. The data link layer divides the stream of bits received from the network layer into manageable data units called frames. The data link layer adds a header to the frame to define the addresses of the sender and receiver of the frame. If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver. The data link layer also adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged, duplicate, or lost frames. When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Overview of Logical Link Control (LLC) and Media Access Control (MAC):

The data link layer is divided into two sublayers:

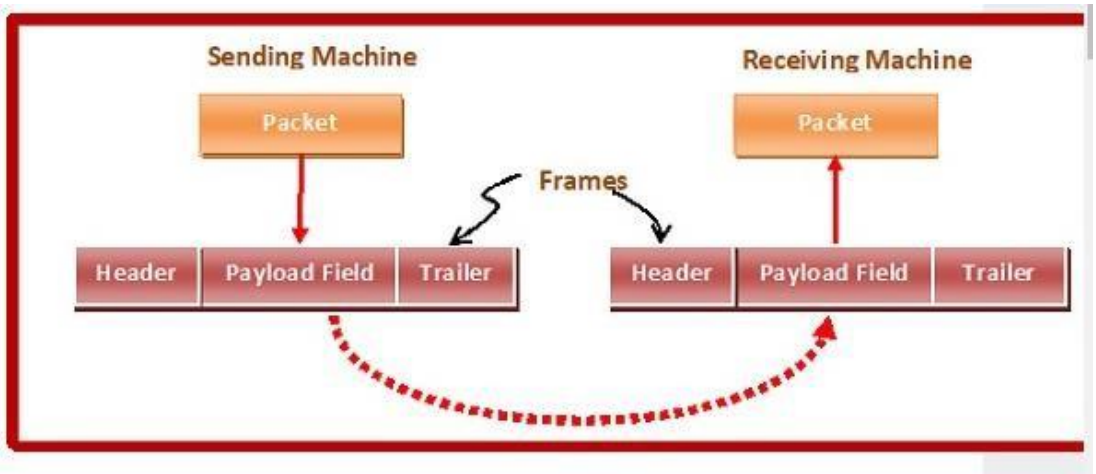


- The LLC sublayer acts as an interface between the media access control (MAC) sublayer and the network layer. Logical Link Control (LLC) sublayer provides the logic for the data link. The LLC sublayer provides multiplexing mechanisms that make it possible for several network protocols to coexist within a multipoint network and to be transported over the same network medium. Thus, it controls the synchronization, flow control, and error checking functions of the data link layer.
- Media Access Control (MAC) sublayer provides control for accessing the transmission medium. It is responsible for moving data packets from one network interface to another, across a shared transmission medium. Physical addressing is handled at the MAC sublayer. When sending data to another device on the network, the MAC sublayer encapsulates higher-level frames into frames appropriate for the transmission medium, adds a frame check sequence to identify transmission

errors, and then forwards the data to the physical layer. Additionally, the MAC is also responsible for compensating for collisions by initiating retransmission if a jam signal is detected.

Framing:

In the physical layer, data transmission involves synchronized transmission of bits from the source to the destination. The data link layer packs these bits into frames. Data-link layer takes the packets from the Network Layer and encapsulates them into frames. If the frame size becomes too large, then the packet may be divided into small sized frames. Smaller sized frames make flow control and error control more efficient. Then, it sends each frame bit-by-bit on the hardware. At receiver's end, data link layer picks up signals from hardware and assembles them into frames.



Parts of a Frame

A frame has the following parts −

Frame Header − It contains the source and the destination addresses of the frame.

Payload field − It contains the message to be delivered.

Trailer − It contains the error detection and error correction bits.

Flag − It marks the beginning and end of the frame.

Types of Framing

Framing can be of two types, fixed sized framing and variable sized framing.

Fixed-sized Framing

Here the size of the frame is fixed and so the frame length acts as delimiter of the frame. Consequently, it does not require additional boundary bits to identify the start and end of the frame.

Example − ATM cells.

Variable – Sized Framing

Here, the size of each frame to be transmitted may be different. So additional mechanisms are kept to mark the end of one frame and the beginning of the next frame.

It is used in local area networks.

Flow Control Mechanisms:

Flow control coordinates the amount of data that can be sent before receiving an acknowledgment and is one of the most important duties of the data link layer. In most protocols, flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver. The flow of data must not be allowed to overwhelm the receiver. Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data. The receiving device must be able to inform the sending device before those limits are reached and to request that the transmitting device send fewer frames or stop temporarily. Incoming data must be checked and processed before they can be used. The rate of such processing is often slower than the rate of transmission. For this reason, each receiving device has a block of memory, called a buffer, reserved for storing incoming data until they are processed. If the buffer begins to fill up, the receiver must be able to tell the sender to halt transmission until it is once again able to receive.

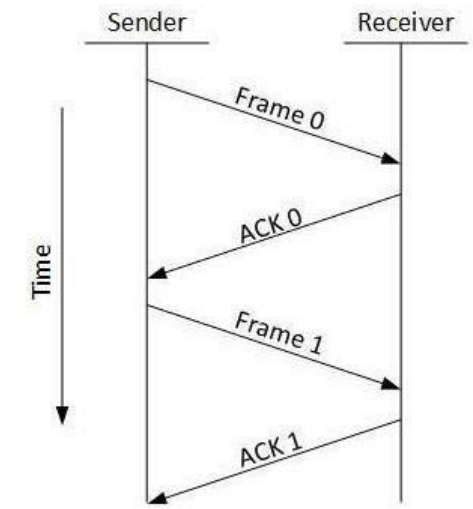
When a data frame is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. If sender is sending too fast, the receiver may be overloaded and data may be lost.

Two types of mechanisms can be deployed to control the flow:

- A simple stop and wait Protocol
- Sliding Window Protocol

<u>Simplex Stop and Wait</u>

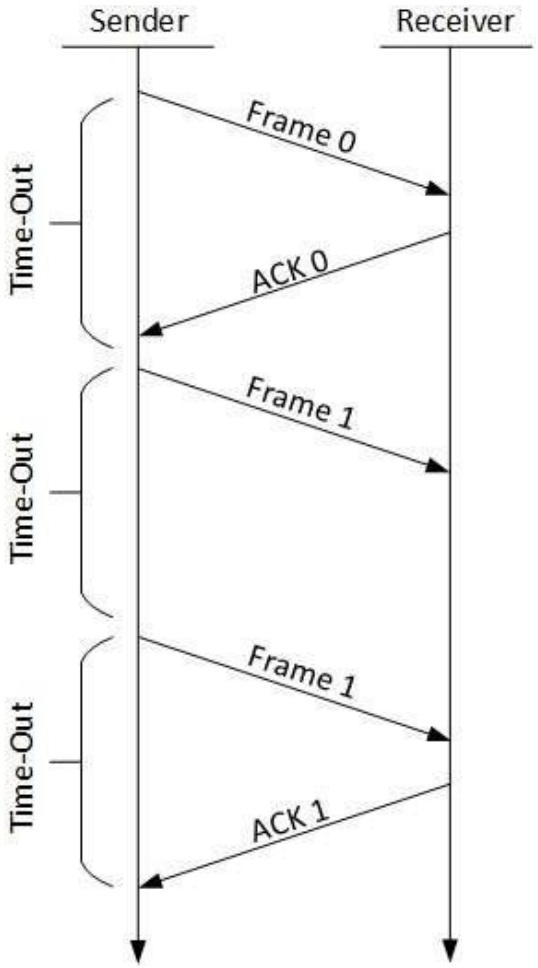
This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received. The sender sends the next frame only when it has received a positive acknowledgement from the receiver that it is available for further data processing. Data transmission is one directional, but must have bidirectional line.



Stop and Wait ARQ

The following transition may occur in Stop-and-Wait ARQ:

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.



