COMPUTER NETWORKS NOTES

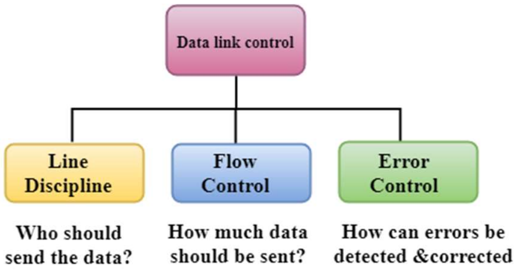
MODULE 3:

DATA LINK CONTROLS

Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium. For example, In the half-duplex transmission mode, one device can only transmit the data at a time. If both the devices at the end of the links transmit the data simultaneously, they will collide and leads to the loss of the information. The Data link layer provides the coordination among the devices so that no collision occurs.

The Data link layer provides three functions:

- Line discipline
- Flow Control
- Error Control


Data link control
Line Discipline
Flow Control
Error Control
Who should send the data?
How much data should be sent?
How can errors be detected &corrected

LINE DISCIPLINE

Line Discipline is a functionality of the Data link layer that provides the coordination among the link systems. It determines which device can send, and when it can send the data.

Line Discipline can be achieved in two ways:

- ENQ/ACK
- Poll/select

END/ACK

END/ACK stands for Enquiry/Acknowledgement is used when there is no wrong receiver available on the link and having a dedicated path between the two devices so that the device capable of receiving the transmission is the intended one. END/ACK coordinates which device will start the transmission and whether the recipient is ready or not.

Working of END/ACK

The transmitter transmits the frame called an Enquiry (ENQ) asking whether the receiver is available to receive the data or not.

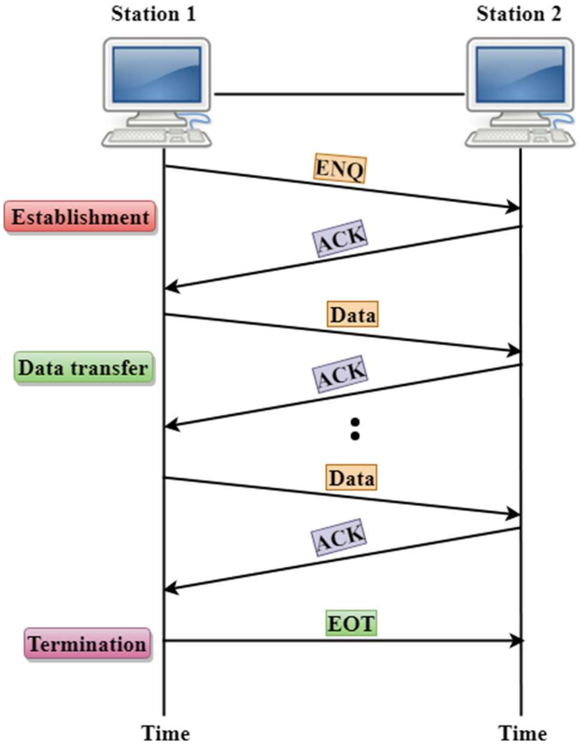
The receiver responses either with the positive acknowledgement (ACK) or with the negative acknowledgement (NACK) where positive acknowledgement means that the receiver is ready to receive the transmission and negative acknowledgement means that the receiver is unable to accept the transmission.

Following are the responses of the receiver:

If the response to the ENQ is positive, the sender will transmit its data, and once all of its data has been transmitted, the device finishes its transmission with an EOT (END-of-Transmission) frame.

If the response to the ENQ is negative, then the sender disconnects and restarts the transmission at another time.

If the response is neither negative nor positive, the sender assumes that the ENQ frame was lost during the transmission and makes three attempts to establish a link before giving up.



Poll/Select

The Poll/Select method of line discipline works with those topologies where one device is designated as a primary station, and other devices are secondary stations.

Working of Poll/Select

In this, the primary device and multiple secondary devices consist of a single transmission line, and all the exchanges are made through the primary device even though the destination is a secondary device.

The primary device has control over the communication link, and the secondary device follows the instructions of the primary device.

The primary device determines which device is allowed to use the communication channel. Therefore, we can say that it is an initiator of the session.

If the primary device wants to receive the data from the secondary device, it asks the secondary device that they anything to send, this process is known as polling.

If the primary device wants to send some data to the secondary device, then it tells the target secondary to get ready to receive the data, this process is known as selecting.

Select

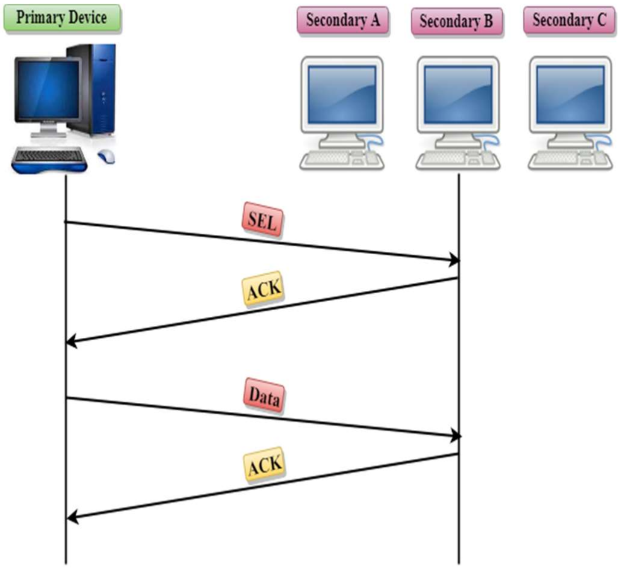
The select mode is used when the primary device has something to send.

When the primary device wants to send some data, then it alerts the secondary device for the upcoming transmission by transmitting a Select (SEL) frame, one field of the frame includes the address of the intended secondary device.

When the secondary device receives the SEL frame, it sends an acknowledgement that indicates the secondary ready status.

If the secondary device is ready to accept the data, then the primary device sends two or more data frames to the intended secondary device.

Once the data has been transmitted, the secondary sends an acknowledgement specifies that the data has been received.

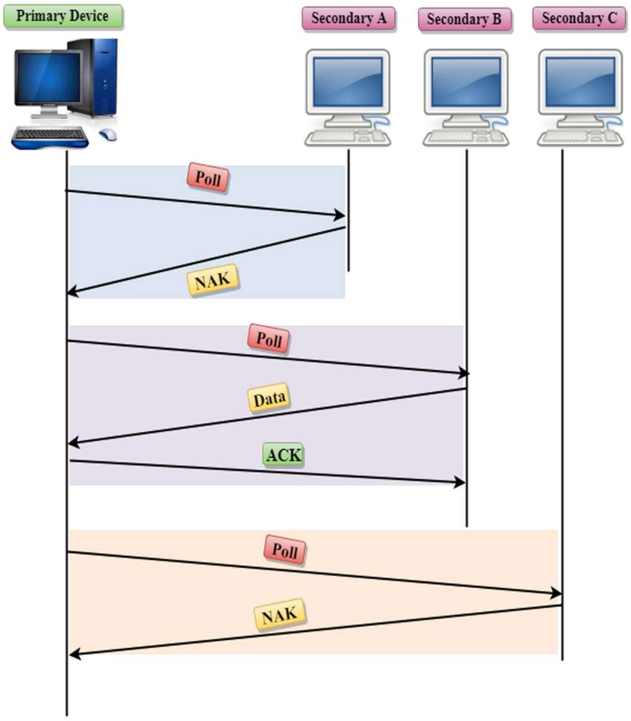


Poll

The Poll mode is used when the primary device wants to receive some data from the secondary device.

When a primary device wants to receive the data, then it asks each device whether it has anything to send.

Firstly, the primary asks (poll) the first secondary device, if it responds with the NACK (Negative Acknowledgement) means that it has nothing to send. Now, it approaches the second secondary device, it responds with the ACK means that it has the data to send. The secondary device can send more than one frame one after another or sometimes it may be required to send ACK before sending each one, depending on the type of the protocol being used.



FLOW CONTROL

It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver.

The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.

It requires a buffer, a block of memory for storing the information until they are processed.

Two methods have been developed to control the flow of data:

- Stop-and-wait
- Sliding window

Stop-and-wait

In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.

When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

Advantage of Stop-and-wait

The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent.

Disadvantage of Stop-and-wait

Stop-and-wait technique is inefficient to use as each frame must travel across all the way to the receiver, and an acknowledgement travels all the way before the next frame is sent. Each frame sent and received uses the entire time needed to traverse the link.

Sliding Window

The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.

In Sliding Window Control, multiple frames can be sent one after the another due to which capacity of the communication channel can be utilized efficiently.

A single ACK acknowledge multiple frames.

Sliding Window refers to imaginary boxes at both the sender and receiver end.

The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement.

Frames can be acknowledged even when the window is not completely filled.

The window has a specific size in which they are numbered as modulo-n means that they are numbered from 0 to n-1. For example, if n = 8, the frames are numbered from 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1........

The size of the window is represented as n-1. Therefore, maximum n-1 frames can be sent before acknowledgement.

When the receiver sends the ACK, it includes the number of the next frame that it wants to receive. For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5. When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received.

Sliding Window Protocol

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).

In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Types of Sliding Window Protocol

Sliding window protocol has two types:

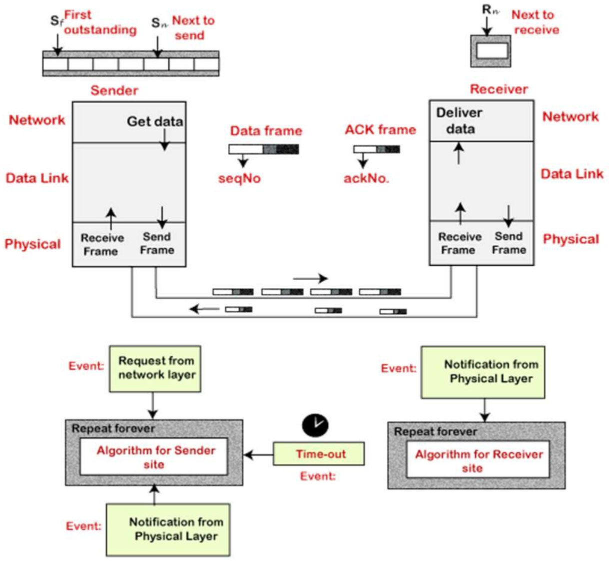
- Go-Back-N ARQ
- Selective Repeat ARQ

Go-Back-N ARQ

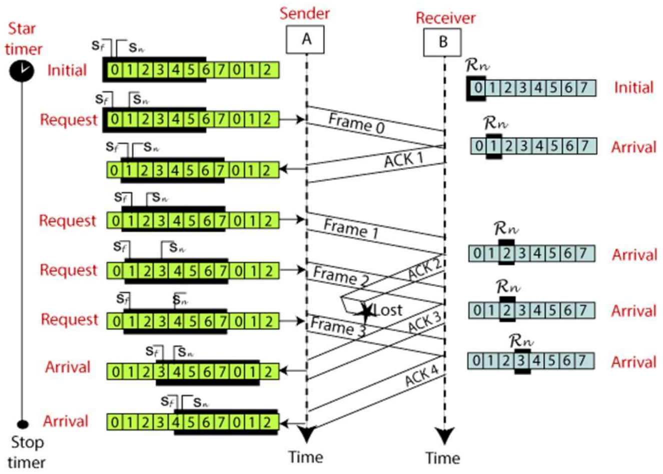
Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.

The size of the sender window is N in this protocol. For example, Go-Back-8, the size of the sender window, will be 8. The receiver window size is always 1.

If the receiver receives a corrupted frame, it cancels it. The receiver does not accept a corrupted frame. When the timer expires, the sender sends the correct frame again. The design of the Go-Back-N ARQ protocol is shown below.



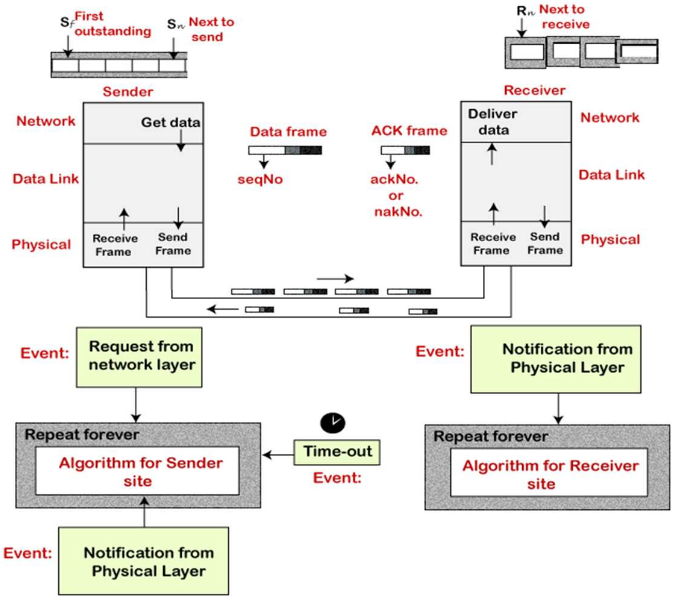
The example of Go-Back-N ARQ is shown below in the figure.

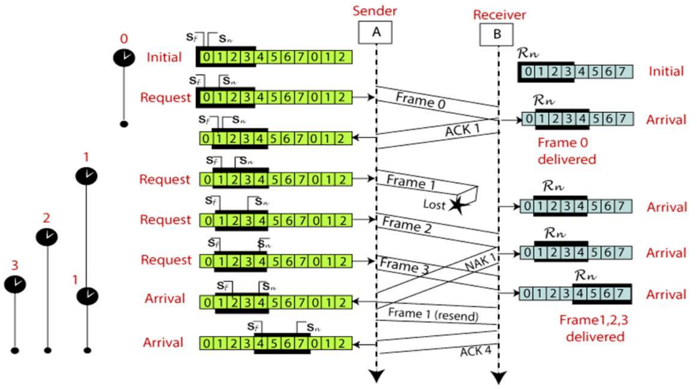


Selective Repeat ARQ

Selective Repeat ARQ is also known as the Selective Repeat Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. The Go-back-N ARQ protocol works well if it has fewer errors. But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again. So, we use the Selective Repeat ARQ protocol. In this protocol, the size of the sender window is always equal to the size of the receiver window. The size of the sliding window is always greater than 1.