Sliding Window

In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible. In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver. The term sliding window refers to the imaginary boxes to hold frames. Sliding window method is also known as windowing. In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window. The size of the sending window determines the sequence number of the outbound frames. The size of the receiving window is the maximum number of frames that the receiver can accept at a time. It determines the maximum number of frames that the sender can send before receiving acknowledgment.

The types of sliding window protocol include:

- A One Bit Sliding Window Protocol
- A Protocol Using Go Back N
- A Protocol Using Selective Repeat

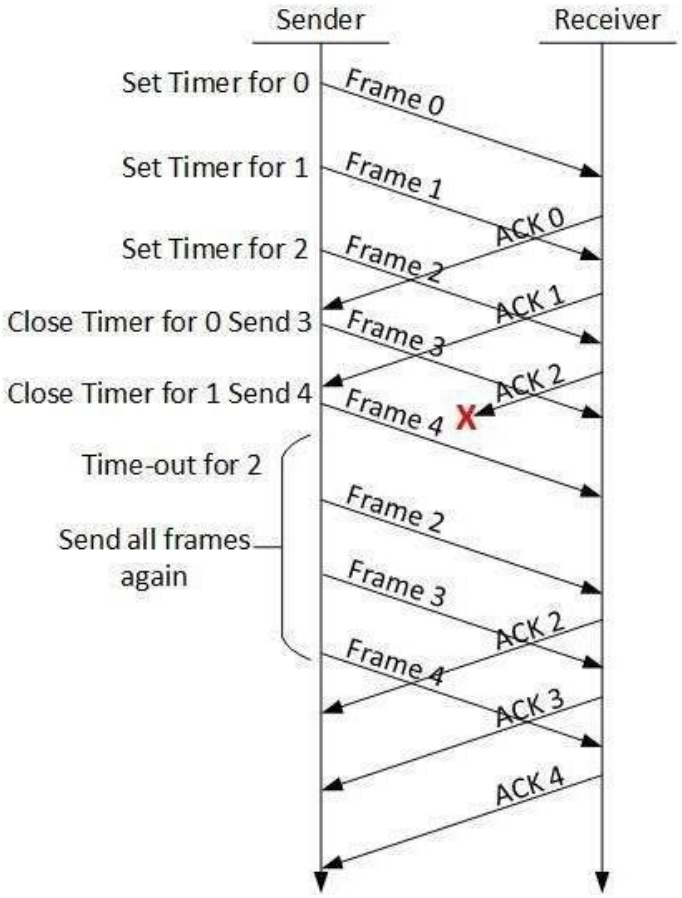
Note: ARQ (Automatic Repeat Request) is designed for noisy channels.

One Bit sliding window protocol:

In one – bit sliding window protocol, the size of the window is 1. So, the sender transmits a frame, waits for its acknowledgment, then transmits the next frame. Thus, it uses the concept of stop and wait protocol. This protocol provides for full – duplex communications. Hence, the acknowledgment is attached along with the next data frame to be sent called piggybacking. So, it is better compared to stop and wait due to full duplex communications.

Go-Back-N ARQ:

In this protocol, we can send several frames before receiving acknowledgements; we keep a copy of these frames until the acknowledgements arrive. Stop and wait mechanism does not utilize the resources at their best. When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N method, both sender and receiver maintain a window.



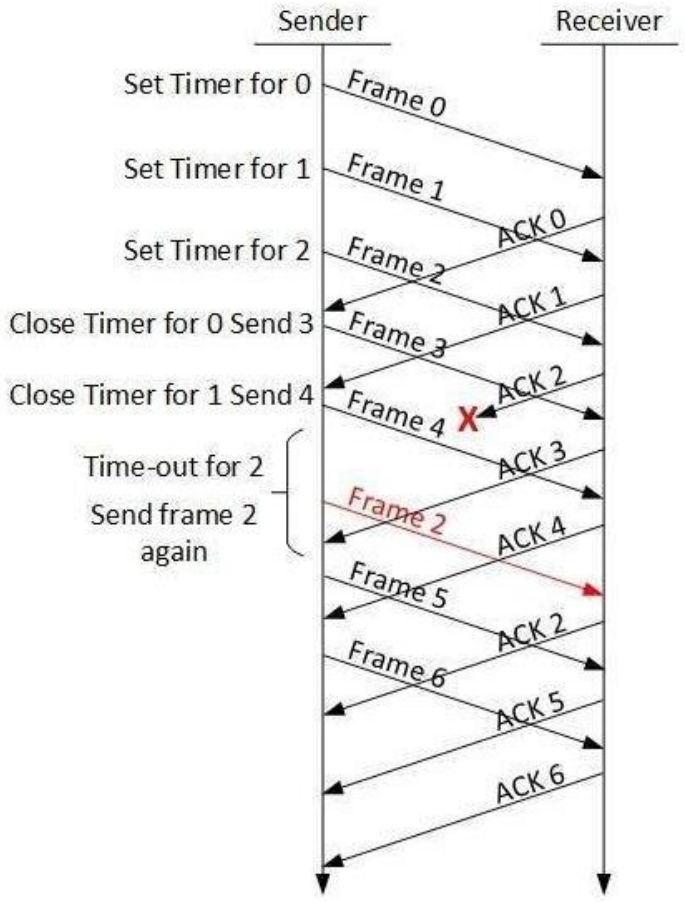
The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames.

If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

Selective Repeat ARQ:

In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.



In Selective-Repeat, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged. The sender in this case, sends only packet for which NACK is received.

Error Detection and Correction Techniques:

Networks must be able to transfer data from one device to another with acceptable accuracy. For most applications, a system must guarantee that the data received are identical to the data transmitted. Any time data are transmitted from one node to the next, they can become corrupted in passage. Many factors can alter one or more bits of a message. Some applications require a mechanism for detecting and correcting errors.

Some applications can tolerate a small level of error. For example, random errors in audio or video transmissions may be tolerable, but when we transfer text, we expect a very high level of accuracy.

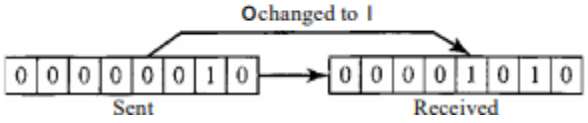
Types of Errors:

Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interference can change the shape of the signal. In a single-bit error, a 0 is changed to a 1 or a 1 to a 0. In a burst error, multiple bits are changed.

Single-Bit Error:

The term single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1.

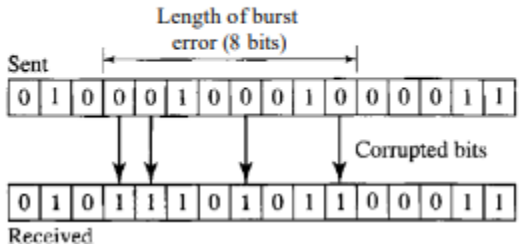
Single-bit error



Burst Error:

The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

Burst error of length 8



A burst error is more likely to occur than a single-bit error. The duration of noise is normally longer than the duration of 1 bit, which means that when noise affects data, it affects a set of bits. The number of bits affected depends on the data rate and duration of noise.

Redundancy

The central concept in detecting or correcting errors is redundancy. To be able to detect or correct errors, we need to send some extra bits with our data. These redundant bits are added by the sender and removed by the receiver. Their presence allows the receiver to detect or correct corrupted bits.

Detection Versus Correction

The correction of errors is more difficult than the detection. In error detection, we are looking only to see if any error has occurred. The answer is a simple yes or no. We are not even interested in the number of errors. A single-bit error is the same for us as a burst error. In error correction, we need to know the exact number of bits that are corrupted and more importantly, their location in the message. The number of the errors and the size of the message are important factors. If we need to correct one single error in an 8-bit data unit, we need to consider eight possible error locations; if we need to correct two errors in a data unit of the same size, we need to consider 28 possibilities.

Forward Error Correction Versus Retransmission

There are two main methods of error correction. Forward error correction is the process in which the receiver tries to guess the message by using redundant bits. This is possible if the number of errors is small. Correction by retransmission is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message. Resending is repeated until a message arrives that the receiver believes is error-free.

Error Detecting Codes

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message.

Some popular techniques for error detection are:

- Parity
- Checksum
- Cyclic redundancy check

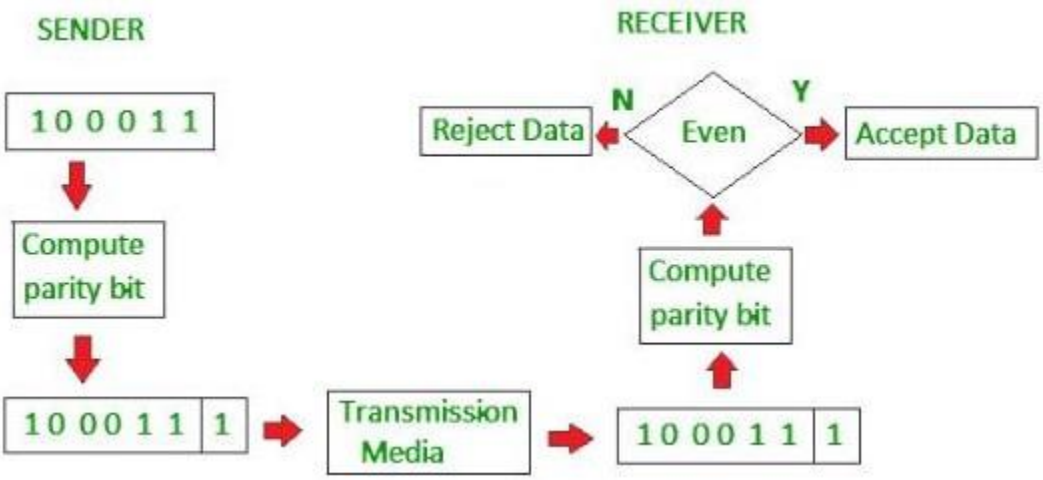
Parity check

The most common and least expensive mechanism for error- detection is the parity check. The parity check is done by adding an extra bit, called parity bit to the data to make a number of 1s either even in case of even parity or odd in case of odd parity. While creating a frame, the sender counts the number of 1s in it and adds the parity bit in the following way:

- In case of even parity: If a number of 1s is even then parity bit value is 0. If the number of 1s is odd then parity bit value is 1.
- In case of odd parity: If a number of 1s is odd then parity bit value is 0. If a number of 1s is even then parity bit value is 1.

On receiving a frame, the receiver counts the number of 1s in it. In case of even parity check, if the count of 1s is even, the frame is accepted, otherwise, it is rejected. A similar rule is adopted for odd parity check.

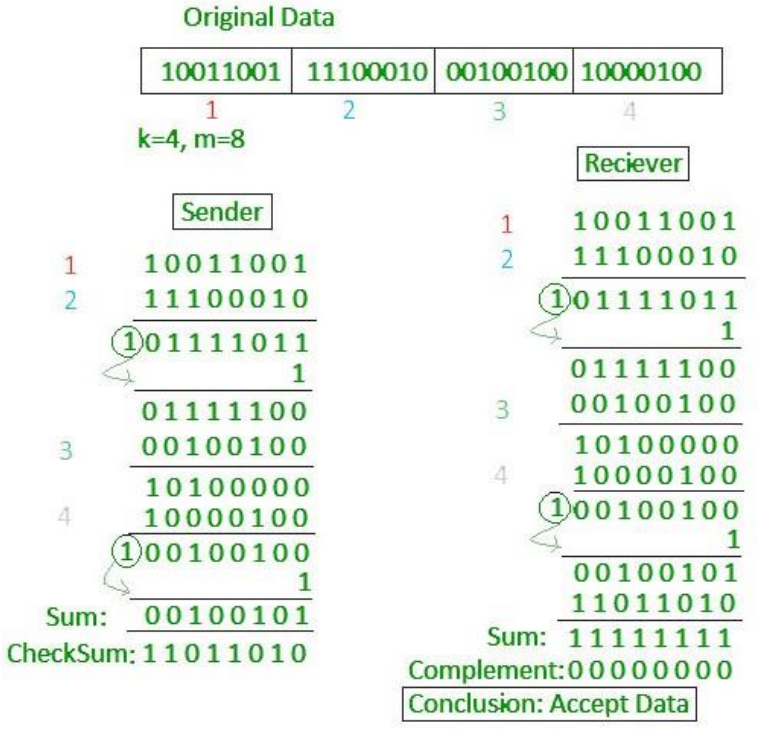
The parity check is suitable for single bit error detection only.



Checksum

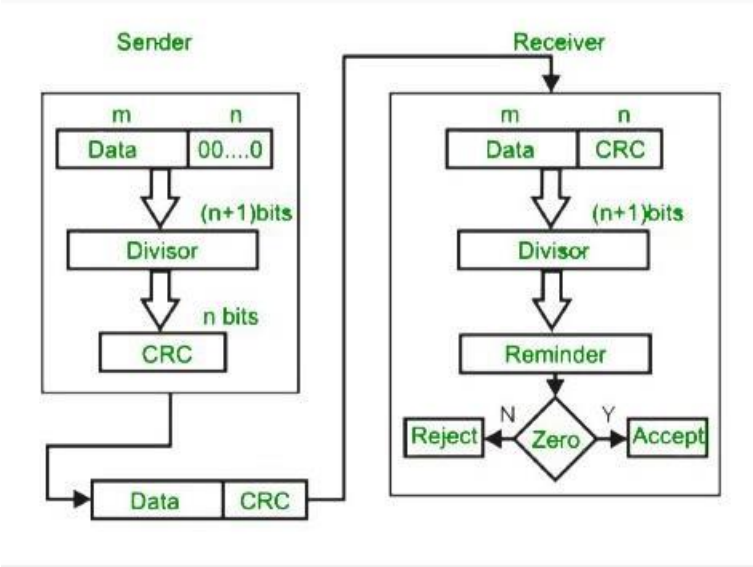
In this error detection scheme, the following procedure is applied:

- Data is divided into fixed sized frames or segments. (k segments each of m bits)
- The sender adds the segments using 1's complement arithmetic to get the sum. It then complements the sum to get the checksum and sends it along with the data frames.
- The receiver adds the incoming segments along with the checksum using 1's complement arithmetic to get the sum and then complements it.
- If the result is zero, the received frames are accepted; otherwise, they are discarded.