If the receiver receives a corrupt frame, it does not directly discard it. It sends a negative acknowledgment to the sender. The sender sends that frame again as soon as on the receiving negative acknowledgment. There is no waiting for any time-out to send that frame. The design of the Selective Repeat ARQ protocol is shown below.





The example of the Selective Repeat ARQ protocol is shown below in the figure.

Difference between the Go-Back-N ARQ and Selective Repeat ARQ?

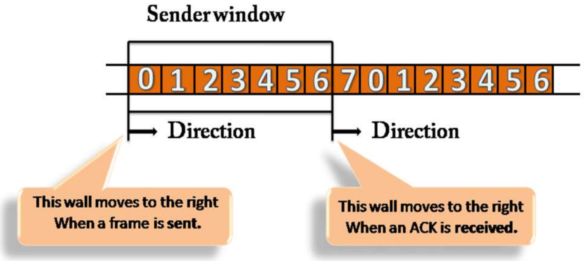
Go-Back-N ARQ	Selective Repeat ARQ
If a frame is corrupted or lost in it,all subsequent frames have to be sent again.	In this, only the frame is sent again, which is corrupted or lost.
If it has a high error rate,it wastes a lot of bandwidth.	There is a loss of low bandwidth.
It is less complex.	It is more complex because it has to do sorting and searching as well. And it also requires more storage.
It does not require sorting.	In this, sorting is done to get the frames in the correct order.
It does not require searching.	The search operation is performed in it.
It is used more.	It is used less because it is more complex.

Sender Window

At the beginning of a transmission, the sender window contains n-1 frames, and when they are sent out, the left boundary moves inward shrinking the size of the window. For example, if the size of the window is w if three frames are sent out, then the number of frames left out in the sender window is w-3.

Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK.

For example, the size of the window is 7, and if frames 0 through 4 have been sent out and no acknowledgement has arrived, then the sender window contains only two frames, i.e., 5 and 6. Now, if ACK has arrived with a number 4 which means that 0 through 3 frames have arrived undamaged and the sender window is expanded to include the next four frames. Therefore, the sender window contains six frames (5,6,7,0,1,2).


Sender window
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6
Direction
Direction
This wall moves to the right When a frame is sent.
This wall moves to the right When an ACK is received.

Receiver Window

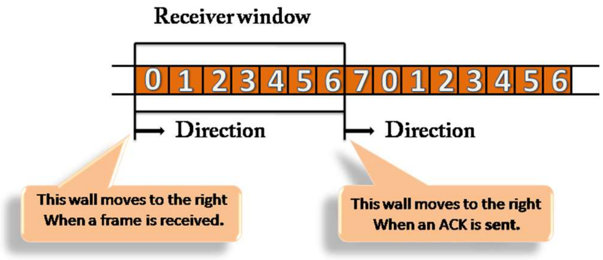
At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames.

When the new frame arrives, the size of the window shrinks.

The receiver window does not represent the number of frames received, but it represents the number of frames that can be received before an ACK is sent. For example, the size of the window is w, if three frames are received then the number of spaces available in the window is (w-3).

Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged.

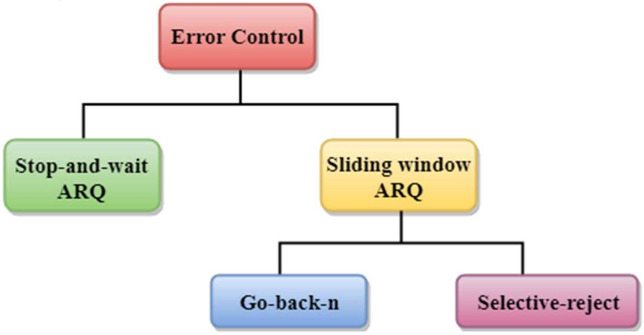
Suppose the size of the window is 7 means that the receiver window contains seven spaces for seven frames. If the one frame is received, then the receiver window shrinks and moving the boundary from 0 to 1. In this way, window shrinks one by one, so window now contains the six spaces. If frames from 0 through 4 have sent, then the window contains two spaces before an acknowledgement is sent.


Receiver window
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6
Direction
Direction
This wall moves to the right When a frame is received.
This wall moves to the right When an ACK is sent.

ERROR CONTROL

Error Control is a technique of error detection and retransmission.

Categories of Error Control:



Stop-and-wait ARQ

Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames.

This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame.

Four features are required for the retransmission:

1. The sending device keeps a copy of the last transmitted frame until the acknowledgement is received. Keeping the copy allows the sender to retransmit the data if the frame is not received correctly.
2. Both the data frames and the ACK frames are numbered alternately 0 and 1 so that they can be identified individually. Suppose data 1 frame acknowledges the data 0 frame means that the data 0 frame has been arrived correctly and expects to receive data 1 frame.
3. If an error occurs in the last transmitted frame, then the receiver sends the NAK frame which is not numbered. On receiving the NAK frame, sender retransmits the data.

4. It works with the timer. If the acknowledgement is not received within the allotted time, then the sender assumes that the frame is lost during the transmission, so it will retransmit the frame.

Two possibilities of the retransmission:

1. **Damaged Frame:** When the receiver receives a damaged frame, i.e., the frame contains an error, then it returns the NAK frame. For example, when the data 0 frame is sent, and then the receiver sends the ACK 1 frame means that the data 0 has arrived correctly, and transmits the data 1 frame. The sender transmits the next frame: data 1. It reaches undamaged, and the receiver returns ACK 0. The sender transmits the next frame: data 0. The receiver reports an error and returns the NAK frame. The sender retransmits the data 0 frame.
2. **Lost Frame:** Sender is equipped with the timer and starts when the frame is transmitted. Sometimes the frame has not arrived at the receiving end so that it can be acknowledged neither positively nor negatively. The sender waits for acknowledgement until the timer goes off. If the timer goes off, it retransmits the last transmitted frame.

Sliding Window ARQ

Sliding Window ARQ is a technique used for continuous transmission error control.

Three Features used for retransmission:

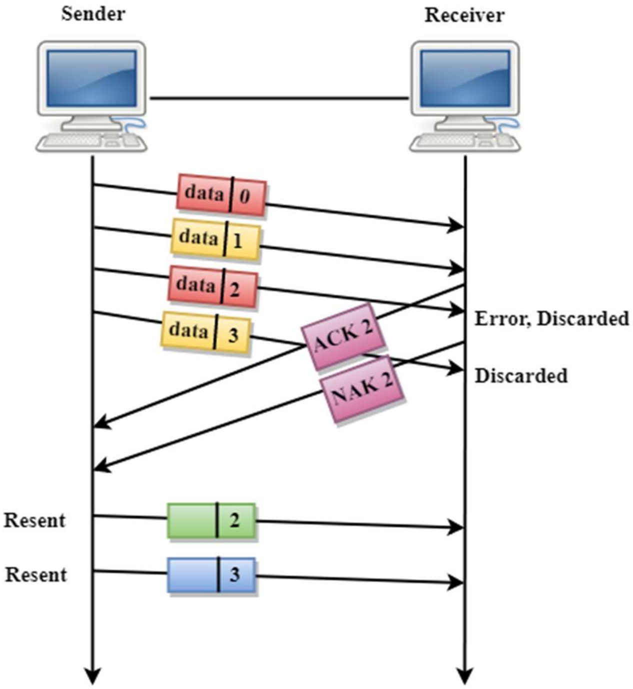
1. In this case, the sender keeps the copies of all the transmitted frames until they have been acknowledged. Suppose the frames from 0 through 4 have been transmitted, and the last acknowledgement was for frame 2, the sender has to keep the copies of frames 3 and 4 until they receive correctly.
2. The receiver can send either NAK or ACK depending on the conditions. The NAK frame tells the sender that the data have been received damaged. Since the sliding window is a continuous transmission mechanism, both ACK and NAK must be numbered for the identification of a frame. The ACK frame consists of a number that represents the next frame which the receiver expects to receive. The NAK frame consists of a number that represents the damaged frame.
3. The sliding window ARQ is equipped with the timer to handle the lost acknowledgements. Suppose then n-1 frames have been sent before receiving any acknowledgement. The sender waits for the acknowledgement, so it starts the timer and waits before sending any more. If the allotted time runs out, the sender retransmits one or all the frames depending upon the protocol used.

Two protocols used in sliding window ARQ:

Go-Back-n ARQ: In Go-Back-N ARQ protocol, if one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK.

Three possibilities can occur for retransmission:

Damaged Frame: When the frame is damaged, then the receiver sends a NAK frame.



In the above figure, three frames have been transmitted before an error discovered in the third frame. In this case, ACK 2 has been returned telling that the frames 0,1 have been received successfully without any error. The receiver discovers the error in data 2 frame, so it returns the NAK 2 frame. The frame 3 is also discarded as it is transmitted after the damaged frame. Therefore, the sender retransmits the frames 2,3.

Lost Data Frame: In Sliding window protocols, data frames are sent sequentially. If any of the frames is lost, then the next frame arrive at the receiver is out of sequence. The receiver checks the sequence number of each of the frame, discovers the frame that has been skipped, and returns the NAK for the missing frame. The sending device retransmits the frame indicated by NAK as well as the frames transmitted after the lost frame.

Lost Acknowledgement: The sender can send as many frames as the windows allow before waiting for any acknowledgement. Once the limit of the window is reached, the sender has no more frames to send; it must wait for the acknowledgement. If the acknowledgement is lost, then the sender could wait forever. To avoid such situation, the sender is equipped with the timer that starts counting whenever the window capacity is reached. If the acknowledgement has not been received within the time limit, then the sender retransmits the frame since the last ACK.

Selective-Reject ARQ

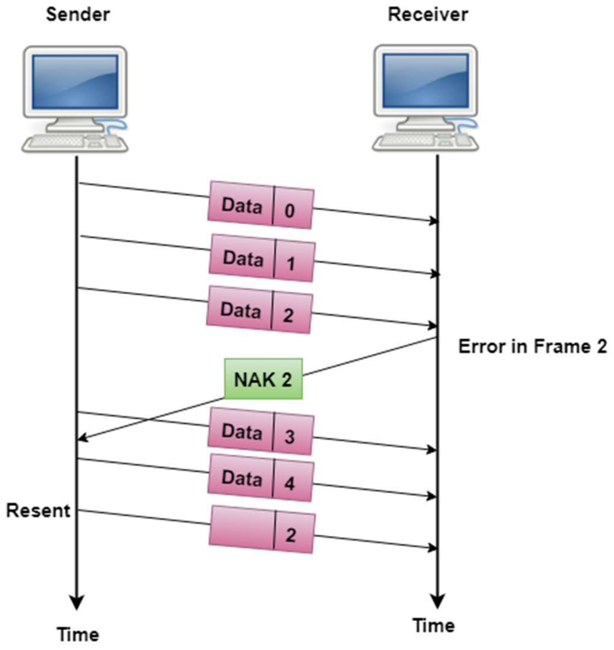
Selective-Reject ARQ technique is more efficient than Go-Back-n ARQ.

In this technique, only those frames are retransmitted for which negative acknowledgement (NAK) has been received.

The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received.

The receiver must have an appropriate logic for reinserting the frames in a correct order.

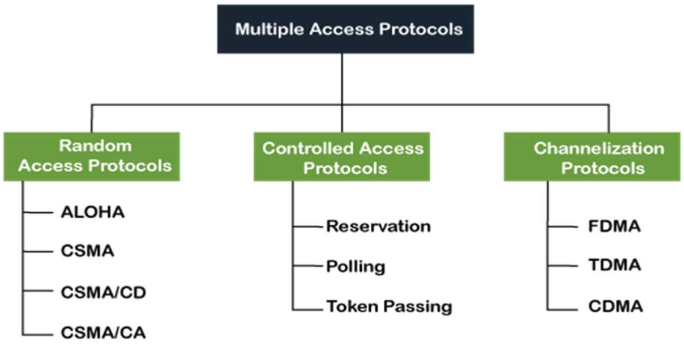
The sender must consist of a searching mechanism that selects only the requested frame for retransmission.



MULTIPLE ACCESS PROTOCOL- ALOHA,CSMA,CSMA/CA AND CSMA/CD

DATA LINK LAYER

The data link layer is used in a computer network to transmit the data between two devices or nodes. It divides the layer into parts such as **data link control** and the **multiple access resolution/protocol**. The upper layer has the responsibility to flow control and the error control in the data link layer, and hence it is termed as **logical of data link control**. Whereas the lower sub-layer is used to handle and reduce the collision or multiple access on a channel. Hence it is termed as **media access control** or the multiple access resolutions.



Data Link Control

A data link control is a reliable channel for transmitting data over a dedicated link using various techniques such as framing, error control and flow control of data packets in the computer network.

What is a multiple access protocol?

When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel. Suppose there is no dedicated path to communicate or transfer the data between two devices. In that case, multiple stations access the channel and simultaneously transmits the data over the channel. It may create collision and cross talk. Hence, the multiple access protocol is required to reduce the collision and avoid crosstalk between the channels.

For example, suppose that there is a classroom full of students. When a teacher asks a question, all the students (small channels) in the class start answering the question at the same time (transferring the data simultaneously). All the students respond at the same time due to which data is overlap or data lost. Therefore, it is the responsibility of a teacher (multiple access

protocol) to manage the students and make them one answer.
Following are the types of multiple access protocol that is subdivided into the different process as:

A. RANDOM ACCESS PROTOCOL

In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on another station nor any station control another station. Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict. Due to the collision, the data frame packets may be lost or changed. And hence, it does not receive by the receiver end.

Following are the different methods of random-access protocols for broadcasting frames on the channel.

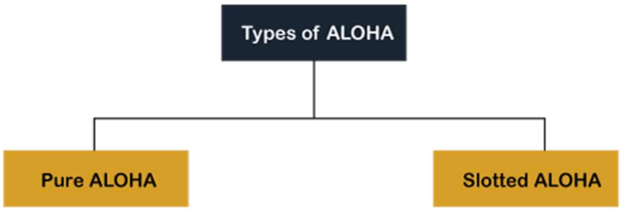
- Aloha
- CSMA
- CSMA/CD
- CSMA/CA

ALOHA Random Access Protocol

It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

Aloha Rules

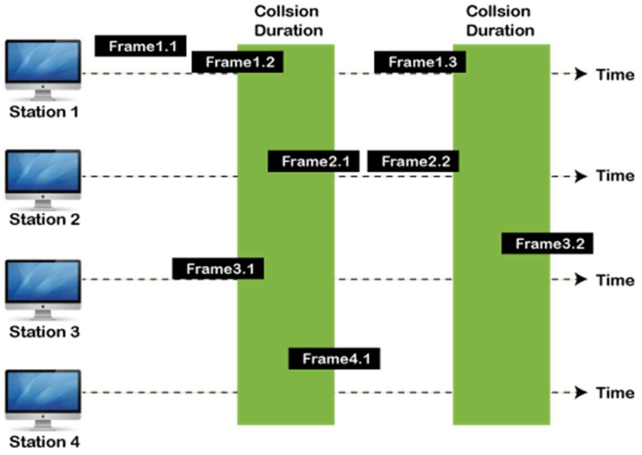
- Any station can transmit data to a channel at any time.
- It does not require any carrier sensing.
- Collision and data frames may be lost during the transmission of data through multiple stations.
- Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
- It requires retransmission of data after some random amount of time.



Pure Aloha

Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

The total vulnerable time of pure Aloha is 2 * Tfr.
Maximum throughput occurs when G = 1/ 2 that is 18.4%.
Successful transmission of data frame is S = G * e ^ - 2 G.

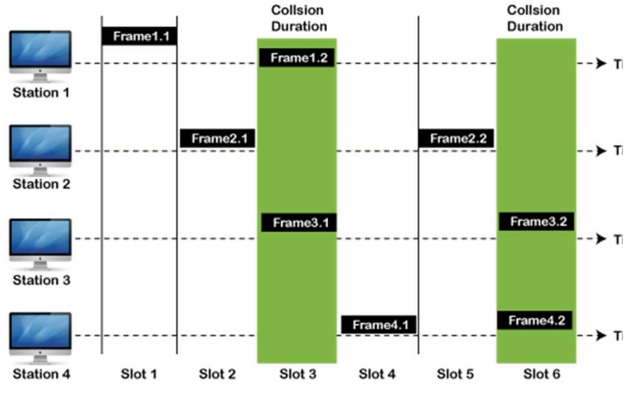


Frames in Pure ALOHA

As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same time, other frames are lost or destroyed. Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage. If the new frame's first bit enters the channel before finishing the last bit of the second frame. Both frames are completely finished, and both stations must retransmit the data frame.

Slotted Aloha

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.
Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.
The total vulnerable time required in slotted Aloha is Tfr.



Frames in Slotted ALOHA

CSMA (CARRIER SENSE MULTIPLE ACCESS)

It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

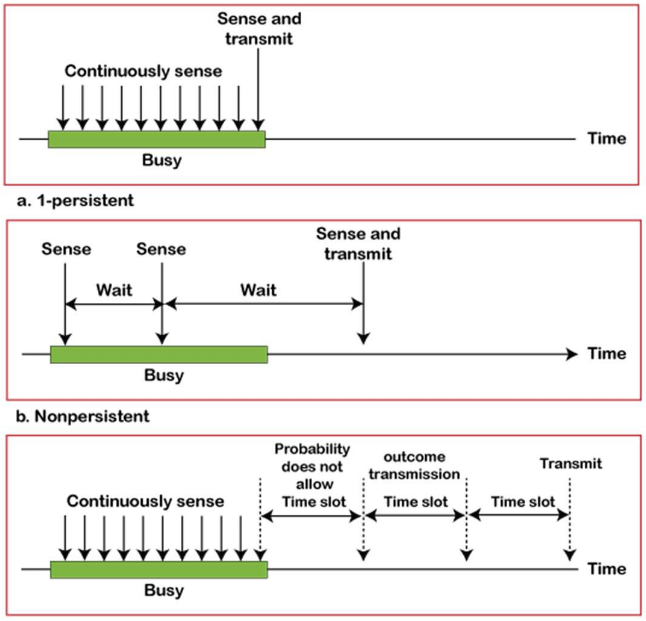
CSMA Access Modes

1-Persistent: In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.

Non-Persistent: It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

P-Persistent: It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time and resumes the frame with the next time slot.

O- Persistent: It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



a. 1-persistent

b. Nonpersistent

c. p-persistent

CSMA/ CD

It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

CSMA/ CA

It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

Following are the methods used in the CSMA/ CA to avoid the collision:

Interframe space: In this method, the station waits for the channel to become idle, and if it gets the channel is idle, it does not immediately send the data. Instead of this, it waits for some time, and this time period is called the **Interframe** space or IFS. However, the IFS time is often used to define the priority of the station.

Contention window: In the Contention window, the total time is divided into different slots. When the station/ sender is ready to transmit the data frame, it chooses a random slot number of slots as **wait time**. If the channel is still busy, it does not restart the entire process, except that it restarts the timer only to send data packets when the channel is inactive.

Acknowledgment: In the acknowledgment method, the sender station sends the data frame to the shared channel if the acknowledgment is not received ahead of time.

B. CONTROLLED ACCESS PROTOCOL

It is a method of reducing data frame collision on a shared channel. In the controlled access method, each station interacts and decides to send a data frame by a particular station approved by all other stations. It means that a single station cannot send the data frames unless all other stations are not approved. It has three types of controlled access: **Reservation, Polling**, and **Token Passing**.

C. CHANNELIZATION PROTOCOLS

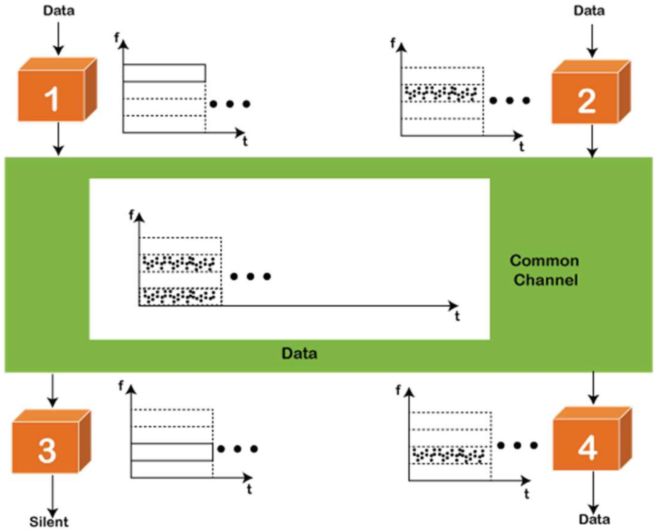
It is a channelization protocol that allows the total usable bandwidth in a shared channel to be shared across multiple stations based on their time, distance and codes. It can access all the stations at the same time to send the data frames to the channel.

Following are the various methods to access the channel based on their time, distance and codes:

- FDMA (Frequency Division Multiple Access)
- TDMA (Time Division Multiple Access)
- CDMA (Code Division Multiple Access)

FDMA

It is a frequency division multiple access (**FDMA**) method used to divide the available bandwidth into equal bands so that multiple users can send data through a different frequency to the subchannel. Each station is reserved with a particular band to prevent the crosstalk between the channels and interferences of stations.



TDMA

Time Division Multiple Access (**TDMA**) is a channel access method. It allows the same frequency bandwidth to be shared across multiple stations. And to avoid collisions in the shared channel, it divides the channel into different frequency slots that allocate stations to transmit the data frames. The same **frequency** bandwidth into the shared channel by dividing the signal into various time slots to transmit it. However, TDMA has an overhead of synchronization that specifies each station's time slot by adding synchronization bits to each slot.

CDMA

The code division multiple access (CDMA) is a channel access method. In CDMA, all stations can simultaneously send the data over the same channel. It means that it allows each station to transmit the data frames with full frequency on the shared channel at all times. It does not require the division of bandwidth on a shared channel based on time slots. If multiple stations send data to a channel simultaneously, their data frames are separated by a unique code sequence. Each station has a different unique code for transmitting the data over a shared channel. For example, there are multiple users in a room that are continuously speaking. Data is received by the users if only two-person interact with each other using the same language. Similarly, in the network, if different stations communicate with each other simultaneously with different code language.

ETHERNET FRAME FORMAT

The IEEE 802.3 standard defines the fundamental frame format that is necessary for all MAC implementations. However, the core functionality of the protocol is being extended by several optional forms.

Preamble and SFD, which operate at the physical layer, begin an Ethernet frame. The packet's payload follows the Ethernet header, which includes the MAC addresses for the source and destination. CRC, the final field, is utilized to find errors. Let's now examine each section of the fundamental frame format.

PREAMBLE - Ethernet frames begin with a 7-byte. This is a sequence of alternate 0s and 1s that denotes the beginning of the frame and enables bit synchronization between the sender and receiver. PRE (Preamble) was initially developed to accommodate the loss of a few bits as a result of signal delays. However, the frame bits in high-speed Ethernet today are protected without the need for a preamble.

Prior to the actual frame beginning, PRE (Preamble) alerts the receiver that a frame is about to start and enables the receiver to lock onto the data stream.

Start of frame Delimiter (SFD) - This 1-byte field is always set to **10101011**. The destination address is the next set of bits that will begin the frame, as indicated by SFD. The preamble is frequently referred to as 8 Bytes since SFD is sometimes seen as a component of PRE. The SFD notifies the station or stations that synchronization is now impossible.

Destination Address - This 6-Byte element contains the MAC address of the device for which the data is intended.

Source Address - This 6-byte element contains the source machine's MAC address. Since Source Address is always a unique address (Unicast), 0 is always the least significant bit of the first byte.

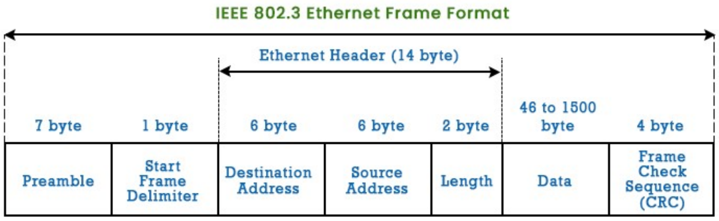
Length - A 2-Byte field called Length represents the size of an Ethernet frame as a whole. Due to some inherent constraints of Ethernet, this 16-bit field can store length values from 0 to 65534, but length values greater than 1500 are not permitted.

Data - This area, sometimes referred to as the Payload, is where the real data is placed. If Internet Protocol is utilised via Ethernet, both the IP header and data will be placed here. The longest possible piece of data might be 1500 bytes long. If the data length is less than the minimum length, which is 46 bytes, padding 0's are appended to make up the difference.

Cyclic Redundancy Check (CRC) - CRC is a field of 4 bytes. The data in this field is a 32-bit hash code created using the fields for the destination address, source address, length, and data. Data is damaged if the checksum calculated by the destination differs from the checksum value supplied.

Note- Ethernet IEEE 802.3 frames range in size from 64 to 1518 bytes, including data length (46 to 1500 bytes),

Below, a thorough explanation of the IEEE 802.3 basic frame format is provided. Let's look at the expanded Ethernet frame header, which allows for a payload of even more than 1500 bytes.



DA [Destination MAC Address]: ***6 bytes***

SA [Source MAC Address]: ***6 bytes***

Type [0x8870 (Ethertype)]: ***2 bytes***

DSAP [802.2 Destination Service Access Point]: ***1 byte***

SSAP [802.2 Source Service Access Point]: ***1 byte***

Ctrl [802.2 Control Field]: ***1 byte***

Data [Protocol Data]: ***> 46 bytes***

FCS [Frame Checksum]: ***4 bytes***

Although the Ethernet II frame lacks a length field, the network interface knows the frame length because it accepts the frame.

ADVANTAGES OF USING ETHERNET:

- Simple to implement
- Maintenance is Easy

- Less cost

FLAWS OF ETHERNET:

It can't be applied in real-time situations. Data delivery within a certain time frame is necessary for real-time applications. Due to the high likelihood of collisions, Ethernet is unreliable. The delivery of the data to its destination may be delayed due to an increased number of collisions. Applications requiring interaction cannot be utilized with it. Even extremely little amounts of data must be delivered for interactive apps like chatting. The minimum data length required by Ethernet is 46 bytes.

It is incompatible with client-server applications. Applications that use client-server architecture demand that the server is prioritised over the client. Priorities cannot be set in Ethernet.

INTRODUCTION TO WIRELESS LAN

Wireless LAN stands for **Wireless Local Area Network**. It is also called LAWN (**Local Area Wireless Network**). WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection.

The IEEE 802.11 group of standards defines the technologies for wireless LANs. For path sharing, 802.11 standard uses the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance). It also uses an encryption method i.e. wired equivalent privacy algorithm.

Wireless LANs provide high speed data communication in small areas such as building or an office. WLANs allow users to move around in a confined area while they are still connected to the network.

In some instance wireless LAN technology is used to save costs and avoid laying cable, while in other cases, it is the only option for providing high-speed internet access to the public. Whatever the reason, wireless solutions are popping up everywhere.

Examples of WLANs that are available today are NCR's waveLAN and Motorola's ALTAIR.

ADVANTAGES OF WLANS

Flexibility: Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).

Planning: Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.

Design: Wireless networks allow for the design of independent, small devices which can for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.

Robustness: Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters.

Cost: The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, after providing wireless access to the wireless network via an access point for the first user, adding additional users to a network will not increase the cost. And second, wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it.

Ease of Use: Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

DISADVANTAGES OF WLANS

Quality of Services: Quality of wireless LAN is typically lower than wired networks. The main reason for this is the lower bandwidth due to limitations is radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.

Proprietary Solutions: Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardization functionality plus many enhanced features. Most components today adhere to the basic standards IEEE 802.11a or 802.11b.