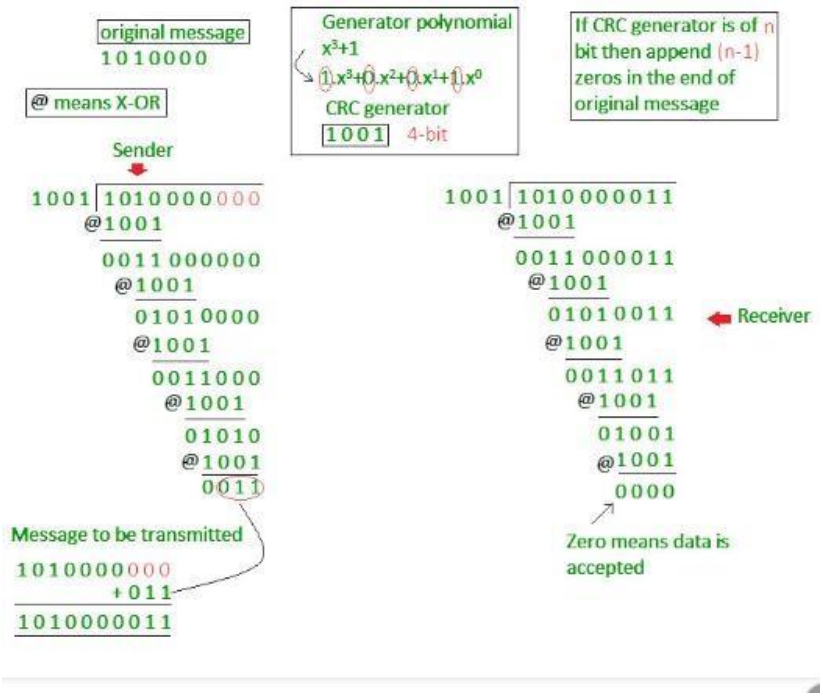


Cyclic Redundancy Check:

A cyclic redundancy check (CRC) is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data. Unlike checksum scheme, which is based on addition, CRC is based on binary division. In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number. At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted. A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.



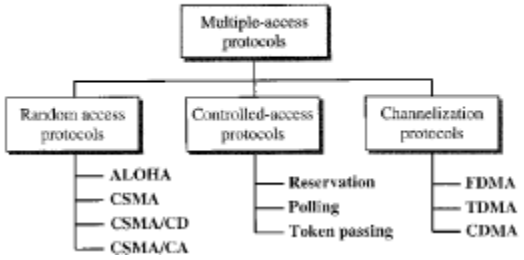
At the sender side, the data unit to be transmitted IS divided by a predetermined divisor (binary number) in order to obtain the remainder. This remainder is called CRC. The CRC has one bit less than the divisor. It means that if CRC is of n bits, divisor is of n+ 1 bit. The sender appends this CRC to the end of data unit such that the resulting data unit becomes exactly divisible by predetermined divisor i.e. remainder becomes zero. At the destination, the incoming data unit i.e. data + CRC is divided by the same number (predetermined binary divisor). If the remainder after division is zero then there is no error in the data unit & receiver accepts it. If remainder after division is not zero, it indicates that the data unit has been damaged in transit and therefore it is rejected. This technique is more powerful than the parity check and checksum error detection.



Multiple Access Protocols (Channel Allocation Techniques):

When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple access protocol to coordinate access to the link. Many formal protocols have been devised to handle access to a shared link. We categorize them into three groups.

Taxonomy of multiple-access protocols discussed in this chapter



Random access:

In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits or does not permit another station to send. At each instance, a station that has to send uses a procedure defined by the protocol to make a decision on whether or not to send. This decision depends on the state of the medium (idle or busy). In other words, each station can transmit when it desires on testing of the state of the medium.

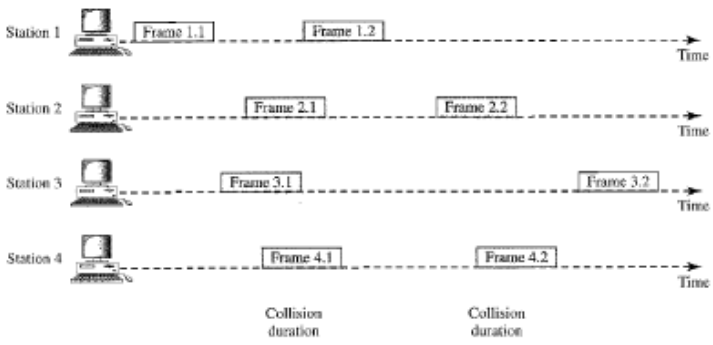
ALOHA:

ALOHA is the earliest random-access method developed for wireless LAN but can be used on any shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision. The data from the two stations collide.

Pure ALOHA:

The idea behind this protocol is that each station sends a frame whenever it has a frame to send. However, since there is only one channel to share, there is possibility of collision between frames from different stations. Even if one bit of a frame coexists on the channel with one bit from another frame, there is a collision and both will be destroyed.

Figure 12.3 *Frames in a pure ALOHA network*



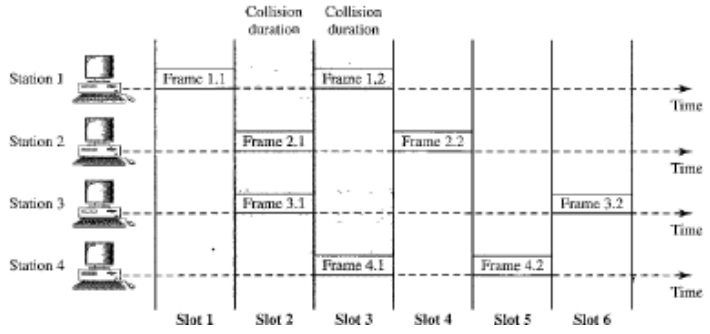
The pure ALOHA protocol relies on acknowledgements from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgement. If the acknowledgement does not arrive after the time out period, the station assumes that the frame (or the acknowledgement) has been destroyed and resends the frame. A collision involves two or more stations. If all these stations try to resend their frames after the time out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions, called back-off time. Since different stations may wait for different amount of time, the probability of further collision decreases.

Slotted ALOHA:

In pure ALOHA, there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished. So, still the collision may occur.

Slotted ALOHA is similar to pure ALOHA, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

Figure 12.6 *Frames in a slotted ALOHA network*



Allowing a station to send only at the beginning of the time slot means that the station sending in the previous slot has finished sending its frame already. However, there is still possibility of collision if two stations try to send at the beginning of the same time slot.

Carrier Sense Multiple Access (CSMA):

The chance of collision can be reduced if a station senses the medium before trying to use it. Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. (listen before talk)

However, there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium. If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA access modes-

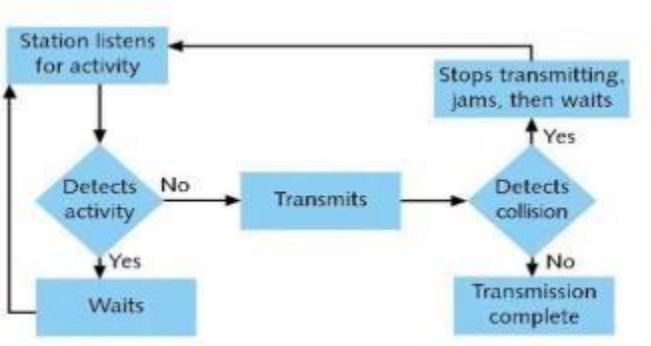
- 1-persistent: The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally (with 1 probability) as soon as the channel gets idle.
- Non-Persistent: The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- P-persistent: The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it sends with p probability. This repeat continues until the frame is sent. It is used in Wi-Fi and packet radio systems.
- O-persistent: Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

Carrier sense multiple access with collision detection (CSMA/CD):

The CSMA method does not specify the procedure following a collision. In Carrier sense multiple access with collision detection method, a station monitors the medium after it sends a frame to see if the

transmission was successful. If so, the transmission is completed. However, if there is a collision, the frame is sent again.

The basic idea behind CSMA/CD is that a station needs to be able to receive while transmitting, to detect a collision. When there is no collision, the station receives one signal; its own signal. When there is a collision, the station receives two signals: its own signal and the signal transmitted by a second station. To distinguish between these two cases, the received signals in these two cases must be significantly different. In other words, the signal from the second station needs to add a significant amount of energy to the one created by the first station.

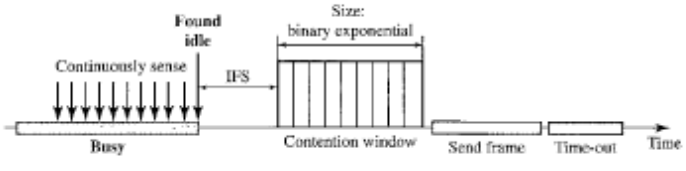


Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA):

The process of collision detection involves sender receiving acknowledgement signals. If there is just one signal (its own), then the data is successfully sent but if there are two signals (its own and the one with which it has collided), then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. The second signal adds significant amount of energy to the first signal. However, this applies only to the wired networks since the received signal has almost the same energy as the sent signal. In wireless networks, much of the sent energy is lost in transmission. The received signal has very little energy. Therefore, a collision may add only 5 to 10 percent additional energy. This is not useful for effective collision detection.

We need to avoid collisions on wireless networks because they cannot be detected. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) was invented for this network. In contrast to the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) protocol, which handles transmissions only after a collision has taken place, CSMA/CA works to avoid collisions prior to their occurrence. Collisions are avoided through the use of CSMA/CA's three strategies as shown in figure below.

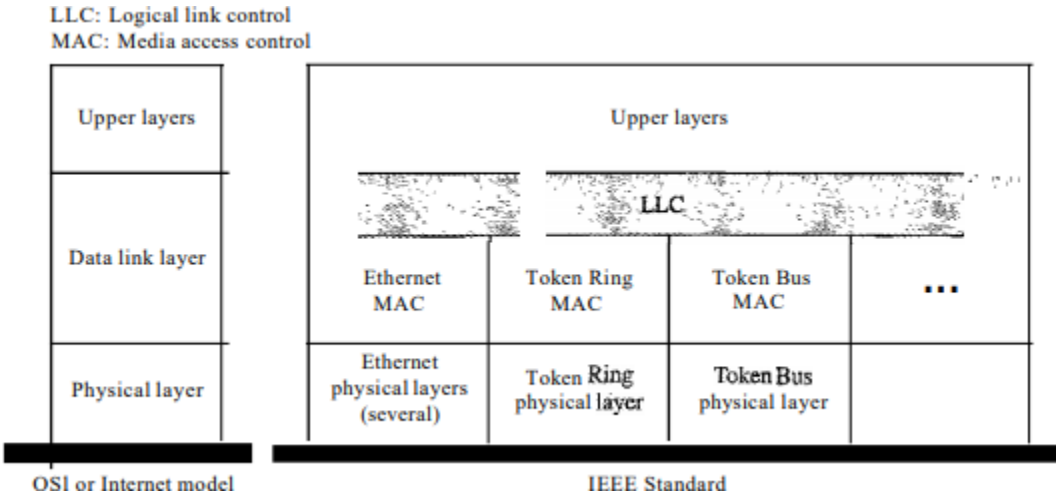
Figure 12.16 *Timing in CSMA/CA*



- Interframe space – Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time, it again checks the medium for being idle. IFS can also be used to define the priority of a station or a frame. Higher the IFS lower is the priority.
- Contention Window –It is the amount of time divided into slots. A station which is ready to send frames chooses random number of slots as wait time.
- Acknowledgement – The positive acknowledgements and time-out timer can help guarantee a successful transmission of the frame.

Overview of IEEE Standard 802:

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 does not seek to replace any part of the OSI or the Internet model. Instead, it is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

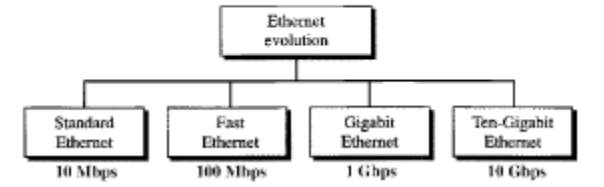


IEEE 802 is comprised of standards with separate working groups that regulate different communication networks, including IEEE 802.1 for bridging (bottom sublayer), 802.2 for Logical link (upper sublayer), 802.3 for Ethernet, 802.5 for token ring, 802.11 for Wi-Fi, 802.15 for Wireless Personal area networks, 802.15.1 for Bluetooth, 802.16 for Wireless Metropolitan Area Networks etc.

Ethernet:

The original Ethernet was created in 1976 and since then, it has gone through four generations.

Ethernet evolution through four generations



Ethernet is a family of computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN). Systems using Ethernet communication divide data streams into packets, which are known as frames. Frames include source and destination address information, as well as mechanisms used to detect errors in transmitted data and retransmission requests. An Ethernet cable is the physical, encased wiring over which the data travels. Compared to wireless LAN technology, Ethernet is typically less vulnerable to disruptions. It can also offer a greater degree of network security and control than wireless technology, as devices must connect using physical cabling, making it difficult for outsiders to access network data or hijack bandwidth for unsanctioned devices.

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. 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.

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. 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.

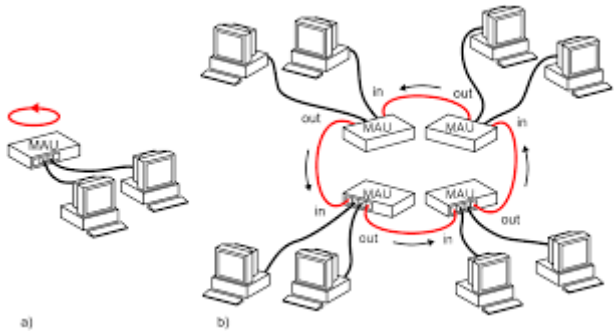


Fig: Two examples of Token Ring networks a) Using a single MAU b) Using several MAUs connected to each other

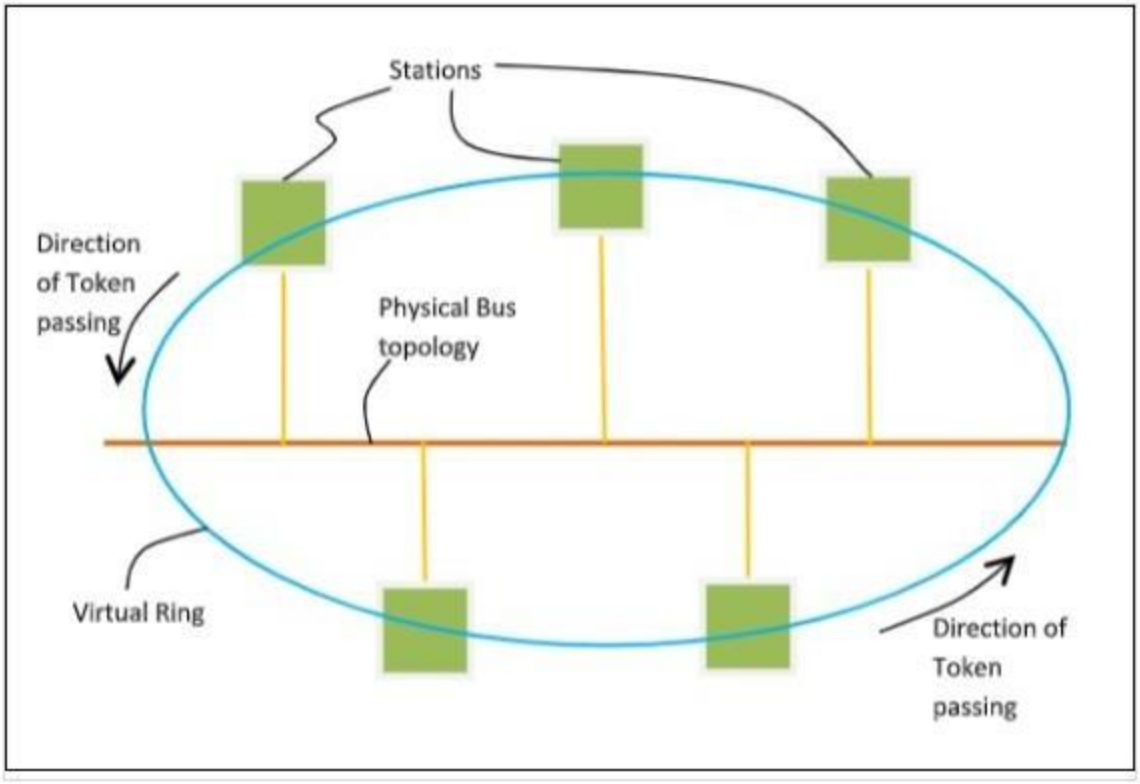
MAU (Media Access Unit)

Token Bus:

Token Bus (IEEE 802.4) is a standard for implementing token ring over virtual ring in LANs. The physical media has a bus or a tree topology and uses coaxial cables. A virtual ring is created with the nodes/stations and the token is passed from one node to the next in a sequence along this virtual ring. Each node knows the address of its preceding station and its succeeding station. A station can only transmit data when it has the token. The working principle of token bus is similar to Token Ring.