Restrictions: Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.

Global operation: Wireless LAN products are sold in all countries so, national and international frequency regulations have to be considered.

Low Power: Devices communicating via a wireless LAN are typically power consuming, also wireless devices running on battery power. Whereas the LAN design should take this into account and implement special power saving modes and power management functions.

License free operation: LAN operators don't want to apply for a special license to be able to use the product. The equipment must operate in a license free band, such as the 2.4 GHz ISM band.

Robust transmission technology: If wireless LAN uses radio transmission, many other electrical devices can interfere with them (such as vacuum cleaner, train engines, hair dryers, etc.).Wireless LAN transceivers cannot be adjusted for perfect transmission is a standard office or production environment.

FUNDAMENTALS OF WLANS

HIPERLAN

HiperLAN stands for High performance LAN. While all of the previous technologies have been designed specifically for an adhoc environment, HiperLAN is derived from traditional LAN environments and can support multimedia data and asynchronous data effectively at high rates (23.5 Mbps).

A LAN extension via access points can be implemented using standard features of the HiperLAN/1 specification. However, HiperLAN does not necessarily require any type of access point infrastructure for its operation.

HiperLAN was started in 1992, and standards were published in 1995. It employs the 5.15GHz and 17.1 GHz frequency bands and has a data rate of 23.5 Mbps with coverage of 50m and mobility< 10 m/s.

It supports a packet-oriented structure, which can be used for networks with or without a central control (BS-MS and ad-hoc). It supports 25 audio connections at 32kbps with a maximum latency of 10 ms, one video connection of 2 Mbps with 100 ms latency, and a data rate of 13.4 Mbps.

HiperLAN/1 is specifically designed to support adhoc computing for multimedia systems, where there is no requirement to deploy a centralized infrastructure. It effectively supports MPEG or other state of the art real time digital audio and video standards.

The HiperLAN/1 MAC is compatible with the standard MAC service interface, enabling support for existing applications to remain unchanged.

HiperLAN 2 has been specifically developed to have a wired infrastructure, providing short-range wireless access to wired networks such as IP and ATM.

The two main differences between HiperLAN types 1 and 2 are as follows:

1. Type 1 has a distributed MAC with QoS provisions, whereas type 2 has a centralized schedule MAC.
2. Type 1 is based on Gaussian minimum shift keying (GMSK), whereas type 2 is based on OFDM.

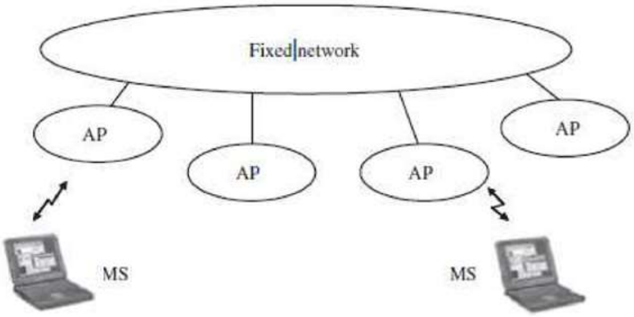
HiperLAN/2 automatically performs handoff to the nearest access point. The access point is basically a radio BS that covers an area of about 30 to 150 meters, depending on the environment. MANETs can also be created easily.

The goals of HiperLAN are as follows:

- QoS (to build multiservice network)
- Strong security
- Handoff when moving between local area and wide areas
- Increased throughput
- Ease of use, deployment, and maintenance
- Affordability
- Scalability

One of the primary features of HiperLAN/2 is its high speed transmission rates (up to 54 Mbps). It uses a modulation method called OFDM to transmit analog signals. It is connection oriented, and traffic is transmitted on bidirectional links for unicast traffic and unidirectional links toward the MSs for multicast and broadcast traffic

This connection oriented approach makes support for QoS easy, which in turn depends on how the HiperLAN/2 network incorporates with the fixed network using Ethernet, ATM, or IP.



The HiperLAN/2 architecture shown in the figure allows for interoperation with virtually any type of fixed network, making the technology both network and application independent.

HiperLAN/2 networks can be deployed at "hot spot" areas such as airports and hotels, as an easy way of offering remote access and internet services.

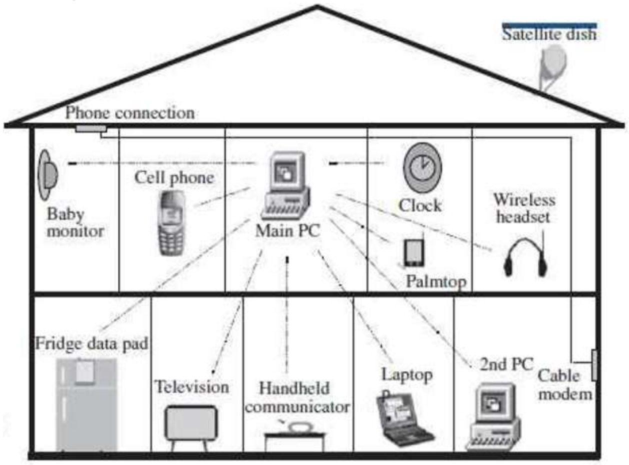
2. Home RF Technology

A typical home needs a network inside the house for access to a public network telephone and internet, entertainment networks (cable television, digital audio and video with the IEEE 1394), transfer and sharing of data and resources (printer, internet connection), and home control and automation.

The device should be able to self-configure and maintain connectivity with the network. The devices need to be plug and play enabled so that they are available to all other clients on the network as soon as they are switched on, which requires automatic device discovery and identification in the system.

Home networking technology should also be able to accommodate any and all lookup services, such as Jini. Home RF products allow you to simultaneously share a single internet connection with all of your computers - without the hassle of new wires, cables or jacks.

Home RF visualizes a home network as shown in the figure:



A network consists of resource providers, which are gateways to different resources like phone lines, cable modem, satellite dish, and so on, and the devices connected to them such as cordless phone, printers and fileservers, and TV.

The goal of Home RF is to integrate all of these into a single network suitable for all applications and to remove all wires and utilize RF links in the network suitable for all applications.

This includes sharing PC, printer, fileserver, phone, internet connection, and so on, enabling multiplayer gaming using different PCs and consoles inside the home, and providing complete control on all devices from a single mobile controller.

With Home RF, a cordless phone can connect to PSTN but also connect through a PC for enhanced services. Home RF makes an assumption that simultaneous support for both voice and data is needed.

Advantages of Home RF

- In Home RF all devices can share the same connection, for voice or data at the same time.
- Home RF provides the foundation for a broad range of interoperable consumer devices for wireless digital communication between PCs and consumer electronic devices anywhere in and around the home.
- The working group includes Compaq computer corp. Ericson enterprise network, IBM Intel corp., Motorola corp. and other.
- A specification for wireless communication in the home called the shared wireless access protocol (SWAP) has been developed.

3. IEEE 802.11 STANDARD

IEEE 802.11 is a set of standards for the wireless area network (WLAN), which was implemented in 1997 and was used in the industrial, scientific, and medical (ISM) band. IEEE 802.11 was quickly implemented throughout a wide region, but under its standards the network occasionally receives interference from devices such as cordless phones and microwave ovens. The aim of IEEE 802.11 is to provide wireless network connection for fixed, portable, and moving stations within ten to hundreds of meters with one medium access control (MAC) and several physical layer specifications. This was later called 802.11a. The major protocols include IEEE 802.11n; their most significant differences lie in the specification of the PHY layer.

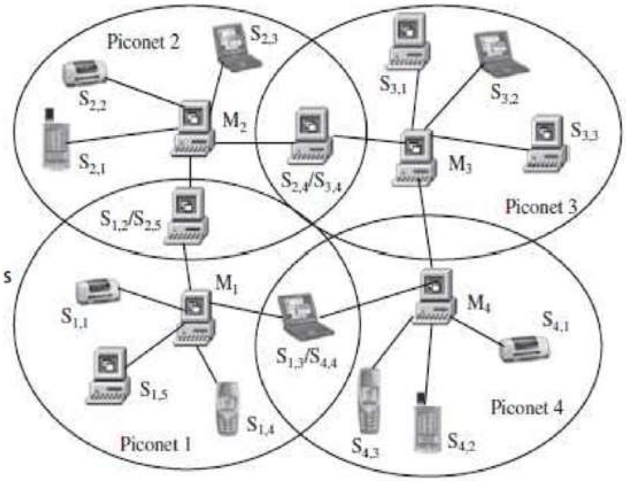
4. BLUETOOTH

Bluetooth is one of the major wireless technologies developed to achieve WPAN (wireless personal area network). It is used to connect devices of different functions such as telephones, computers (laptop or desktop), notebooks, cameras, printers, and so on.

Architecture of Bluetooth

Bluetooth devices can interact with other Bluetooth devices in several ways in the figure. In the simplest scheme, one of the devices acts as the master and (up to) seven other slaves.

A network with a master and one or more slaves associated with it is known as a piconet. A single channel (and bandwidth) is shared among all devices in the piconet.



Each of the active slaves has an assigned 3-bit active member address. many other slaves can remain synchronized to the master though remaining inactive slaves, referred to as parked nodes.

The master regulates channel access for all active nodes and parked nodes. Of two piconets are close to each other, they have overlapping coverage areas.

This scenario, in which nodes of two piconets intermingle, is called a scatternet. Slaves in one piconet can participate in another piconet as either a master or slave through time division multiplexing.

In a scatternet, the two (or more) piconets are not synchronized in either time or frequency. Each of the piconets operates in its own frequency hopping channel, and any devices in multiple piconets participate at the appropriate time via time division multiplexing.

The Bluetooth baseband technology supports two link types. Synchronous connection oriented (SCO) types, used primarily for voice, and asynchronous connectionless (ACL) type, essentially for packet data.

INFRARED VS RADIO TRANSMISSION

INFRARED TRANSMISSION

Infrared technology uses diffuse light reflected at walls, furniture etc. or a directed light if a line of sight (LOS) exists between sender and receiver.

Infrared light is the part of the electromagnetic spectrum, and is an electromagnetic form of radiation. It comes from the heat and thermal radiation, and it is not visible to the naked eyes.

In infrared transmission, senders can be simple light emitting diodes (LEDs) or laser diodes. Photodiodes act as receivers.

Infrared is used in wireless technology devices or systems that convey data through infrared radiation. Infrared is electromagnetic energy at a wave length or wave lengths somewhat longer than those of red light.

Infrared wireless is used for medium and short range communications and control. Infrared technology is used in instruction detectors; robot control system, medium range line of sight laser communication, cordless microphone, headsets, modems, and other peripheral devices.

Infrared radiation is used in scientific, industrial, and medical application. Night vision devices using active near infrared illumination allow people and animals to be observed without the observer being detected.

Infrared transmission technology refers to energy in the region of the electromagnetic radiation spectrum at wavelength longer than those of visible light but shorter than those of radio waves.

Infrared technology allows computing devices to communicate via short range wireless signals. With infrared transmission, computers can transfer files and other digital data bidirectional.

Advantages of infrared

- The main advantage of infrared technology is its simple and extremely cheap senders and receivers which are integrated into nearly all mobile devices available today.
- No licenses are required for infrared and shielding is very simple.
- PDAs, laptops, notebooks, mobile phones etc. have an infrared data association (IrDA) interface.
- Electrical devices cannot interfere with infrared transmission.

Disadvantages of Infrared

- Disadvantages of infrared transmission are its low bandwidth compared to other LAN technologies.
- Limited transfer rates to 115 Kbit/s and we know that even 4 Mbit/s is not a particular high data rate.
- Their main disadvantage is that infrared is quite easily shielded.
- Infrared transmission cannot penetrate walls or other obstacles.
- Typically, for good transmission quality and high data rates a LOS (Line of site), i.e. direct connection is needed.

RADIO TRANSMISSION

Almost all networks use radio waves for data transmission, e.g., GSM at 900, 1800, and 1900 MHz, DECT at 1880 MHz etc. Radio transmission technologies can be used to set up ad-hoc connections for work groups, to connect, e.g., a desktop with a printer without a wire, or to support mobility within a small area.

The two main types of radio transmission are AM (Amplitude Modulation) and (FM) Frequency Modulation.

FM minimizes noise and provides greater reliability. Both AM and FM process sounds in patterns that are always varying of electrical signals.

In an AM transmission the carrier wave has a constant frequency, but the strength of the wave varies. The FM transmission is just the opposite; the wave has constant amplitude but a varying frequency.

Usually the radio transmission is used in the transmission of sounds and pictures. Such as, voice, music and television.

The images and sounds are converted into electrical signals by a microphone or video camera. The signals are amplified, and transmitted. If the carrier is amplified it can be applied to an antenna.

The antenna converts the electrical signals into electromagnetic waves and sends them out or they can be received. The antenna consists commonly of a wire or set of wires.

Advantages of Radio Transmission

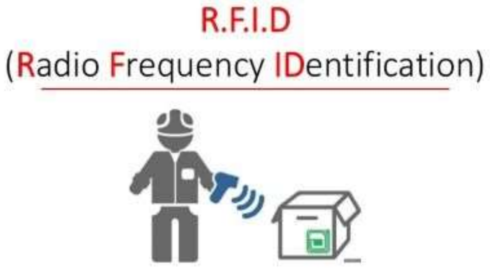
- Advantages of radio transmission include the long-term experiences made with radio transmission for wide area networks (e.g. microwave links) and mobile cellular phones.
- Radio transmission can cover larger areas and can penetrate (thinner) walls, plants, furniture etc.
- Additional coverage is gained by reflection.
- Radio typically does not need a LOS (Line of Site) if the frequencies are not too high.
- Higher transmission rates (e.g. 54 Mbit/s) than infrared (directed laser links, which offer data rates well above 100 Mbit/s).

Disadvantages of Radio Transmission

- Radio transmission can be interfered with other senders, or electrical devices can destroy data transmitted via radio.
- Bluetooth is simple than infrared.
- Radio is only permitted in certain frequency bands.
- Shielding is not so simple.
- Very limited ranges of license free bands are available worldwide and those that are available are not the same in all countries.
- A lot harmonization is going on due to market pressure.

RFID: RADIO FREQUENCY IDENTIFICATION

RFID stands for Radio Frequency Identification. It is a technology which is used to track RFID tags and to capture the data encoded in these tags. It uses radio waves to identify and track tags attached to objects. The tags contain information which is stored electronically. So, it is a type of wireless communication that uses electromagnetic or electrostatic coupling in the radio frequency to identify an object, animal, or person to which a tag is attached. Today, RFID is used in various industries such as automobile, pharmaceuticals, and can also be implanted in livestock and pets to identify them.



How RFID Works?

RFID is an Automatic Identification and Data Capture (AIDC) technology. Using radio waves, it automatically identifies objects, gathers data about them, and enter this data into computer systems with little or no human intervention.

An RFID system comprises three basic components: **a scanning antenna, a transceiver, and a transponder**. The scanning antenna and transceiver are collectively known as RFID reader or interrogator. It is a network-connected device that uses radiofrequency waves to transmit signals that activate the RFID tag. The transponder is located in the RFID tag itself and comprises an integrated circuit and an antenna. After activation, the tag sends a signal back to the antenna or RFID reader, where it is translated into meaningful data. The data is then transferred through a communication interface to a host computer system, where it is stored in a database and analyzed.

Numerical Problems from Data Link Control (DLC) Layer

1. The following code vectors (101101, 110110 and 100011) are generated from a (6,3) parity check code. Find the rule for generating each of the parity checks. What is the minimum distance of this code? What is the error detection and correction capability of this code?

Final answer:

The rule for generating parity checks is inferred from the (6,3) format of the code, and the minimum distance of the given code vectors is 3, which allows for the detection of up to two-bit errors and correction of a one-bit error.

Explanation:

To determine the rule for generating parity checks for the given code vectors (101101, 110110, and 100011) in a (6,3) parity check code, we look at the patterns of ones and zeros. The (6,3) indicates that each code vector is six bits long and encodes three bits of data, with the remaining three bits being parity checks.

The minimum distance of the code can be found by calculating the Hamming distance, which is the number of positions at which the corresponding symbols are different, between each pair of code vectors. Looking at the provided vectors:

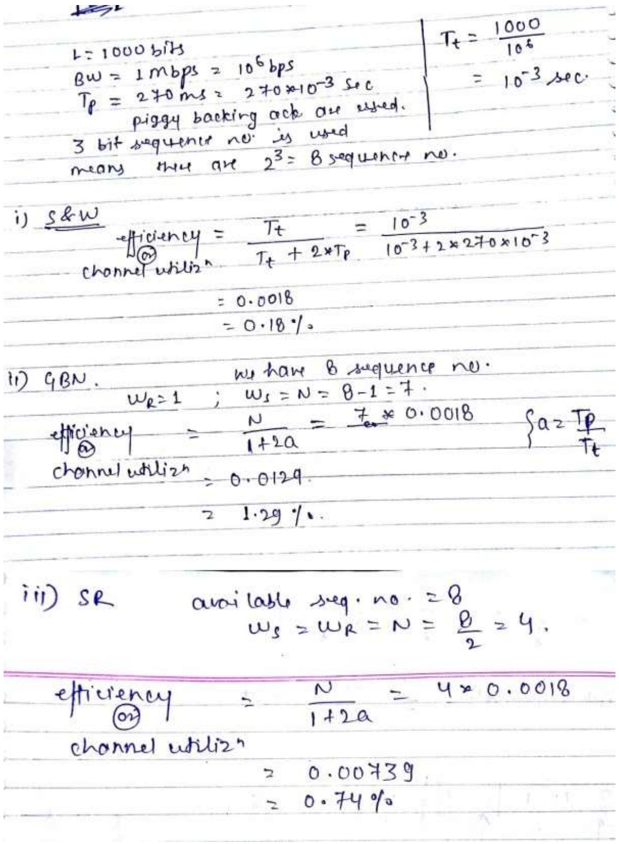
Between 101101 and 110110, the Hamming distance is 3,

Between 101101 and 100011, the Hamming distance is 3, and

Between 110110 and 100011, the Hamming distance is 3.

Since the smallest distance is 3, the minimum distance of this code is 3. This minimum distance indicates error detection and correction capabilities of the code; specifically, it can detect up to two errors and correct one error within the six-bit code.

2. Frames of 1000 bits are sent over a 1 Mbps channel using a geostationary satellite whose propagation time from the earth is 270 msec. Acknowledgements are always piggybacked onto data frames. The headers are very short. Three bit sequence numbers are used. What is the maximum achievable channel utilization for (a) stop-and-wait, (b) go back-n and (c) selective repeat ARQs.



$L = 1000$ bits

$BW = 1\,\text{mbps} = 10^6$ bps

$T_p = 270\,\text{ms} = 270 * 10^{-3}$ sec

piggy backing ack are used.

3 bit sequence no. is used

means there are $2^3 = 8$ sequence no.

$T_t = \frac{1000}{10^6}$

$= 10^{-3}$ sec.

i) S&W

efficiency ⓞʳ channel utiliz^n $= \frac{T_t}{T_t + 2 * T_p} = \frac{10^{-3}}{10^{-3} + 2 * 270 * 10^{-3}}$

$= 0.0018$

$= 0.18\%$

ii) GBN.

we have 8 sequence no.

$W_R = 1$; $W_s = N = 8 - 1 = 7$.

efficiency ⓞʳ channel utiliz^n $= \frac{N}{1+2a} = 7 * 0.0018$ $\left\{ a = \frac{T_p}{T_t} \right.$

$= 0.0129$

$= 1.29\%$.

iii) SR

available seq. no. $= 8$

$W_s = W_R = N = \frac{8}{2} = 4$.

efficiency ⓞʳ channel utiliz^n $= \frac{N}{1+2a} = 4 * 0.0018$

$= 0.00739$

$= 0.74\%$

where L is the frame size

BW is bandwidth

Tt and Tp are transmission delay and propagation delay respectively

3. Consider a (7,4) cyclic code generated by g(x) = x3 + x + 1. (i) Illustrate the encoding procedure with the message vector 1101 using feedback shift register and verify with polynomial division using modulo-2 operations. (ii) Illustrate the decoding procedure for the received code vector corresponding to the transmitted code vector in step (i) with an error at 4th bit position and verify the same with polynomial division using modulo-2 operations.

4.Let Tmin be the minimum transmission time for data frames and Td be the propagation and processing delay in each direction. Find the maximum allowable value Tmax for frame transmission time such that a go-back-n ARQ system will never have to go back or wait in the following cases: (i) absence of transmission errors or lost frames and (ii) isolated errors can occur in the feedback direction.

5.A channel has a bit rate of 4 kbps and a propagation delay of 20 msec. Find what range

of frame sizes does stop and-wait ARQ give an efficiency of at least 50 percent?
Bit rate = 4 kbps
One-way propagation delay = 20 ms

Efficiency = Transmission time of packet/(Transmission time of packet + 2 * Propagation delay)
0.5 = x/(x + 2 * 20 * 10-3)
x = 20 * 10-3
x = 40 * 10-3

Minimum frame size / Bit rate = 40 * 10-3
Therefore, Minimum frame size = 40 * 10-3 * 4 * 103 = 160 bits

6. The generator polynomial for a (15,7) cyclic code is g(x) = 1+x4 +x6 +x7 +x8 . Find the code vector (in systematic form) for the message polynomial m(x) = x2 + x3 + x4 . Assume that the first and last bits of the code vector T (x) for m(x) = x2 + x3 + x4 suffer transmission errors. Find the syndrome s(x) of the received code vector R(x). (syndrome is the reminder obtained by dividing R(x) by g(x).)

7. Design an optimum selective repeat ARQ (optimize the buffer space) for the round trip delay of 40 ms and frame transmission time of 1 ms.
(i) What is the size of sender window and receiver window?
(ii) How many bits are required to represent sequence and request numbers?
(iii) When the sender window will get exhaust (go back)?
(iv) What will be the frame error patterns (repeated frame error) to achieve the channel utilization of 50% and 25%?

8. The following code vectors (1011001, 1001110, and 1100101) are generated from a (7,4) parity check code. Find the rule for generating each of the parity checks. What is the minimum distance of this code? What is the error detection and correction capability of this code? 9. The generator polynomial for a (15,7) cyclic code is g(x) = 1+x4 +x6 +x7 +x8 . Find the code vector for the message 0011100, and draw the encoder circuit for generating the parity bits.

10. If each packet carries 1000 bits of data, how long does it take to send 1 million bits of data using (i) stop and wait ARQ, (ii) go-back-n ARQ and (iii) selective repeat ARQ. Assume that all three ARQs are using 3 bits for representing sequence numbers. The distance between sender and receiver is 5000 Km and the propagation speed is 2 x 108 m? Ignore transmission, waiting and processing delays. Assume no data or control frame is lost or damaged.

11. Design an optimum selective repeat ARQ (optimize the buffer space) for the round trip delay of 40 ms and frame transmission time of 1 ms. (i) What is the size of sender window and receiver window? (ii) How many bits are required to represent sequence and request numbers? (iii) When the sender window will get exhaust (go back)? (iv) What will be the frame error patterns (repeated frame error) to achieve the channel utilization of 50% and 25%

MODULE 4

Network Addressing

Network Addressing is one of the major responsibilities of the network layer.

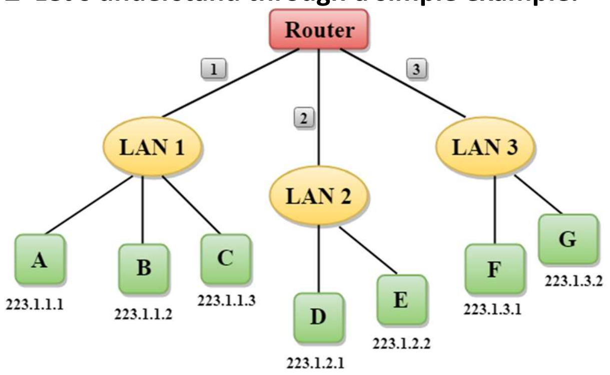
Network addresses are always logical, i.e., software-based addresses.

A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.

A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.

Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

 Let's understand through a simple example.



In the above figure, a router has three interfaces labeled as 1, 2 & 3 and each router interface contains its own IP address.

Each host contains its own interface and IP address.

All the interfaces attached to the LAN 1 is having an IP address in the form of 223.1.1.xxx, and the interfaces attached to the LAN 2 and LAN 3 have an IP address in the form of 223.1.2.xxx and 223.1.3.xxx respectively.

Each IP address consists of two parts. The first part (first three bytes in IP address) specifies the network and second part (last byte of an IP address) specifies the host in the network.

Classful Addressing

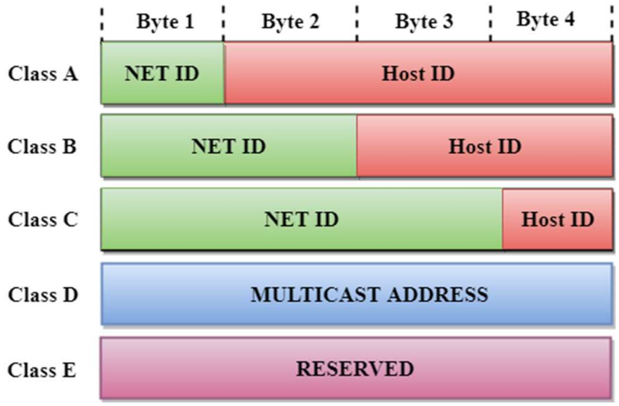
An IP address is 32-bit long. An IP address is divided into sub-classes:

- Class A
- Class B
- Class C
- Class D
- Class E

An ip address is divided into two parts:

Network ID: It represents the number of networks.

Host ID: It represents the number of hosts.



In the above diagram, we observe that each class have a specific range of IP addresses. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

Class A

In Class A, an IP address is assigned to those networks that contain a large number of hosts.

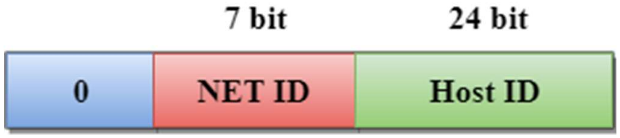
The network ID is 8 bits long.

The host ID is 24 bits long.

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = 2^7 = 128 network address

The total number of hosts in Class A = 2^{24} - 2 = 16,777,214 host address



Class B

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

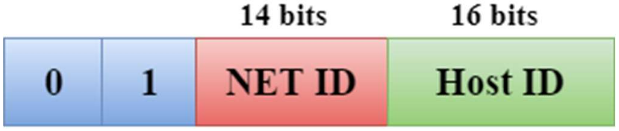
The Network ID is 16 bits long.

The Host ID is 16 bits long.

In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B = 2^{14} = 16384 network address

The total number of hosts in Class B = 2^{16} - 2 = 65534 host address



Class C

In Class C, an IP address is assigned to only small-sized networks.

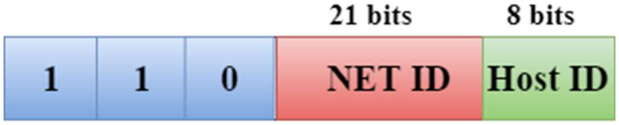
The Network ID is 24 bits long.

The host ID is 8 bits long.

In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

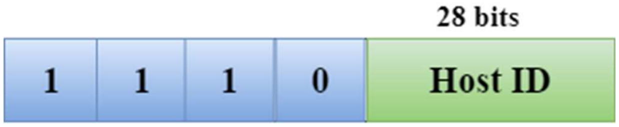
The total number of networks = 2^{21} = 2097152 network address

The total number of hosts = 2^{8} - 2 = 254 host address



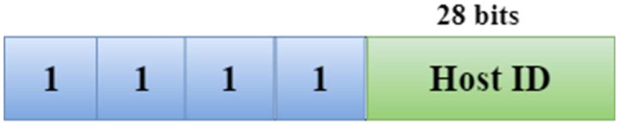
Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.



Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.