Token Passing Mechanism in Token Bus

A token is a small message that circulates among the stations of a computer network providing permission to the stations for transmission. If a station has data to transmit when it receives a token, it sends the data and then passes the token to the next station; otherwise, it simply passes the token to the next station. This is depicted in the following diagram:



Differences between Token Ring and Token Bus

Token Ring	Token Bus
The token is passed over the physical ring formed by the stations and the coaxial cable network.	The token is passed along the virtual ring of stations connected to a LAN.
The stations are connected by ring topology, or sometimes star topology.	The underlying topology that connects the stations is either bus or tree topology.
It is defined by IEEE 802.5 standard.	It is defined by IEEE 802.4 standard.
The maximum time for a token to reach a station can be calculated here.	It is not feasible to calculate the time for token transfer.

Wireless LANs:

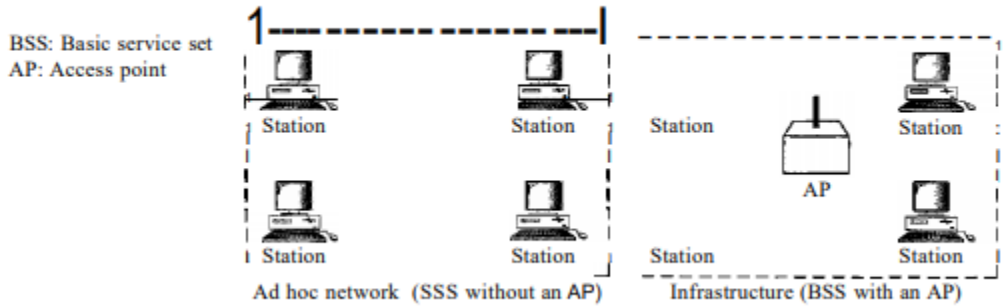
IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

Basic Service Set

IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made up of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). Figure below shows two sets in this standard.

Figure 14.1 *Basic service sets (BSSs)*

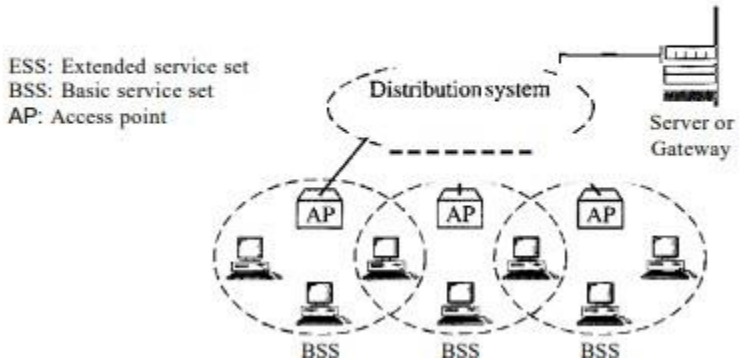


The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture. In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an infrastructure network.

Extended Service Set

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.

Extended service sets (ESSs)



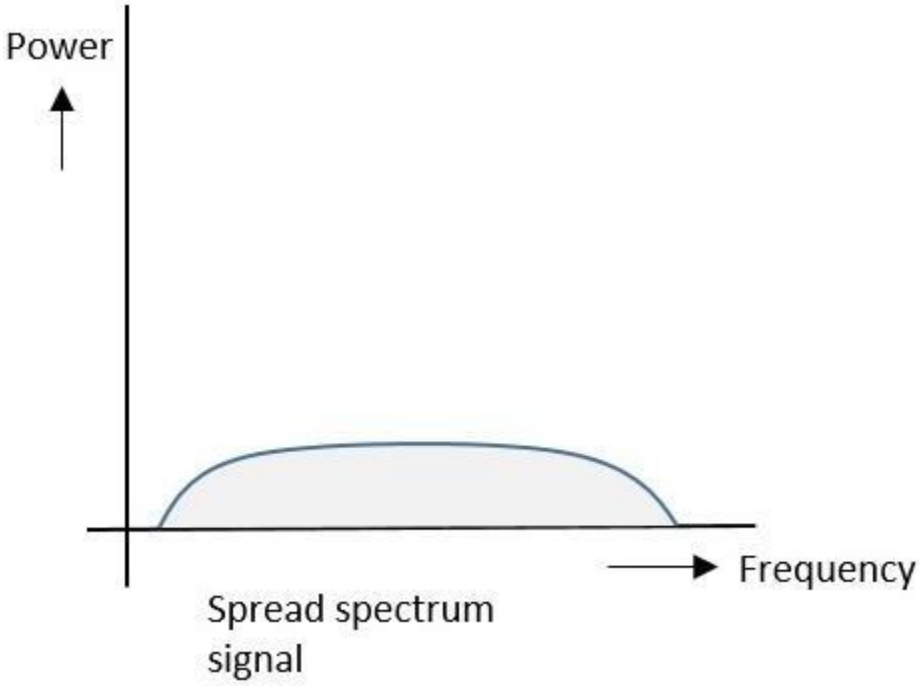
When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. However, communication between two stations in two different BSSs usually occurs via two APs. The idea is similar to communication in a cellular network if we consider each BSS to be a cell and each AP to be a base station. Note that a mobile station can belong to more than one BSS at the same time.

Spread Spectrum:

Spread spectrum is currently the most widely used transmission technique for wireless LANs. It was initially developed by the military to avoid jamming and eavesdropping of the signals. This is done by spreading the signal over a range of frequencies.

A collective class of signaling techniques are employed before transmitting a signal to provide a secure communication, known as the Spread Spectrum Modulation. The main advantage of spread spectrum communication technique is to prevent “interference” whether it is intentional or unintentional.

The signals modulated with these techniques are hard to interfere and cannot be jammed. An intruder with no official access is never allowed to crack them. Hence, these techniques are used for military purposes. These spread spectrum signals transmit at low power density and has a wide spread of signals.



Bluetooth:

Bluetooth is a short-range wireless communication technology that allows devices such as mobile phones, computers, and peripherals to transmit data or voice wirelessly over a short distance. The purpose of Bluetooth is to replace the cables that normally connect devices, while still keeping the communications between them secure. It creates a 10-meter radius wireless network, called a personal area network (PAN) or piconet, which can network between two and eight devices. Bluetooth uses less power and costs less

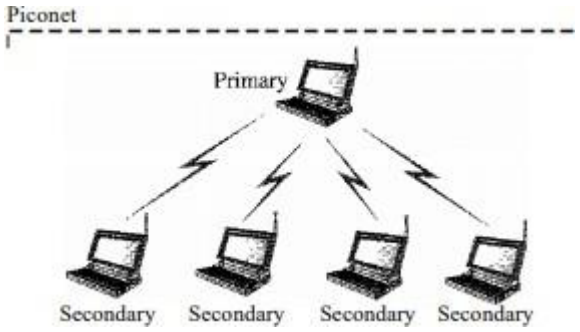
to implement than Wi-Fi. Its lower power also makes it far less prone to suffering from or causing interference with other wireless devices in the same 2.4GHz radio band.