Rules for assigning Host ID:

- The Host ID is used to determine the host within any network. The Host ID is assigned based on the following rules:
- The Host ID must be unique within any network.
- The Host ID in which all the bits are set to 0 cannot be assigned as it is used to represent the network ID of the IP address.
- The Host ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Rules for assigning Network ID:

- If the hosts are located within the same local network, then they are assigned with the same network ID. The following are the rules for assigning Network ID:
- The network ID cannot start with 127 as 127 is used by Class A.

Class	Higher bits	NET ID bits	HOST ID bits	No.of networks	No.of hosts per network	Range
A	0	8	24	2^{7}	2^{24}	0.0.0.0 to 127.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 to 191.255.255.255
C	110	24	8	2^{21}	2^{8}	192.0.0.0 to 223.255.255.255
D	1110	Not Defined	Not Defined	Not Defined	Not Defined	224.0.0.0 to 239.255.255.255
E	1111	Not Defined	Not Defined	Not Defined	Not Defined	240.0.0.0 to 255.255.255.255

- The Network ID in which all the bits are set to 0 cannot be assigned as it is used to specify a particular host on the local network.
- The Network ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

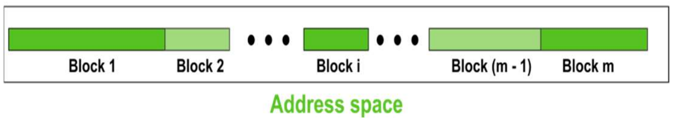
Classful Network Architecture diagram on top

CLASSLESS ADDRESSING

The address depletion issue was not fully resolved by classful addressing's subnetting and supernetting techniques. As the Internet expanded, it became obvious that a bigger address space was required as a long-term fix. However, the expanded address space necessitates that IP addresses should be longer as well, necessitating a change in IP packet syntax. The short-term solution, which uses the same address space but modifies the distribution of addresses to deliver a fair amount to each business, was developed despite the fact that the long-term solution, known as IPv6, has already been developed. ***Classless addressing is the temporary fix, which nevertheless makes use of IPv4 addresses.*** In order to make up for address depletion, the class privilege was taken out of the distribution.

The entire address space is partitioned into blocks of varying lengths with classless addressing. An address's prefix designates the block (network); its suffix designates the node (device). We are capable of having a block of 20, 21, 22 ,..., 232 addresses, theoretically. One of the limitations is that a block of addresses must have a power of two addresses. One address block may be given to an organization. The given figure demonstrates the non-overlapping block segmentation of the entire address space.

Variable-length block in classless addressing



In contrast to classful addressing, classless addressing allows for varying prefix lengths. Prefix lengths that vary from 0 to 32 are possible. The length of the prefix has an inverse relationship with network size. A smaller network has a large prefix; a larger one has a small prefix.

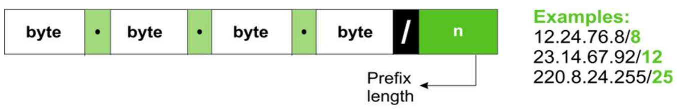
We must stress that classful addressing is just as easily adaptable to the concept of classless addressing. Consider an address in class A as a classless address with a prefix length of 8. Class B addresses can be viewed as classless addresses with the prefix 16 and so on. Putting it another way, ***classless addressing is a specific instance of classful addressing.***

Prefix Length - Slash Notation

In classless addressing, the first issue that needs to be resolved is how to determine the prefix length if an address is provided. We must individually provide the prefix length because it is not a property of the address. The address is inserted in this scenario, followed by a slash, and the prefix length, n. Slash notation is the colloquial name for the notation, while classless interdomain routing, or CIDR (pronounced cider) method, is the official name. An address in classless addressing can thus be expressed as illustrated in the figure below.

To put it another way, we must also provide the prefix length in classless addressing because an address does not automatically define the block or network to which it belongs.

Slash notation (CIDR)



Extracting Information from an Address

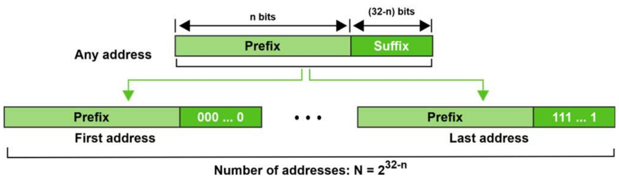
With respect to any given address in the block, we typically like to know three things: the number of addresses in the block, the start address in the block, and the last address. These three pieces of information, which are depicted in the picture below, are simple to locate because the prefix length, n, is known.

The block has N = 232n addresses, according to the calculation.

The n leftmost bits are kept, and the (32 - n) rightmost bits are all set to zeroes to determine the first address.

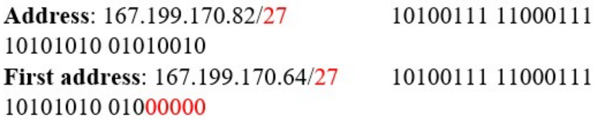
The n leftmost bits are kept, while the (32 - n) rightmost bits are all set to 1s to determine the last address.

Information extraction in classless addressing



For Example - The address 167.199.170.82/27 is a classless address. The following is where we can find the aforementioned three pieces of data. In the network, there are $2^{32-n} = 2^5 = 32$ addresses in all.

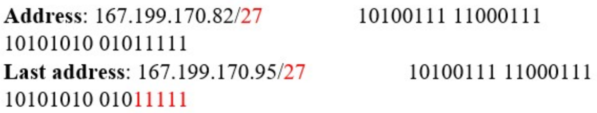
The first 27 bits are kept while the remaining bits are converted to 0s to determine the first address.



Address: 167.199.170.82/27 10100111 11000111 10101010 01010010

First address: 167.199.170.64/27 10100111 11000111 10101010 01000000

Keeping the first 27 bits and turning the remaining bits to 1s will allow you to determine the last address.

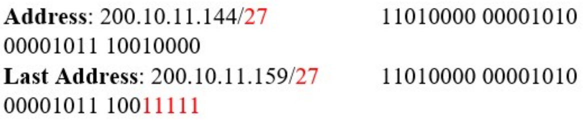


Address: 167.199.170.82/27 10100111 11000111 10101010 01011111

Last address: 167.199.170.95/27 10100111 11000111 10101010 01011111

Quick Quiz *- In the network 200.10.11.144/27, the fourth octet (in decimal) of the last IP address of the network, which can be assigned to a host is ______ (GATE 2015, 2 Marks)*

Ans.



Address: 200.10.11.144/27 11010000 00001010 00001011 10010000

Last Address: 200.10.11.159/27 11010000 00001010 00001011 10011111

Here, the maximum possible value of the last octet is 159 in decimal. Hence, the fourth octet of the last IP address, which can be assigned to a host is 10011110 in binary or 158 in decimal. Hence***, the answer to the question is 158***.

Difference Between Classful and Classless Addressing

IP addresses are divided into five groups using the classful addressing approach when they are assigned. In order to prevent the depletion of IP addresses, classless addressing is used. It is a method of IP address allocation that will eventually replace classful addressing.

A further distinction is the usefulness of classful and classless addressing. Comparatively speaking, classless addressing is more beneficial and useful than classful addressing.

In classful addressing, the network ID and host ID are adjusted according to the classes. However, the distinction between network ID and host ID does not exist with classless addressing. This opens up the possibility of making yet another contrast between both addressing.

IP Address Format and Table

IP address is a short form of "Internet Protocol Address." It is a unique number provided to every device connected to the internet network, such as Android phone, laptop, Mac, etc. An IP address is represented in an integer number separated by a dot (.), for example, 192.167.12.46.

Types of IP Address

An IP address is categorized into two different types based on the number of IP address it contains. These are:

IPv4 (Internet Protocol version 4)

IPv6 (Internet Protocol version 6)

WHAT IS IPV4?

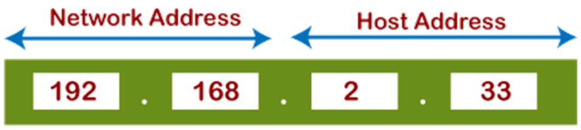
IPv4 is version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by a dot (.), i.e., periods. This address is unique for each device. For example, 66.94.29.13

WHAT IS IPV6?

IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong. IPv6 is the next generation of IP addresses. The main difference between IPv4 and IPv6 is the address size of IP addresses. The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

IP Address Format

Originally IP addresses were divided into five different categories called **classes**. These divided IP classes are class A, class B, class C, class D, and class E. Out of these, classes A, B, and C are most important. Each address class defines a different number of bits for its **network prefix (network address)** and **host number (host address)**. The starting address bits decide from which class an address belongs.

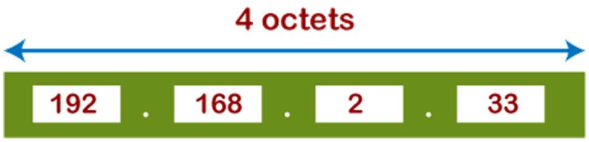


Network Address: The network address specifies the unique number which is assigned to your network. In the above figure, the network address takes two bytes of IP address.

Host Address: A host address is a specific address number assigned to each host machine. With the help of the host address, each machine is identified in your network. The network address will be the same for each host in a network, but they must vary in host address.

ADDRESS FORMAT IPV4

The address format of IPv4 is represented into **4-octets** (32-bit), which is divided into three different classes, namely class A, class B, and class C.



The above diagram shows the address format of IPv4. An IPv4 is a 32-bit decimal address. It contains four octets or fields separated by 'dot,' and each field is 8-bit in size. The number that each field contains should be in the range of 0-255.

CLASS A

Class A address uses only first higher order octet (byte) to identify the network prefix, and remaining three octets (bytes) are used to define the individual host addresses. The class A address ranges between 0.0.0.0 to 127.255.255.255. The first bit of the first octet is always set to 0 (zero), and next 7 bits determine network address, and the remaining 24 bits determine host address. So the first octet ranges from 0 to 127 (00000000 to 01111111).

CLASS B

Class B addresses use the initial two octets (two bytes) to identify the network prefix, and the remaining two octets (two bytes) define host addresses. The class B addresses are range between 128.0.0.0 to 191.255.255.255. The first two bits of the first higher octet is always set to 10 (one and zero bit), and next 14 bits determines the network address and remaining 16 bits determines the host address. So the first octet ranges from 128 to 191 (10000000 to 10111111).

CLASS C

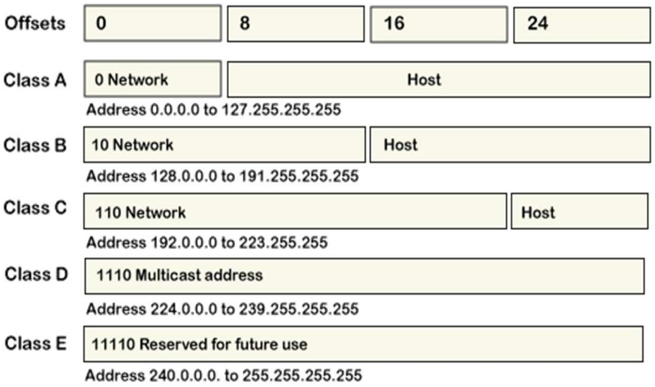
Class C addresses use the first three octets (three bytes) to identify the network prefix, and the remaining last octet (one byte) defines the host address. The class C address ranges between 192.0.0.0 to 223.255.255.255. The first three bit of the first octet is always set to 110, and next 21 bits specify network address and remaining 8 bits specify the host address. Its first octet ranges from 192 to 223 (11000000 to 11011111).

CLASS D

Class D IP address is reserved for multicast addresses. Its first four bits of the first octet are always set to 1110, and the remaining bits determine the host address in any IP address. The first higher octet bits are always set to 1110, and the remaining bits specify the host address. The class D address ranges between 224.0.0.0 to 239.255.255.255. In multicasting, data is not assigned to any particular host machine, so it is not required to find the host address from the IP address, and also, there is no subnet mask present in class D.

CLASS E

Class E IP address is reserved for experimental purposes and future use. It does not contain any subnet mask in it. The first higher octet bits are always set to 1111, and next remaining bits specify the host address. Class E address ranges between 240.0.0.0 to 255.255.255.255.



Offsets 0 8 16 24

Class A 0 Network Host

Address 0.0.0.0 to 127.255.255.255

Class B 10 Network Host

Address 128.0.0.0 to 191.255.255.255

Class C 110 Network Host

Address 192.0.0.0 to 223.255.255

Class D 1110 Multicast address

Address 224.0.0.0 to 239.255.255.255

Class E 11110 Reserved for future use

Address 240.0.0.0. to 255.255.255.255

In every IP address class, all host-number bits are specified by a power of 2 that indicates the total numbers of the host's address that can create for a particular network address. Class A address can contain the maximum number of 2^{24} (16,777,216) host numbers. Class B addresses contain the maximum number of 2^{16} (65, 536) host numbers. And class C contains a maximum number of 2^{8} (256) host numbers.

Subnet address of IP address, understand with an example:

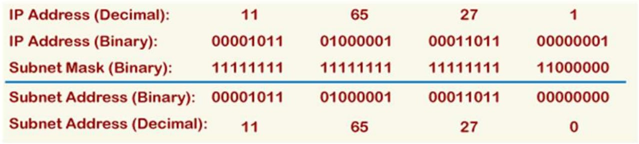
Suppose a class A address is 11.65.27.1, where 11 is a network prefix (address), and 65.27.1 specifies a particular host address on the network. Consider that a network admin wants to use 23 to 6 bits to identify the subnet and the remaining 5 to 0 bits to identify the host address. It can be represented in the *Subnet mask* with all 1 bits from 31 to 6 and the remaining (5 to 0) with 0 bits.