There are some downsides to Bluetooth. The first is that it can be a drain on battery power for mobile wireless devices like smartphones, though as the technology (and battery technology) has improved, this problem is less significant than it used to be. Also, the range is fairly limited, usually extending only about 30 feet, and as with all wireless technologies, obstacles such as walls, floors, or ceilings can reduce this range further. The pairing process may also be difficult, often depending on the devices involved, the manufacturers, and other factors that all can result in frustration when attempting to connect.

Bluetooth defines two types of networks: piconet and scatternet.

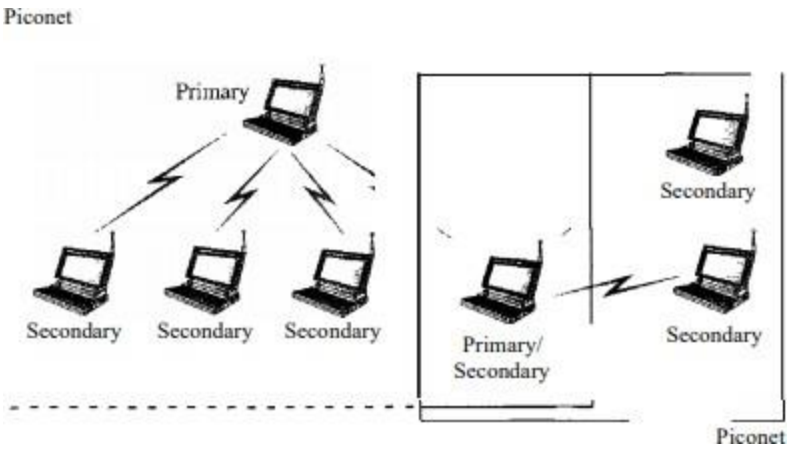
Piconets

A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary; t the rest are called secondaries. All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station. The communication between the primary and the secondary can be one-to-one or one-to-many. Figure below shows a piconet.



Scatternet

Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets. Figure below illustrates a scatternet.



Wi-Fi:

The IEEE 802.11 wireless LAN, also known as Wi-Fi, is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. Wi-Fi networks have no physical wired connection between sender and receiver, by using radio frequency (RF) technology (a frequency within the electromagnetic spectrum associated with radio wave propagation). When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space.

There are several 802.11 standards for wireless LAN technology, including 802.11b, 802.11a, and 802.11g. Table below summarizes the main characteristics of these standards. 802.11g is by far the most popular technology.

Standard	Frequency Range (United States)	Data Rate
802.11b	2.4–2.485 GHz	up to 11 Mbps
802.11a	5.1–5.8 GHz	up to 54 Mbps
802.11g	2.4–2.485 GHz	up to 54 Mbps

Wi-Fi uses multiple parts of the IEEE 802 protocol family and is designed to seamlessly interwork with its wired sister protocol Ethernet. Devices that can use Wi-Fi technologies include desktops and laptops, smartphones and tablets, smart TVs, printers, digital audio players, digital cameras, cars and drones. Compatible devices can connect to each other over Wi-Fi through a wireless access point as well as to connected Ethernet devices and may use it to access the Internet. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometers achieved by using multiple overlapping access points.

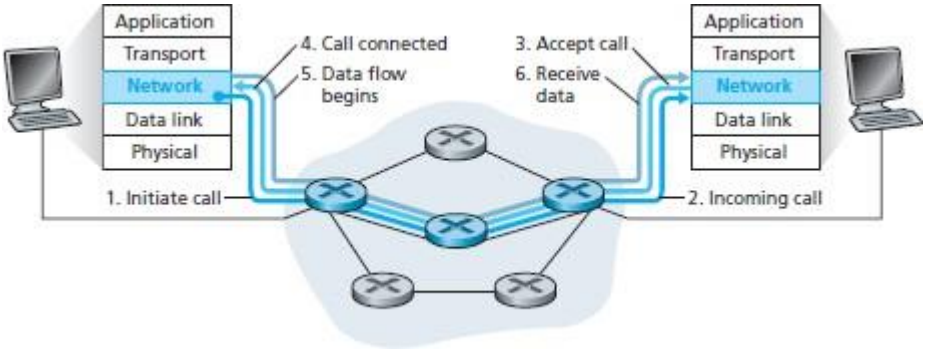
Wi-Fi is potentially more vulnerable to attack than wired networks because anyone within range of a network with a wireless network interface controller can attempt access. Wi-Fi Protected Access (WPA) is

a family of technologies created to protect information moving across Wi-Fi networks and includes solutions for personal and enterprise networks.

Overview of Virtual Circuit Switching:

Virtual circuit switching is a packet switching methodology whereby a path is established between the source and the final destination through which all the packets will be routed during a call. This path is called a virtual circuit because to the user, the connection appears to be a dedicated physical circuit. However, other communications may also be sharing the parts of the same path. So, virtual circuit packet switching is connection oriented.

Before the data transfer begins, the source and destination identify a suitable path for the virtual circuit. All intermediate nodes between the two points put an entry of the routing in their routing table for the call. Additional parameters, such as the maximum packet size, are also exchanged between the source and the destination during call setup. The virtual circuit is cleared after the data transfer is completed.



Advantages of virtual circuit switching are:

- Packets are delivered in order, since they all take the same route;
- The overhead in the packets is smaller, since there is no need for each packet to contain the full address;
- The connection is more reliable, network resources are allocated at call setup so that even during times of congestion, provided that a call has been setup, the subsequent packets should get through;
- Billing is easier, since billing records need only be generated per call and not per packet.

Overview of Frame Relay:

Frame Relay is a virtual-circuit wide-area network that was designed in response to demands for a new type of WAN. Frame Relay is a wide area network with the following features:

1. Frame Relay operates at a higher speed (1.544 Mbps and recently 44.376 Mbps).

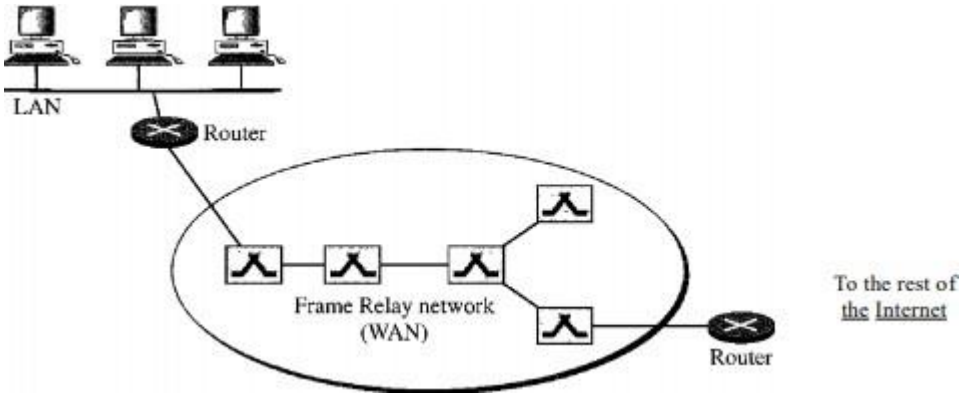
2. Frame Relay operates in just the physical and data link layers. This means it can easily be used as a backbone network to provide services to protocols that already have a network layer protocol, such as the Internet.

3. Frame Relay allows bursty data.

4. Frame Relay allows a frame size of 9000 bytes, which can accommodate all local area network frame sizes.

5. Frame Relay is less expensive than other traditional WANs.

6. Frame Relay has error detection at the data link layer only. There is no flow control or error control. There is not even a retransmission policy if a frame is damaged; it is silently dropped. Frame Relay was designed in this way to provide fast transmission capability for more reliable media and for those protocols that have flow and error control at the higher layers.



Frame relay is a virtual circuit packet switching technology that fragmented into transmission units called frames and sent in high-speed bursts through a digital network. Establishes an exclusive connection during the transmission period called virtual connection. Frame relay puts data in a variable-size unit called a frame and leaves any necessary error correction (retransmission of data) up to the endpoints, which speeds up overall data transmission. Configuring user equipment in a Frame Relay network is extremely simple. The connection-oriented service provided by Frame Relay has properties like non-duplication of frames, preservation of the frame transfer order and small probability of frame loss. The features provided by Frame Relay make it one of the best choices for interconnecting local area networks using a wide area network. However, the drawback in this method is that it becomes prohibitively expensive with growth of the network.

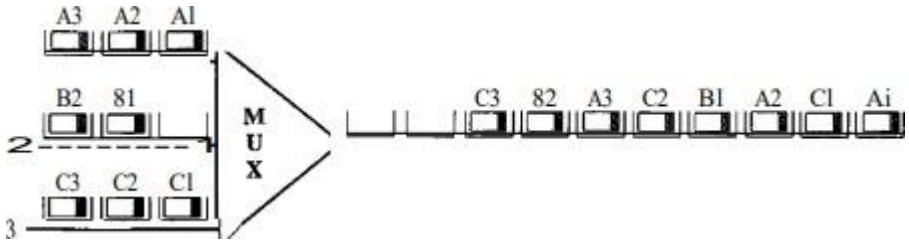
There are certain benefits which are associated with Frame Relay.

- It helps in reducing the cost of internetworking, as there is considerable reduction in the number of circuits required and the associated bandwidths.
- It helps in increasing the performance due to reduced network complexity.
- It increases the interoperability with the help of international standards.
- Frame Relay is protocol independent and can easily be used to combine traffic from other networking protocols.

In business scenarios, where there is a slow connection or continuous traffic flow due to applications like multimedia, Frame Relay is not a recommended choice.

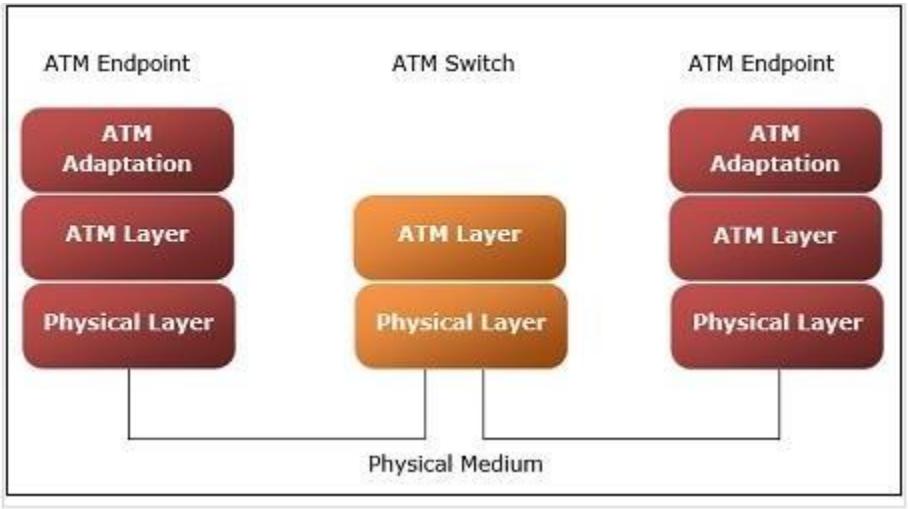
Overview of ATM:

Asynchronous transfer mode (ATM) is a switching technique used by telecommunication networks that uses asynchronous time-division multiplexing to encode data into small, fixed-sized cells.



ATM networks are connection-oriented networks that supports voice, video and data communications. It encodes data into small fixed - size cells so that they are suitable for TDM and transmits them over a physical medium.

The size of an ATM cell is 53 bytes: 5-byte header and 48-byte payload.



Physical Layer − This layer corresponds to physical layer of OSI model. At this layer, the cells are converted into bit streams and transmitted over the physical medium.

ATM Layer −This layer is comparable to data link layer of OSI model. It accepts the 48-byte segments from the upper layer, adds a 5-byte header to each segment and converts into 53-byte cells. This layer is responsible for routing of each cell, traffic management, multiplexing and switching.

ATM Adaptation Layer −This layer corresponds to network layer of OSI model. It provides facilities to the existing packet switched networks to connect to ATM network and use its services. It accepts the data and converts them into fixed sized segments.

Benefits of ATM Networks are

- It provides the dynamic bandwidth that is particularly suited for bursty traffic.

- Since all data are encoded into identical cells, data transmission is simple, uniform and predictable.
- Uniform packet size ensures that mixed traffic is handled efficiently.
- Small sized header reduces packet overload, thus ensuring effective bandwidth usage.
- ATM networks are scalable both in size and speed.

Data Link Layer Protocols (DLL):

Data Link Layer protocols are generally responsible to simply ensure and confirm that the bits and bytes that are received are identical to the bits and bytes being transferred. It is basically a set of specifications that are used for implementation of data link layer just above the physical layer of the OSI Model.

High-Level Data Link Protocol (HDLC):

HDLC is basically a protocol that is now assumed to be an umbrella under which many Wide Area protocols reside. It is used to connect all of the remote devices to mainframe computers at central locations may be in point-to-point or multipoint connections. It is also used to make sure that the data units should arrive correctly and with right flow from one network point to next network point. It also provides best-effort unreliable service and also reliable service. HDLC is a bit-oriented protocol that is applicable for point-to-point and multipoint communications both.

Point to Point Protocol (PPP):

PPP is a protocol that is basically used to provide functionality to add a framing byte at end of IP packet. It is basically a data link control facility that is required for transferring IP packets usually among Internet Service Providers (ISP) and a home user. It is most robust protocol that is used to transport other types of packets also along with IP Packets. It is a byte-oriented protocol that is also used for error detection.

Difference Between High-level Data Link Control (HDLC) and Point-to-Point Protocol (PPP):

The main difference between High-level Data Link Control (HDLC) and Point-to-Point Protocol (PPP) is that High-level Data Link Control is the bit-oriented protocol, on the other hand, Point-to-Point Protocol is the byte-oriented protocol.

Another difference between HDLC and PPP is that HDLC is implemented by Point-to-point configuration and also multi-point configurations on the other hand While PPP is implemented by Point-to-Point configuration only.

S.NO	HDLC	PPP
1.	HDLC stands for High-level Data Link Control.	PPP stands for Point-to-Point Protocol.
2.	HDLC is a bit oriented protocol.	PPP is a byte oriented protocol.
3.	HDLC is implemented by Point-to-point configuration and also multi-point configurations.	PPP is implemented by Point-to-Point configuration only.
4.	Dynamic addressing is not offered by HDLC.	While in this Dynamic addressing is offered.
5.	HDLC is used in synchronous media.	PPP is used in synchronous media as well as asynchronous media.
6.	HDLC is not compatible with non-Cisco devices.	PPP is compatible with non-Cisco devices.
7.	HDLC does not provide link authentication.	While PPP provide link authentication using various protocols.
8.	HDLC is more costly comparatively.	While PPP is comparatively less costly.