Subnet Mask (binary): 11111111 11111111 11111111 11000000

IP address (binary): 00001011 01000001 00011011 00000001

Now, the subnet can be calculated by applying AND operation (1+1=1, 1+0=0, 0+1=0, 0+0=0)

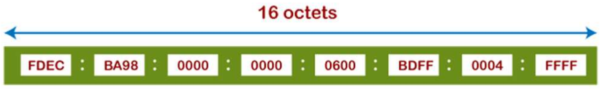
between complete IP address and Subnet mask. The result is:
00001011 01000001 00011011 00000000 = 11.65.27.0 subnet address



IP Address (Decimal):	11	65	27	1
IP Address (Binary):	00001011	01000001	00011011	00000001
Subnet Mask (Binary):	11111111	11111111	11111111	11000000
Subnet Address (Binary):	00001011	01000001	00011011	00000000
Subnet Address (Decimal):	11	65	27	0

IP ADDRESS FORMAT IPV6

All IPv6 addresses are 128-bit hexadecimal addresses, written in 8 separate sections having each of them have 16 bits. As the IPv6 addresses are represented in a hexadecimal format, their sections range from 0 to FFFF. Each section is separated by colons (:). It also allows to removes the starting zeros (0) of each 16-bit section. If two or more consecutive sections 16-bit contains all zeros (0 : 0), they can be compressed using double colons (::).



IPv6 addresses are consist of 8 different sections, each section has a 16-bit hexadecimal values separated by colon (:). IPv6 addresses are represented as following format:
xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx
Each "xxxx" group contains a 16-bit hexadecimal value, and each "x" is a 4-bit hexadecimal value. For example:
FDEC : BA98 : 0000 : 0000 : 0600 : BDFF : 0004 : FFFF
You can also remove the starting zeros (0) of each 16-bit section. For example, the above IPv6 can be rewritten by omitting starting zeros (0) as follow:
FDEC : BA98 : 0 : 0 : 600 : BDFF : 4 : FFFF
You can also compress the consecutive sections 16-bit zeros (0 : 0) using double colons (::). But keep in mind that you can do it only once per IP address.
FDEC : BA98 : : 600 : BDFF : 4 : FFFF

IP ADDRESS TABLE

On the basis of ranges, IP addresses are categorized into five address classes which are given below.

Class	**Higher bits**	**Network address bits**	**Host address bits**	**No. of networks**	**No.of hosts per network**	**Range**
A	0	8	24	2^7	2^{24}	0.0.0.0 to 125.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 to 191.255.255.255
C	110	24	8	2^{21}	2^8	192.0.0.0 to 223.255.255.255
D	1110	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	224.0.0.0 to 239.255.255.255
E	1111	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	240.0.0.0 to 255.255.255.255

DIFFERENCE BETWEEN NETWORK ADDRESS TRANSLATION (NAT) AND PORT ADDRESS TRANSLATION (PAT)

Network Address Translation (NAT) and **Port Address Translation (PAT)** are the two protocols via which we can map the unregistered private (inside local address of an internal network to a registered public (inside global) address of an external network before moving the packet.

The primary distinction is that **NAT** is used to map public IP addresses to private IP addresses in a one-to-one or many-to-one relationships. On the other hand, **PAT** is a sort of **NAT** in which numerous private IP addresses (many-to-one) are mapped into a single public IP address via ports.

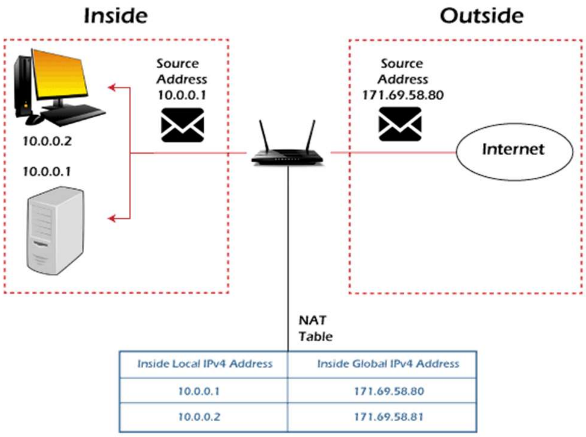
An internal network user with a private IP (unregistered) could not connect to the Internet or external network because each device in the network must have a unique IP address. **NAT** operates on a router connecting two networks together, and translates internal network private addresses (i.e., not globally unique) into legal public addresses.

It was also created with the intention of preserve IP addresses. As the number of internet users grew faster than the restricted number of IP addresses available, internet users faced the problem of IP address scarcity.

The **NAT** and **PAT** protocols are used for a specific reason.

WHAT IS NAT?

NAT (Network Address Translation) connects two networks and maps the private (inside local) addresses into public addresses (inside global). Inside local denotes that the best address belonged to an internal network and was not assigned by a ***Network Information Centre*** or ***service power***. The inside global signifies that the address is a valid address assigned by the **NIC** or service provider, and one or more inside local addresses to the outside world.



Inside Local IPv4 Address	Inside Global IPv4 Address
10.0.0.1	171.69.58.80
10.0.0.2	171.69.58.81

NAT is a method of converting a private IP address or a local address into a public IP address. NAT is a technique for reducing the rate at which available IP addresses are depleted by translating a local IP or private IP address into a global or public IP address. The NAT relation might be one-to-one or many-to-one.

Furthermore, NAT can only configure one address in order to represent the entire network to the outside world. As a result, the translation process is transparent. NAT can be used to migrate and merge networks, share server loads, and create virtual servers, etc.

Types of NAT

There are three types of NAT:

- **Static NAT**
  In static NAT, a local address is mapped to a global address. In this type of NAT, the relationship is one-to-one. Static NAT is used if a host needs a consistent address that must be acceded from the internet. For example, networking devices or enterprise servers.
- **Dynamic NAT**
  Unregistered private IP addresses can be converted to registered public IP numbers from a pool of public IP addresses using dynamic NAT.
- **PAT/NAT Overloading/IP masquerading**
  Among the three varieties, PAT is the most famous. It's a form of Dynamic NAT that's comparable to it, but it uses ports to translate many private IP addresses to a single public IP address.

ADVANTAGES OF NAT

- The following are the advantages of NAT:
- NAT protects the public addresses that have been registered and slow down the IP address space exhaustion.

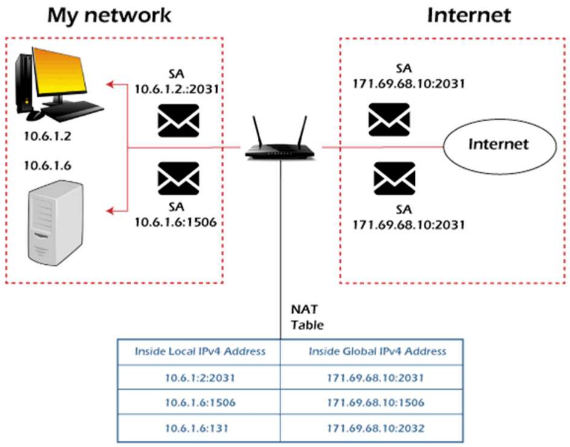
- Removes the address renumbering process that occurs when switching networks
- The occurrence of address overlap was significantly reduced.
- Increases flexibility of the connection establishment.

DISADVANTAGES OF NAT

- The following are the disadvantages of NAT:
- Lack of end-to-end traceability
- Certain applications are not compatible with NAT
- Switching path delays are the outcome of THE TRANSLATION

WHAT IS PAT?

Port Address Translation (PAT) is a sort of Dynamic NAT that allows us to configure address translation at the port level while simultaneously optimising the remaining IP address utilisation. PAT maps numerous source local addresses and ports to a single global IP address and ports from a pool of IP addresses which are routable on the destination network. Here the interface IP address is used in conjunction with the port number, and numerous hosts may have similar IP address because the port number is unique.



Inside Local IPv4 Address	Inside Global IPv4 Address
10.6.1:2:2031	171.69.68.10:2031
10.6.1.6:1506	171.69.68.10:1506
10.6.1.6:131	171.69.68.10:2032

In order to identify the different translations, it uses a unique source port address on the inside global IP address. Because the port number is encoded in 16 bits, the total number of NAT translations that can be performed is 65536.
The original source is preserved by the PAT. If the source port is already allocated, the available ports are searched. The ports groups are split into three ranges 0 to 511,
512 to 1023, and 1024 to 65535.
If PAT doesn't find an available port from the proper port group and if more than one external IPv4 address is configured, PAT moves to the next IPv4 address and tries to allocate the original source port until it runs out of available ports and external IPv4 addresses.

ADVANTAGES OF PAT

- The following are the advantages of PAT:
- Conserve IP addresses by assigning single public IP to a group of hosts using different port numbers.

Basic for Comparison	Network Address Translation (NAT)	Port Address Translation (PAT)
Basic	It converts the private local IP address to the public global IP address.	It is similar to NAT; it also uses port numbers to transform private IP addresses from an internal network to public IP addresses.
Full-Form	The full-form of NAT is Network Address Translation.	The full-form of PAT is Port Address Translation.
Uses	NAT uses an IPv4 address.	PAT uses IPv4 addresses along with the port number.
Relationship	Superset of PAT.	A variant of NAT (a form of a Dynamic NAT)
Types	There are three types of NAT: Static NAT, Dynamic NAT and PAT/NAT Overloading/IP masquerading.	There are two types of PAT: Static PAT and overloaded PAT.

- Lessens security flaws or security attacks as the private address prevent the public address from being exposed.

DISADVANTAGES OF PAT

- The following are the disadvantages of PAT:
- The internal table can only have a certain number of entries to keep track of connections.
- In PAT, more than one instance of the same sort of public service cannot be run from the same IP address.

Key Differences Between NAT and PAT

- PAT is a form of Dynamic NAT
- PAT uses IP addresses along with port numbers, while NAT uses IP addresses along with port numbers
- NAT translates the inside local addresses into inside global addresses; similarly, PAT translates the private unregistered IP addresses into public registered IP addresses. However, unlike NAT, PAT also uses source port numbers, allowing multiple hosts to share a single IP address while using different port numbers.

IPV4 HEADER IN COMPUTER NETWORKS

In this article, we will discuss about IPV4 Header which is a very important topic in Computer Networking.

Introduction

The **Internet Protocol version 4** (IPv4) is a fundamental component of computer networks that serves as the foundation for transmitting data packets across the internet and other interconnected networks. Each data packet transmitted over the internet contains an IPv4 header, which plays a crucial role in routing and delivering data to its intended destination. In this article, we will delve deep into the IPv4 header, exploring its structure, purpose, and the significance it holds in the realm of computer networks.

IPv4 Header Overview

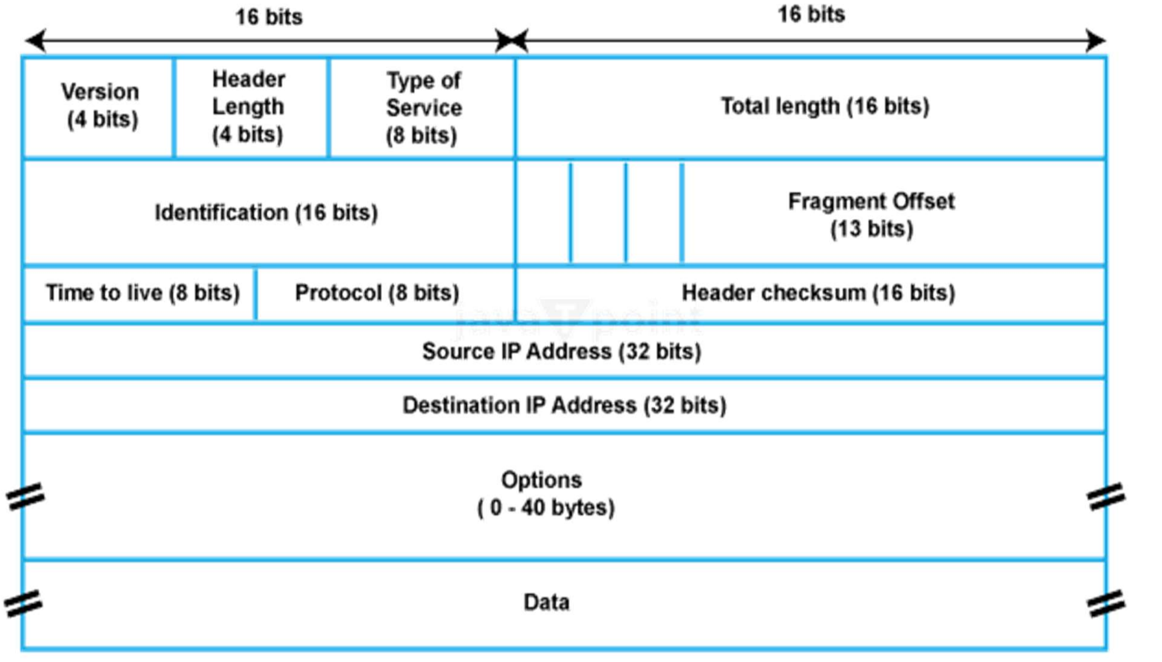
The IPv4 header is a fixed-size, 20-byte (160-bit) data structure that is appended to the beginning of every IPv4 packet. This header contains essential information that routers and networking devices use to route, forward, and deliver data packets from the source to the destination. The IPv4 header is divided into several fields, each serving a specific purpose in the packet delivery process.

Structure of the IPv4 Header

The IPv4 header consists of 12 fields, which are organized in the following manner:

Version (4 bits): This field specifies the version of the IP protocol being used, which is IPv4 in this case.

Header Length (4 bits): The header length field indicates the length of the IPv4 header in 32-bit



IPc4 Header

words. Since the header is a fixed size of 20 bytes, the value of this field is typically 5.

Type of Service (8 bits): This field is used to define the quality of service (QoS) for the packet, including priorities and other parameters for routing and processing.

Total Length (16 bits): The total length field specifies the length of the entire IPv4 packet, including both the header and the data, in bytes.

Identification (16 bits): The identification field is used for packet fragmentation and reassembly. It helps in grouping fragments of a larger packet together.

Flags (3 bits): These bits are used for controlling and identifying packet fragmentation. The flags include the "Don't Fragment" (DF) and "More Fragments" (MF) flags.

Fragment Offset (13 bits): The fragment offset field specifies the position of the fragment within the original packet. It is used to reassemble fragmented packets correctly.

Time to Live (TTL) (8 bits): The TTL field represents the maximum number of hops (routers or network segments) that the packet can traverse before it is discarded. Each router decrements this value by one.

Protocol (8 bits): This field indicates the type of protocol used in the data portion of the packet, such as TCP, UDP, ICMP, or others.

Header Checksum (16 bits): The header checksum field is used to verify the integrity of the IPv4 header during transmission. Routers and devices recalculate this checksum to check for errors.

Source IP Address (32 bits): This field contains the IP address of the sender or source of the packet.

Destination IP Address (32 bits): This field holds the IP address of the recipient or destination of the packet.

PURPOSE OF IPV4 HEADER FIELDS

Version and Header Length: These fields identify the version of the IP protocol and the length of the header, respectively.

Type of Service: The Type of Service field is used to classify packets based on their requirements, allowing for differentiated handling of various types of traffic.

Total Length: This field specifies the overall length of the packet, ensuring that routers and devices can process it correctly.

Identification, Flags, and Fragment Offset: These fields facilitate packet fragmentation and reassembly, crucial for handling large packets that cannot be transmitted in one piece.

TTL: The Time to Live field prevents packets from circulating endlessly in the network by specifying a maximum number of hops they can take.

Protocol: The Protocol field indicates the transport layer protocol used in the packet, enabling routers to forward the packet to the appropriate service.

Header Checksum: This checksum verifies the integrity of the header, reducing the chances of forwarding corrupted packets.

Source and Destination IP Addresses: These fields specify the source and destination of the packet, allowing routers to make routing decisions based on the destination address.

SIGNIFICANCE OF IPV4 HEADER IN ROUTING

The IPv4 header plays a central role in the routing process within computer networks. When a device sends a data packet, it populates the IPv4 header fields with relevant information. Routers along the path to the destination examine the header to determine the next hop and route the packet accordingly. Here's how the header fields influence the routing process:

Source and Destination IP Addresses: Routers use the destination IP address to determine the next hop for the packet. The routing table within each router contains entries that map destination IP addresses to specific interfaces or next-hop routers.

Time to Live (TTL): The TTL field helps in preventing packet loops. Each router that processes the packet decrements the TTL by one. If the TTL reaches zero, the router discards the packet and sends an ICMP Time Exceeded message back to the sender.

Protocol: The Protocol field identifies the transport layer protocol (e.g., TCP, UDP) that the packet carries. Routers use this information to determine how to handle the packet.

Type of Service (TOS): Quality of Service (QoS) mechanisms use the TOS field to prioritize and manage network traffic, ensuring that critical data receives appropriate treatment.

Fragmentation and Reassembly: Routers use the Flags, Identification, and Fragment Offset fields to handle packet fragmentation and reassembly, ensuring that large packets are correctly reconstructed at their destination.

ADDITIONAL CONSIDERATIONS

IPv4 Addressing: The IPv4 header contains the Source and Destination IP Address fields, which are essential for routing. IPv4 addresses are 32-bit numerical labels that uniquely identify devices on a network. These addresses are typically represented in dotted-decimal notation (e.g., 192.168.1.1). IPv4 addresses are divided into classes (A, B, C, D, and E) and can be either public or private.

Classful vs. Classless Routing: In the early days of the internet, IPv4 addressing used a classful routing approach, where IP addresses were divided into fixed classes (A, B, C) based on the range of the first octet. However, this approach was replaced by classless routing (CIDR - Classless Inter-Domain Routing), which allows for more efficient allocation of IP addresses and better route aggregation.

Network Address Translation (NAT): NAT is a technique used in IPv4 networks to conserve public IP addresses. It allows multiple devices on a private network to share a single public IP address. NAT routers modify the source IP address in outgoing packets and maintain a translation table to map incoming traffic to the correct private IP address.

IPv4 Header Options: While we've discussed the standard 20-byte IPv4 header, there are also options that can be included, making the header longer. These options provide additional features and information, such as record route, timestamp, and security options. However, these options are used infrequently and can increase the size of the header.

IPv6 Transition: IPv4 has limitations in terms of available addresses due to its 32-bit address space. IPv6 was developed to overcome this limitation with its 128-bit address space, allowing for an enormous number of unique addresses. The transition from IPv4 to IPv6 is an ongoing process to ensure the continued growth of the internet.

Header Compression: In certain scenarios, such as in wireless networks or virtual private networks (VPNs), header compression techniques are employed to reduce the overhead introduced by the IPv4 header. These techniques help optimize network performance by minimizing the size of transmitted packets.

Security Concerns: The IPv4 header, like any other part of the IP packet, is susceptible to various security threats, including IP spoofing, packet sniffing, and denial-of-service (DoS) attacks. Security measures such as IPsec (IP Security) can be employed to encrypt and authenticate IP packets, providing a layer of protection for data in transit.

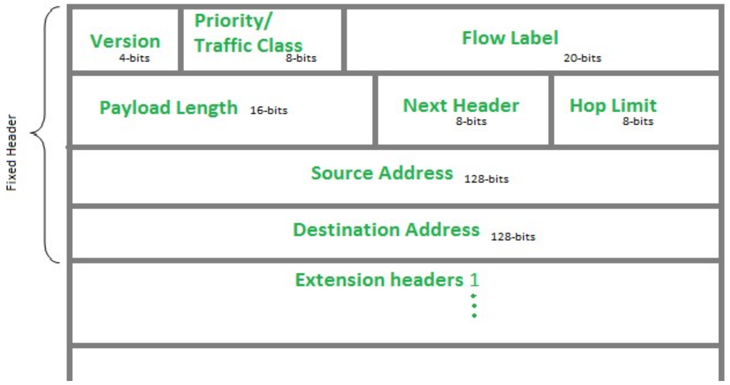
IPv4 Header Limitations: While IPv4 has served as the workhorse of the internet for several decades, it has some limitations, including address exhaustion, scalability issues, and limited support for modern networking features. These limitations have driven the adoption of IPv6 as the next-generation internet protocol.

Legacy Support: Despite the transition to IPv6, IPv4 is still widely used, and many networks continue to operate with IPv4 infrastructure. Various mechanisms, such as dual-stack operation and network address translation (NAT64), have been implemented to facilitate communication between IPv4 and IPv6 networks.

INTERNET PROTOCOL VERSION 6 (IPV6) HEADER

IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. Let's look at the header of IP version 6 and understand how it is different from the IPv4 header.

IP version 6 Header Format :

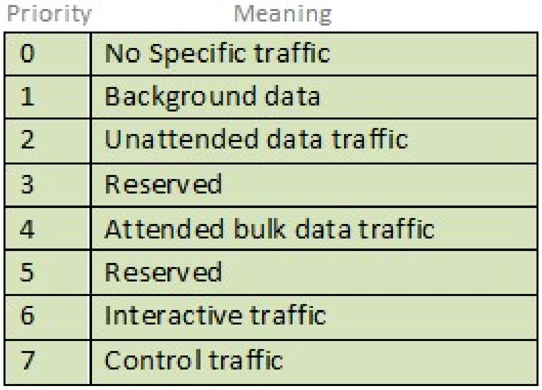


Version (4-bits): Indicates version of Internet Protocol which contains bit sequence 0110.

Traffic Class (8-bits): The Traffic Class field indicates class or priority of IPv6 packet which is similar to *Service Field* in IPv4 packet. It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded.

As of now, only 4-bits are being used (and the remaining bits are under research), in which 0 to

7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic. Priority assignment of Congestion controlled traffic :



Priority	Meaning
0	No Specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

Uncontrolled data traffic is mainly used for Audio/Video data. So we give higher priority to Uncontrolled data traffic.
The source node is allowed to set the priorities but on the way, routers can change it. Therefore, the destination should not expect the same priority which was set by the source node.

Flow Label (20-bits): Flow Label field is used by a source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality of service or real-time service. In order to distinguish the flow, an intermediate router can use the source address, a destination address, and flow label of the packets. Between a source and destination, multiple flows may exist because many processes might be running at the same time. Routers or Host that does not support the functionality of flow label field and for default router handling, flow label field is set to 0. While setting up the flow label, the source is also supposed to specify the lifetime of the flow.

Payload Length (16-bits): It is a 16-bit (unsigned integer) field, indicates the total size of the payload which tells routers about the amount of information a particular packet contains in its payload. The payload Length field includes extension headers(if any) and an upper-layer packet. In case the length of the payload is greater than 65,535 bytes (payload up to 65,535 bytes can be indicated with 16-bits), then the payload length field will be set to 0 and the jumbo payload option is used in the Hop-by-Hop options extension header.

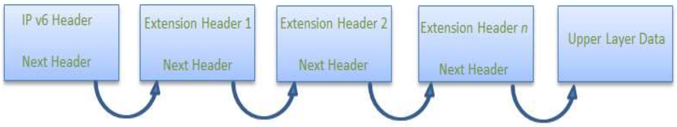
Next Header (8-bits): Next Header indicates the type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper-layer packets, such as TCP, UDP.

Hop Limit (8-bits): Hop Limit field is the same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and the packet is discarded if the value decrements to 0. This is used to discard the packets that are stuck in an infinite loop because of some routing error.

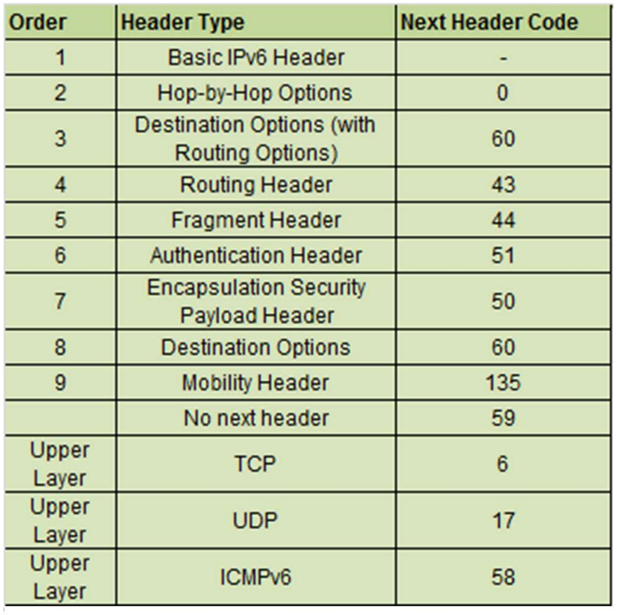
Source Address (128-bits): Source Address is the 128-bit IPv6 address of the original source of the packet.

Destination Address (128-bits): The destination Address field indicates the IPv6 address of the final destination(in most cases). All the intermediate nodes can use this information in order to correctly route the packet.

Extension Headers: In order to rectify the limitations of the *IPv4 Option Field*, Extension Headers are introduced in IP version 6. The extension header mechanism is a very important part of the IPv6 architecture. The next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.

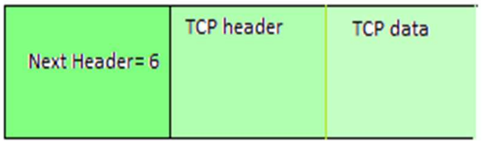


IPv6 packet may contain zero, one or more extension headers but these should be present in their recommended order:

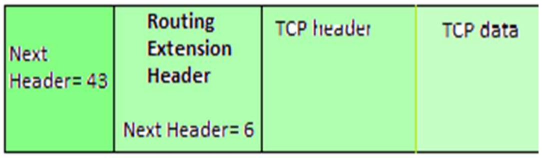


Order	Header Type	Next Header Code
1	Basic IPv6 Header	-
2	Hop-by-Hop Options	0
3	Destination Options (with Routing Options)	60
4	Routing Header	43
5	Fragment Header	44
6	Authentication Header	51
7	Encapsulation Security Payload Header	50
8	Destination Options	60
9	Mobility Header	135
	No next header	59
Upper Layer	TCP	6
Upper Layer	UDP	17
Upper Layer	ICMPv6	58

Example: *TCP is used in IPv6 packet*



Example2:



Rule: Hop-by-Hop options header(if present) should always be placed after the IPv6 base header.

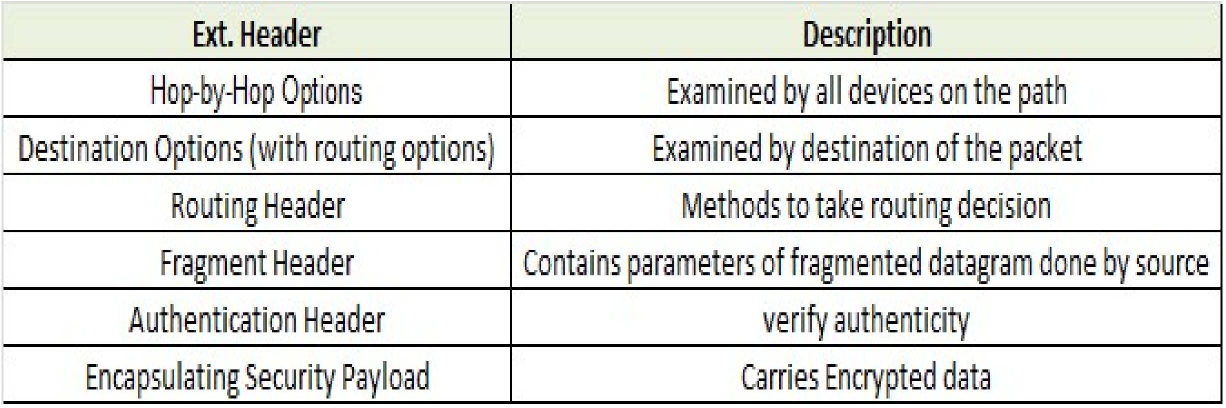
Conventions :

Any extension header can appear at most once except Destination Header because Destination Header is present two times in the above list itself.

If Destination Header is present before Routing Header then it will be examined by all intermediate nodes specified in the routing header.

If Destination Header is present just above the Upper layer then it will be examined only by the Destination node.

Given order in which all extension header should be chained in IPv6 packet and working of each extension header



Ext. Header	Description
Hop-by-Hop Options	Examined by all devices on the path
Destination Options (with routing options)	Examined by destination of the packet
Routing Header	Methods to take routing decision
Fragment Header	Contains parameters of fragmented datagram done by source
Authentication Header	verify authenticity
Encapsulating Security Payload	Carries Encrypted data

: