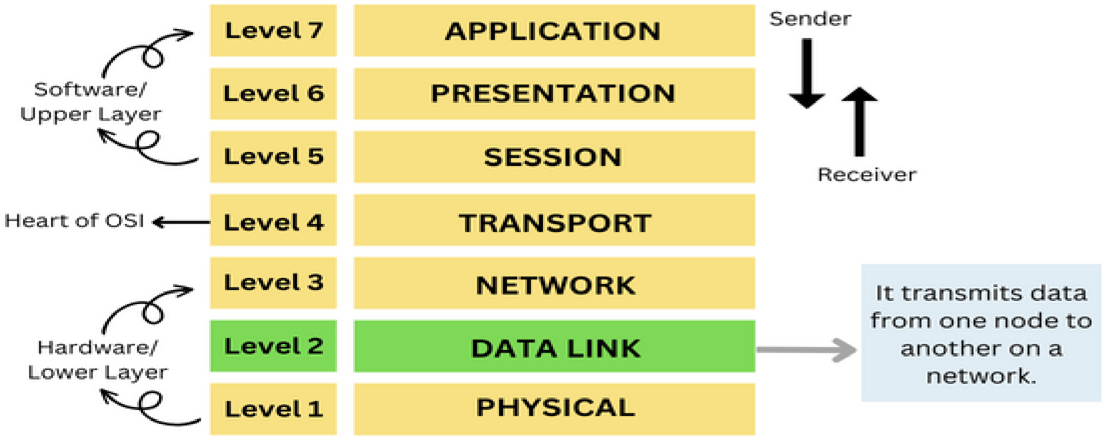
Unit 2: Data Link Layer

- Main Functions, Framing, Error Control, Flow Control, Error Correcting Codes, Error-Detecting Codes,
- Data Link Protocols: Stop-and-Wait Protocol, One-Bit Sliding Window Protocol, Go Back N, Selective Repeat,
- HDLC Queuing Models: Poisson Process, Markov Chain, M/M/1 Queue-delay and little’s formula. M/M/S/K, Queues – average queue length, delay and waiting times. M/G/1 Queues
- Medium Access Control Sublayer: Channel Allocation: Static, Dynamic, MAC PROTOCOLS – ALOHA, CSMA, Collision-Free Protocols, Limited-Contention Protocols, Detailed Study of Ethernet, 802.11 WIRELESS LANS

Topic: data link layer

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

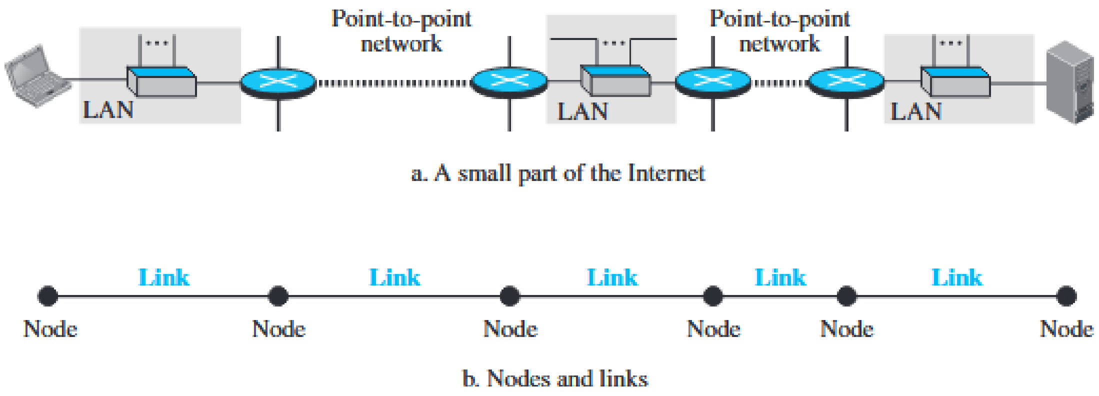


The OSI Model: Data Link Layer

Nodes and Links

Communication at the data-link layer is node-to-node. A data unit from one point in the Internet needs to pass through many networks (LANs and WANs) to reach another point. Theses LANs and WANs are connected by routers. It is customary to refer to the two end hosts and the routers as nodes and the networks in between as links.

Figure 9.2 *Nodes and Links*



Two Categories of Links

Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Systems on broadcast network are said to be on same link. The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain.

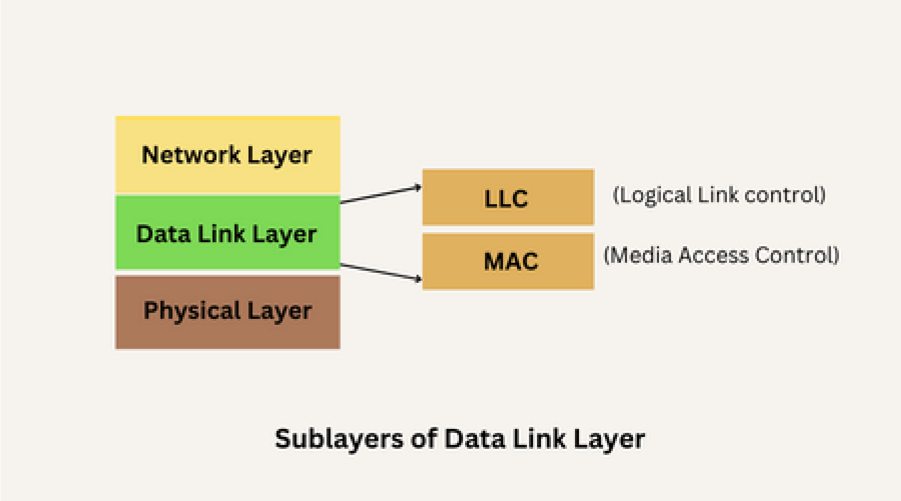
We can have a point-to-point link or a broadcast link. In a point-to-point link, the link is dedicated to the two devices; in a broadcast link, the link is shared between several pairs of devices. For example, when two friends use the traditional home phones to chat, they are using a point-to-point link; when the same two friends use their cellular phones, they are using a broadcast link (the air is shared among many cell phone users).

Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

Two Sublayers

Data link layer has two sub-layers:

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



Sublayers of Data Link Layer

Functionality of Data-link Layer

Data link layer does many tasks on behalf of upper layer. These are:

- **Framing**

  Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.

- **Addressing**

Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.

- **Synchronization**

When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

- **Error Control**

Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.

At the sending node, a frame in a data-link layer needs to be changed to bits, trans- formed to electromagnetic signals, and transmitted through the transmission media. At the receiving node, electromagnetic signals are received, transformed to bits, and put together to create a frame. Since electromagnetic signals are susceptible to error, a frame is susceptible to error. The error needs first to be detected. After detection, it needs to be either corrected at the receiver node or discarded and retransmitted by the sending node.

- **Flow Control**

Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on same speed.

Whenever we have a producer and a consumer, we need to think about flow control. If the producer produces items that cannot be consumed, accumulation of items occurs. The sending data-link layer at the end of a link is a producer of frames; the receiving data-link layer at the other end of a link is a consumer. If the rate of produced frames is higher than the rate of consumed frames, frames at the receiving end need to be buffered while waiting to be consumed (processed). Definitely, we cannot have an unlimited buffer size at the receiving side. We have two choices. The first choice is to let the receiving data-link layer drop the frames if its buffer is full. The second choice is to let the receiving data-link layer send a feedback to the sending data-link layer to ask it to stop or slow down. Different data-link-layer protocols use different strategies for flow control.

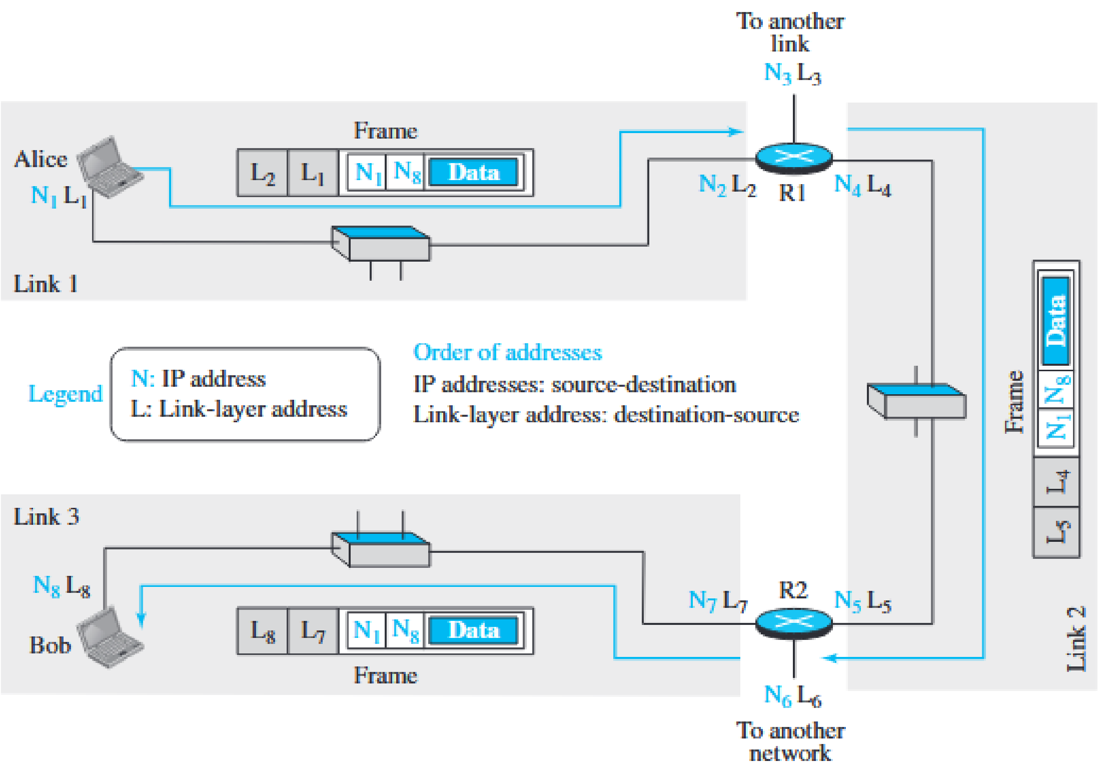
- **Multi-Access**

  When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

LINK-LAYER ADDRESSING

A link-layer address is sometimes called a link address, sometimes a physical address, and some- times a MAC address. We use these terms interchangeably in this book. Since a link is controlled at the data-link layer, the addresses need to belong to the data-link layer. When a datagram passes from the network layer to the data-link layer, the datagram will be encapsulated in a frame and two data-link addresses are added to the frame header. These two addresses are changed every time the frame moves from one link to another.

Figure 9.5 *IP addresses and link-layer addresses in a small internet*



TOPIC: DATA-LINK LAYER PROTOCOLS

Flow Control In the Network

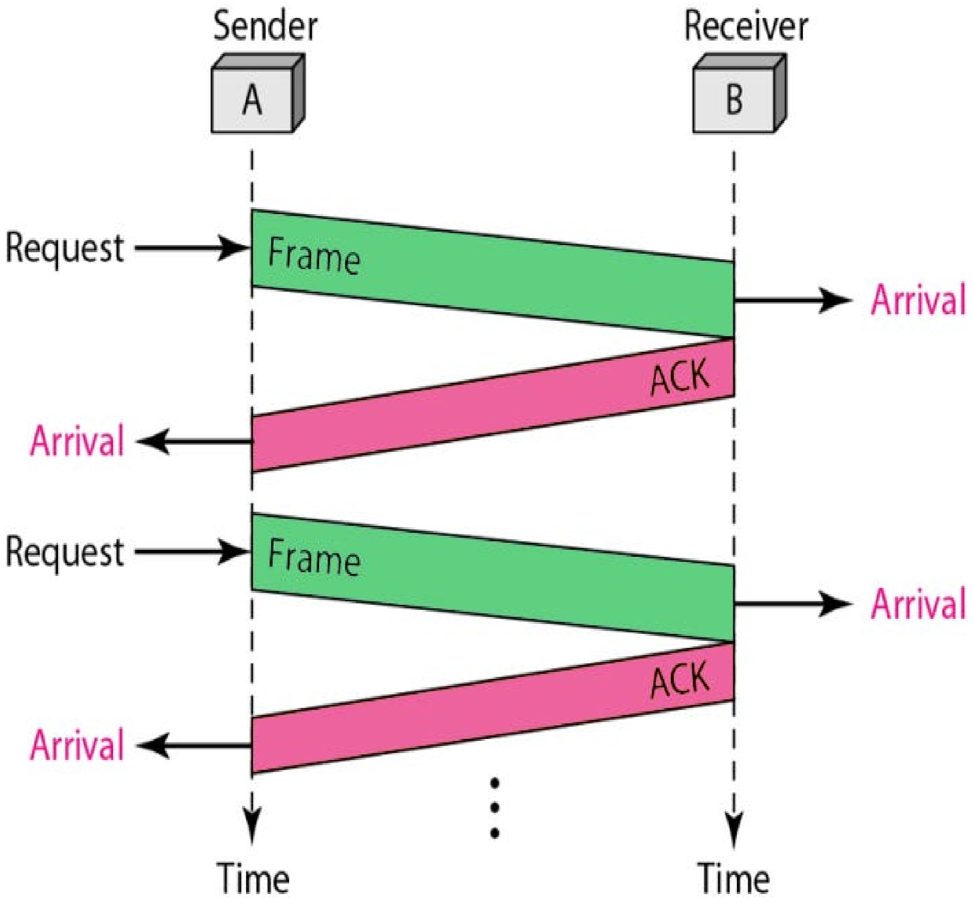
The handling of data flow between different nodes, such as computers, printers, and wireless devices, is referred to as flow control in the network. It is an essential mechanism for effectively transmitting data in the network. Data flow is a serious concern when transmitting data from one node to another. It is caused when the receiving node is unable to handle the data. The data transmitted is more than the receiving node can manage. This leads to data loss and re-transmission of the =data frames.

In order to prevent data loss and effectively transmit data in the network, flow control instructs the sending node about how much data should be retransmitted to the receiving node. The node transmitting the data should wait for an acknowledgment from the receiving node before sending additional data frames into the network.

The flow control protocols that determine the mechanism used to send acknowledgment and retransmit data are **Stop and Wait, GoBackN, and Selective Repeat.**

Stop And Wait Protocol

- This is the most simple protocol that ensures guaranteed transmission of the data in the network.
- Here the stop and wait refer to the two steps performed by the protocols. **The sender node transmits the data into the network.** The data frame is sent sequentially in one by one manner. Once a data frame is transmitted in the network. **The sending node waits for the receiving node to send an acknowledgment in the network.**
- The stop and wait protocol is implemented as a flow control mechanism when the data link layer in the network provides the flow control services. This data link protocol enables the sender to transmit the data over **noiseless channels.**
- This protocol supports **unidirectional data transmission in the network.** This means that there is only one sender or receiver in the network. Both nodes cannot simultaneously send or receive the data in the network. The nodes cannot utilize the resources of the network. The protocol ensures that the data flow is maintained in the network, but it lacks any error control mechanism to the network.

- The primary concept behind implementing this protocol is that whenever the sender node transmits a data frame in the network, it waits for an acknowledgment from the receiver. Only when the acknowledgment is received it transmit to the other node in the network. The transmission is halted if the acknowledgment is received.
- The idea behind using this frame is that when the sender sends the frame, he waits for the acknowledgment before sending the next frame.
- Before discussing GoBackN and Selective Repeat protocols, the user must have prior knowledge of another important protocol: the sliding window protocol.
- 

Sliding Window Protocol

The Sliding Window Protocol is a mechanism that allows the data-transmitting node to transmit multiple data frames simultaneously in the network. This protocol manages the data packets shared between two nodes where reliable and guaranteed data frame delivery is required. This protocol is implemented in the TCP (Transmission Control Protocol).

In this protocol, each data frame is assigned a sequence number. This protocol is implemented to ensure that the successfully transmitted data is not transmitted again by the sender node. This is useful as it increases the efficiency of the network and avoids duplicate data. The sequence number is unique for each data frame and used to confirm whether the receiving node successfully receives the data frame.

Two types of Sliding Window Protocols can be implemented in the network:

- Go-Back-N ARQ
- Selective Repeat ARQ

Go-Back-N ARQ

- In Go-Back-N ARQ, N stands for the Window size of the sender node, and ARQ stands for Automatic Repeat Request. Let us consider an example to explain this protocol where the sender window size is 3. this means that the sender node can transmit three data frames before waiting for an acknowledgment from the receiving node.
- The nodes use protocol pipelining that allows the nodes to transmit multiple data frames in the network simultaneously without waiting for the acknowledgment of the first frame. Suppose the sender needs to send 5 data frames in the network. If the protocol Go-Back-3 is implemented, the user can send frame 1, frame 2, and frame 3 simultaneously without waiting for the acknowledgment of frame 1.
- Since multiple data frames are transmitted in this protocol, each data frame sent is numbered sequentially. This step is performed to ensure that each

data frame can be differentiated. These numbers are referred to as sequential numbers.

- The number of frames that can be sent simultaneously may differ with the sending node. The sender window size determines it. We can say that N data frames can be sent simultaneously in the network before the sender node receives the acknowledgment for the first frame sent to the receiver.
- If the sender does not receive an acknowledgment from the receiver node within an agreed-upon time, then all the data frames transmitted and stored in the current window are retransmitted by the sender. Suppose the sender has transmitted frame 1, frame 2, and frame 3 and does not receive the acknowledgment for frame 1; then all three frames will be retransmitted.

Selective Repeat ARQ

- Selective Repeat ARQ is also called the Selective Repeat Automatic Repeat Request. This protocol is implemented in the data link layer of the OSI model. This protocol implements a sliding window method to transmit the data frames in the network.
- If there are limited mistakes during the data frame transmission, then the user can implement Go-Back-N ARQ, but if there are a lot of errors, then implementing Selective Repeat ARQ is the best option. It works well in a limited bandwidth.
- The window size for both the sender and receiver nodes is kept equal. This is done by making the window size for the sender node equal to the receiver node window. The sliding window is always more than 1.
- Suppose a corrupt frame is transmitted in the network. When this corrupt data frame reaches the receiver node, it is not directly rejected by the receiver; instead, the receiving node transmits a negative acknowledgment to the sender. Upon receiving the negative acknowledgment, the sender

resends the data frame instantly. There is no waiting for any time out to transmit that data frame.

Difference Between Stop and Wait Protocol and Sliding Window Protocol

These two protocols act as a flow control mechanism and can be implemented in the network that ensures that the data is successfully transmitted from the sender node to receiving node since Go-Back-N and Selective Repeat protocols are sliding window protocols.

Let us discuss the difference between Stop and Wait Protocol and Sliding Window Protocol.

BASIS FOR COMPARISON	**STOP-AND-WAIT PROTOCOL**	**SLIDING WINDOW PROTOCOL**
Behaviour	Request and reply	Simultaneous transmit
Number of data frames transferred simultaneously	The nodes cannot fully utilize the network capabilities as only one data frame is transferred at a time.	Multiple frames can be transmitted together.
Efficiency	It is less efficient when compared to sliding window protocols.	Both Go-Back-N and selective repeat protocols are more efficient than the Stop and Wait Protocol. Selective Repeat protocol is the most efficient.
Acknowledgement	The sender node waits for acknowledgment from the	Both protocols can transmit multiple data frames in the

	receiving node after transmitting each data frame in the network.	network before waiting for an acknowledgment. They maintain a Window of Acknowledgement to determine the frames they can wait before getting acknowledged.
Type of transmission	It uses half-duplex communication; that is, there can be only one sender and one receiver at a time. Both nodes cannot simultaneously transmit and receive the data.	It uses full duplex transmission of communication. This allows bi-directional transmission in the network. Both nodes can transmit and receive data nodes simultaneously.
Propagation delay	The propagation delay is longer in the stop and wait protocol.	It is comparatively less for sliding window protocol.
Link utilisation	The link utilization is less efficient.	It is better at link utilization.

Difference Between Go-Back-N and Selective Repeat

The two sliding window protocol also differs in their function and working. The difference between Go-Back-N and Selective Repeat protocols are as follows:

BASIS FOR COMPARISON	**GO-BACK-N**	**SELECTIVE REPEAT**

Basic	Retransmits all the frames that sent after the frame which suspects to be damaged or lost.	Retransmits only those frames that are suspected to lost or damaged.
Bandwidth Utilization	If the possibility of error in transmission is high or a lot of corrupt frames are transmitted, then this protocol wastes a lot of bandwidth.	Since only the erroneous or corrupted data frames are retransmitted in the network. It saves network bandwidth and is more efficient than the Go-Back-N protocol.
Complexity	The implementation of this protocol is simpler than selective repeat. It is less complex because of its less logical implementation.	It is more complex than the Go-Back-N protocol as additional logic and sorting algorithm is applied at both the sender and receiver node. Moreover, it also requires additional storage to work efficiently.
Window size	N-1	<= (N+1)/2
Sorting	Sorting of the data frames is not performed at either end of the transmission.	The sorting of data frames is done at the receiving end. It is necessary to maintain the correct sequential order of the data frame to ensure the correct frame is requested.
Storing	Receivers do not store the frames received after the	The receiver stores the frames received after the

	damaged frame until the damaged frame is retransmitted.	damaged frame in the buffer until the damaged frame is replaced.
Searching	It does not perform a search as all the nodes in the current window are represented if the sender does not receive acknowledgment of a frame. Search is not performed at either end of transmission.	The sender needs to perform a search operation as only the requested node is retransmitted in the network.
ACK Numbers	NAK number represents the expected frame number of the next data frame in the network.	NAK number represents the number of the data frame that is lost during transmission.
Use	It is more used because it is less complex and requires less storage.	It is less implemented. It is used where the bandwidth is limited, and efficiency is important.

Difference between Stop and Wait, Go-Back-N, and Selective Repeat

The following table differentiates between all three flow control protocols that are Stop and Wait, Go-Back-N, and Selective Repeat protocols:

BASIS FOR COMPARISON	**STOP AND WAIT PROTOCOL**	**GO-BACK-N PROTOCOL**	**SELECTIVE REPEAT PROTOCOL**

Sender Window Size	The sender window size is 1. This means that only 1 data frame can be transmitted at a time by the sender.	The window size of the sender node is N in the Go-Back-N protocol.	The Window size of the sender node is greater than 1. It is also N for selective repeat protocol.
Receiver Window Size	The size of the receiver window is also 1 in the stop and wait protocol.	The size of the receiver window is 1.	The size of both the sender and receiver window is equal to implement selective repeat. Thus, it is N in this protocol.
Minimum Sequence Number	Since one data frame is transmitted at a time. The possible minimum sequence number is 2.	The possible minimum sequence number for the Go-Back-N protocol is N+1. Here N is the number of data frames transmitted by the sender.	The possible minimum sequence number for the Selective Repeat protocol is 2N. Here N is the number of data frames transmitted by the sender.
Efficiency of the Protocol	It is the least efficient protocol. The formula to compute the efficiency is	The formula to compute the efficiency is N/(1+2*a), where a represents the ratio	The formula to compute the efficiency is N/(1+2*a), where a represents the ratio

	1/(1+2*a), where a represents the ratio of propagation delay to transmission delay.	of propagation delay to transmission delay and N represents the data packets transmitted in the network.	of propagation delay to transmission delay and N represents the data packet transmitted in the network.
Acknowledgement Type	The receiver node acknowledges each data frame is successfully transmitted individually.	It sends a cumulative acknowledgment for the data frames to the sender node.	In selective repeat, the acknowledgment is individual for each frame.
Supported Order	At the receiving node of the Stop and Wait protocol, no specific order is needed.	It only accepts in-order delivery at the receiver node in this protocol.	In Selective Repeat ARQ, the receiver node only accepts out-of-order delivery in the network.
Retransmissions	Since the sender waits for each data frame to be acknowledged. Therefore, if a packet is dropped, then it is immediately	All the data frames in the current window are retransmitted by the sender node if it does not receive the acknowledgment for the data frame.	In selective repeat protocol, only the erroneous data frames are retransmitted. Thus, the number of retransmission is 1.

	retransmitted. Therefore, the number of transmissions is 1.	Thus, the number of retransmission is N.	

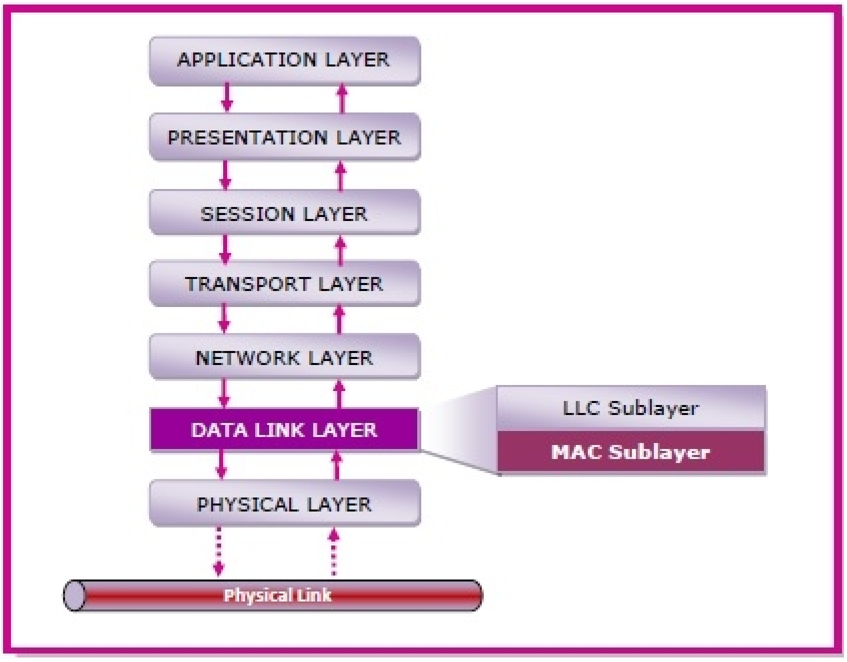
Conclusion

Go-Back-N and Selective Repeat both use Sliding Window Protocol that enables the sender node to transmit multiple data frames simultaneously in the network. The sender node does not require waiting for the acknowledgment from the receiver node to send several data frames.

The Stop-and-Wait protocol is different from the sliding window protocol as this protocol cannot transmit multiple data frames simultaneously in the network. It only allows the sender to node sends one data frame at a time. The sender waits for an acknowledgment after transmitting each data frame in the network. If it does not receive the data frame in a given time, it then retransmits the frame.

Topic: MAC SUBLAYER

The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.



TOPIC: Channel Allocation: Static, Dynamic

When there are more than one user who desire to access a shared network channel, an algorithm is deployed for channel allocation among the competing users. The network channel may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum. Channel allocation algorithms allocate the wired channels and bandwidths to the users, who may be base stations, access points or terminal equipment.

Channel Allocation Schemes

Channel Allocation may be done using two schemes –

- Static Channel Allocation
- Dynamic Channel Allocation

Static Channel Allocation

In static channel allocation scheme, a fixed portion of the frequency channel is allotted to each user. For N competing users, the bandwidth is divided into N channels using frequency division multiplexing (FDM), and each portion is assigned to one user.

This scheme is also referred as fixed channel allocation or fixed channel assignment.

In this allocation scheme, there is no interference between the users since each user is assigned a fixed channel. However, it is not suitable in case of a large number of users with variable bandwidth requirements.

Dynamic Channel Allocation

In dynamic channel allocation scheme, frequency bands are not permanently assigned to the users. Instead channels are allotted to users dynamically as needed, from a central pool. The allocation is done considering a number of parameters so that transmission interference is minimized.

This allocation scheme optimises bandwidth usage and results is faster transmissions.

TOPIC: MAC PROTOCOLS – ALOHA, CSMA, Collision-Free Protocols, Limited-Contention Protocols

- 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

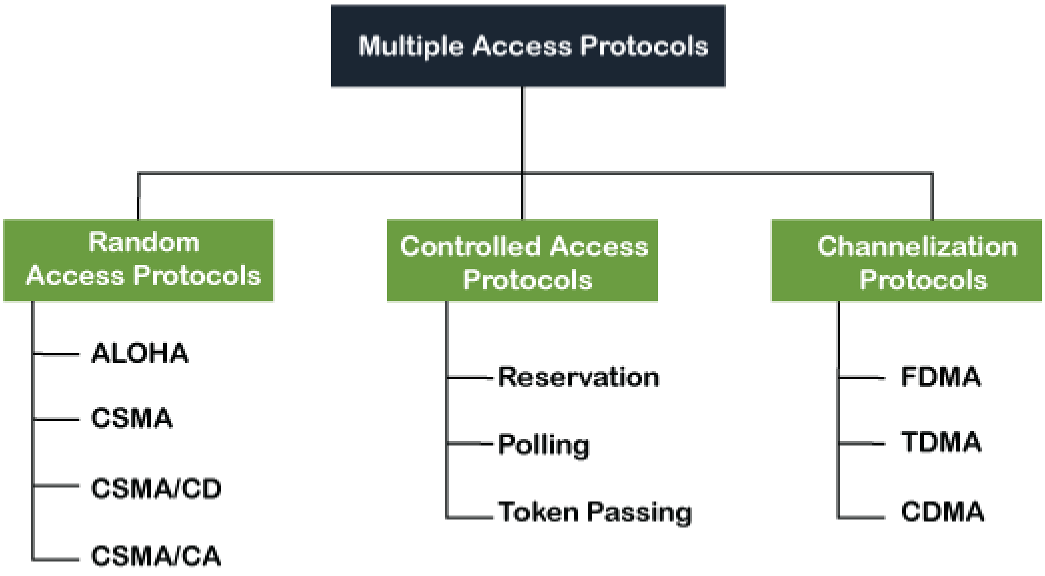
A data link control is a reliable channel for transmitting data over a dedicated link using various techniques such as framing, error control and flow control of data packets in the computer network.

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:



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

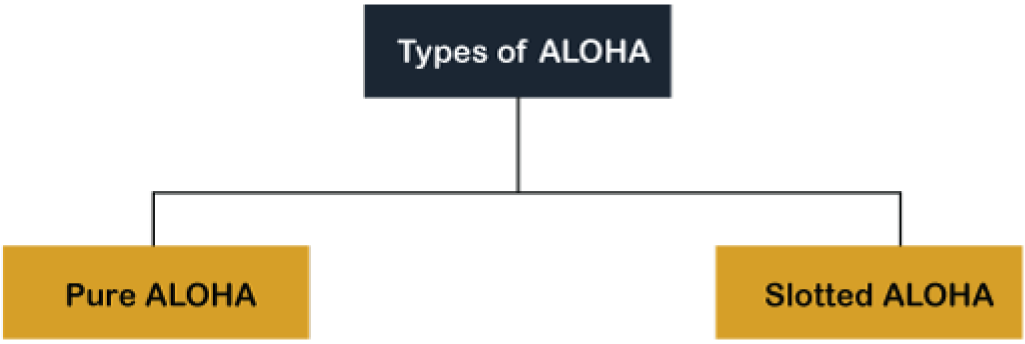
ALOHA Random Access Protocol

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

1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.

3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.

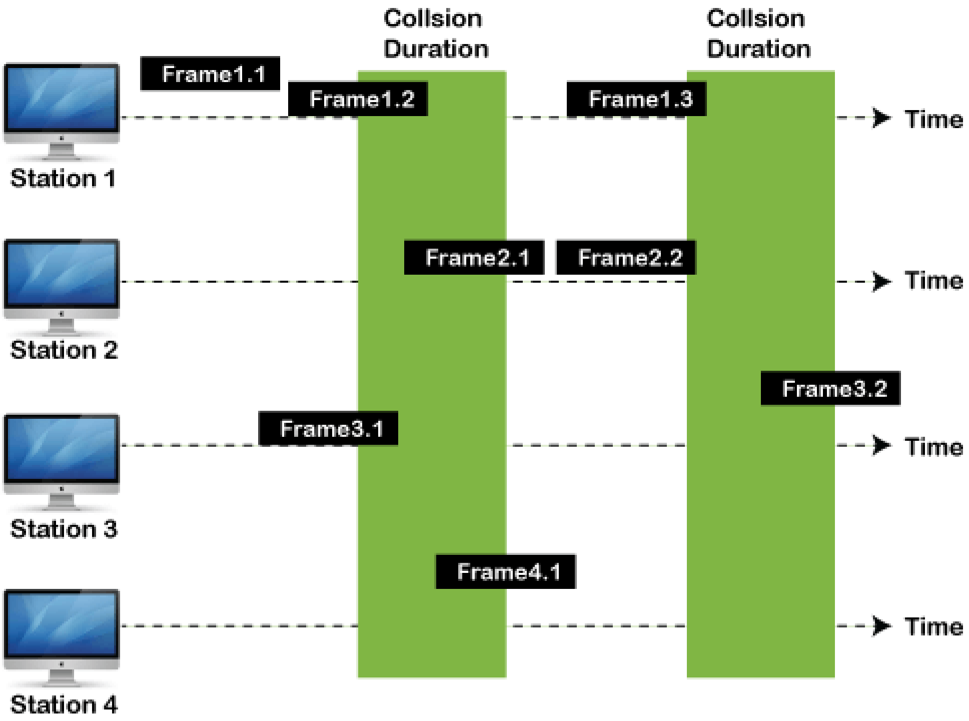


Pure Aloha

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.



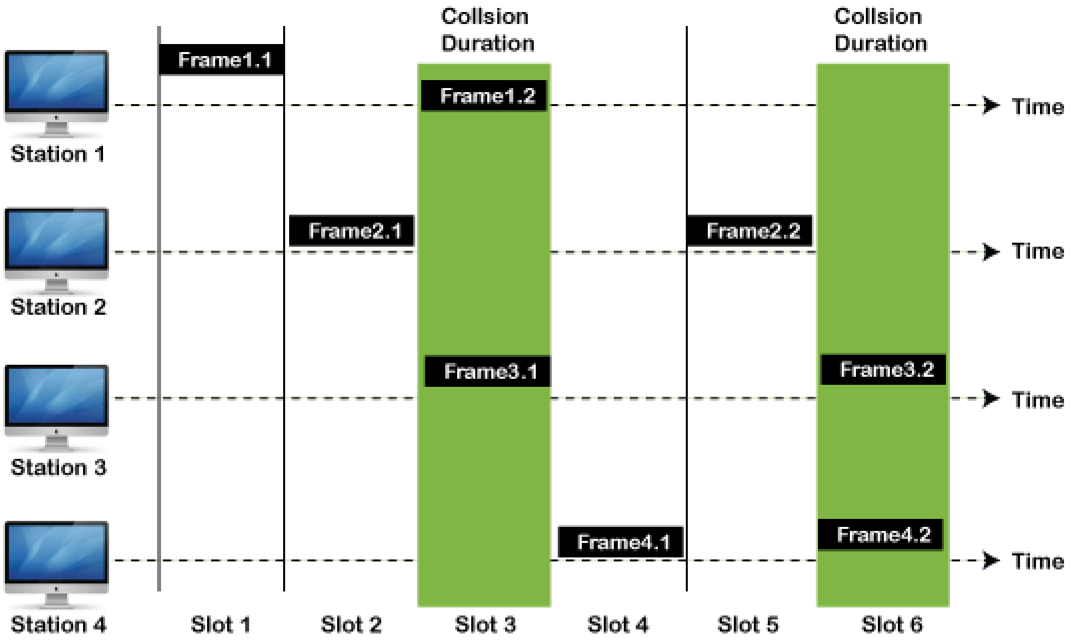
Frames in Pure ALOHA

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.



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.

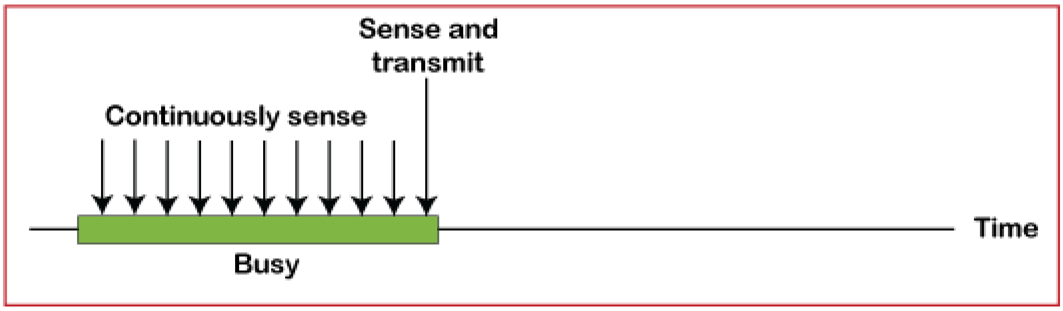
CSMA Access Modes

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.

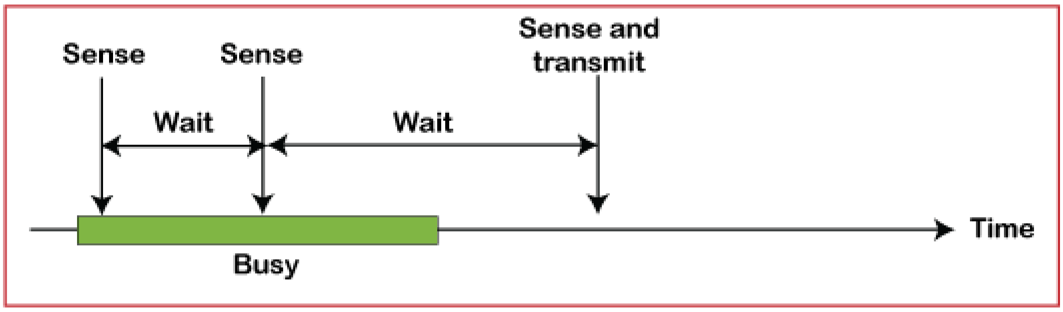
Non-Persistent: It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it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

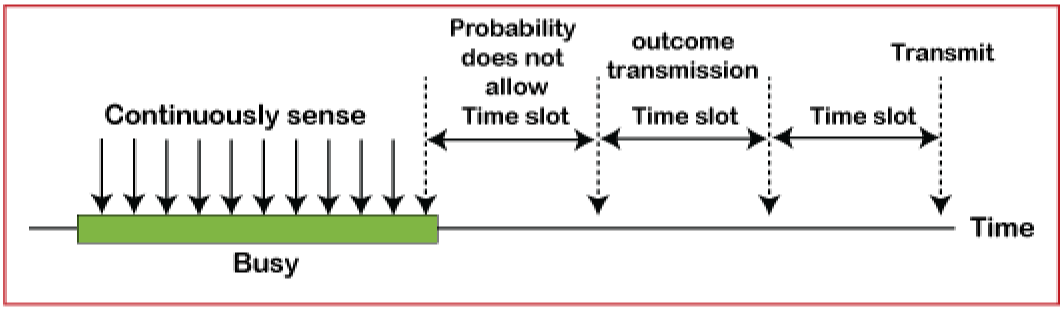
O- Persistent: It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



a. 1-persistent



b. Nonpersistent



c. p-persistent

TOPIC: COLLISSION FREE PROTOCOLS

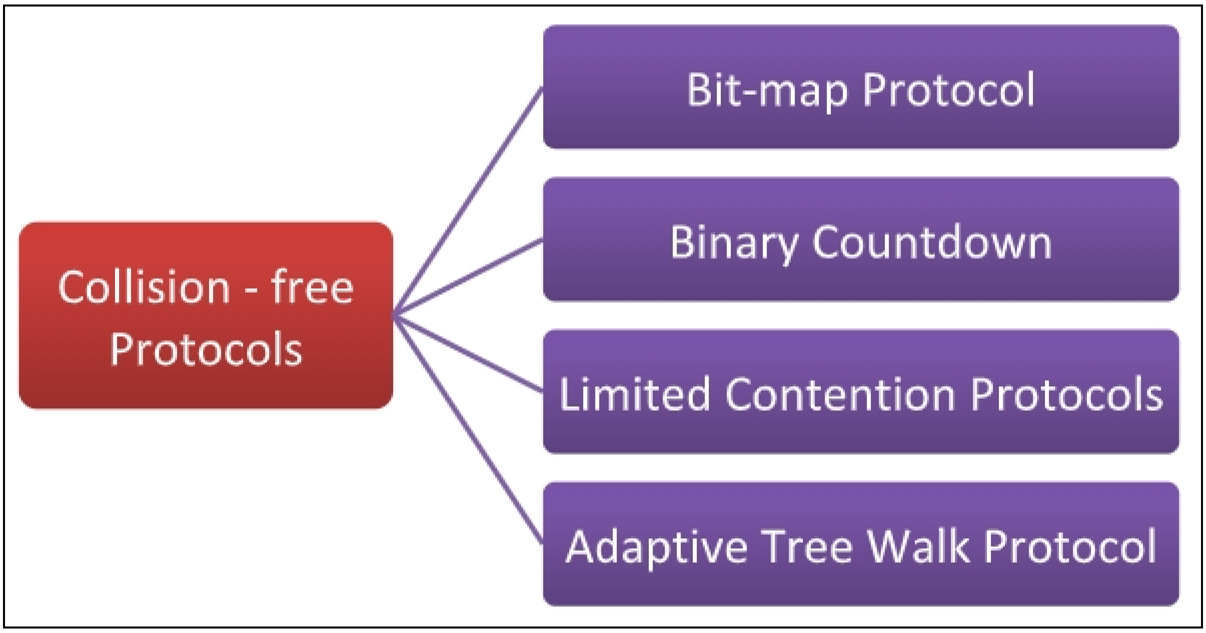
In computer networks, when more than one station tries to transmit simultaneously via a shared channel, the transmitted data is garbled. This event is called collision.

The Medium Access Control (MAC) layer of the OSI model is responsible for handling collision of frames.

Collision – free protocols are devised so that collisions do not occur. Protocols like CSMA/CD and CSMA/CA nullifies the possibility of collisions once the transmission channel is acquired by any station. However, collision can still occur during the contention period if more than one stations starts to transmit at the same time.

Collision – free protocols resolves collision in the contention period and so the possibilities of collisions are eliminated.

Types of Collision – free Protocols


Collision - free Protocols
Bit-map Protocol
Binary Countdown
Limited Contention Protocols
Adaptive Tree Walk Protocol

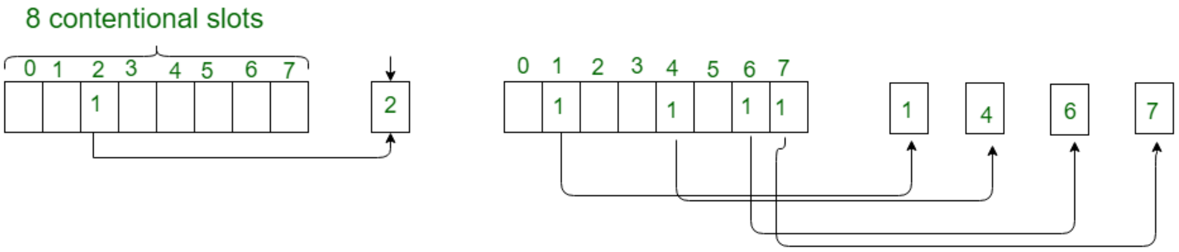
Bit – map Protocol

In bit map protocol, the contention period is divided into N slots, where N is the total number of stations sharing the channel. If a station has a frame to send, it sets the corresponding bit in the slot. So, before transmission, each station knows whether the other stations want to transmit. Collisions are avoided by mutual agreement among the contending stations on who gets the channel.

In this protocol, the contention period is divided into N slots, where N is the total number of stations sharing the channel. If a station has a frame to send, it sets the corresponding bit in the slot.

Suppose that there are 10 stations. So the number of contention slots will be 10. If the stations 2, 3, 8 and 9 wish to transmit, they will set the corresponding slots to 1 as shown in the following diagram:

Once each station announces itself, one of them gets the channel based upon any agreed criteria. Generally, transmission is done in the order of the slot numbers. Each station has complete knowledge whether every other station wants to transmit or not, before transmission starts. So, all possibilities of collisions are eliminated.



A Bit-map Protocol.

Binary Countdown

This protocol overcomes the overhead of 1 bit per station of the bit – map protocol. Here, binary addresses of equal lengths are assigned to each station. For example, if there are 6 stations, they may be assigned the binary addresses 001, 010, 011, 100, 101 and 110. All stations wanting to communicate broadcast their addresses. The station with higher address gets the higher priority for transmitting.

In a binary countdown protocol, each station is assigned a binary address. The binary addresses are bit strings of equal lengths. When a station wants to transmit, it broadcasts its address to all the stations in the channel, one bit at a time starting with the highest order bit.

In order to decide which station gets the channel access, the addresses of the stations which are broadcasted are ORed. The higher numbered station gets the channel access.

Example

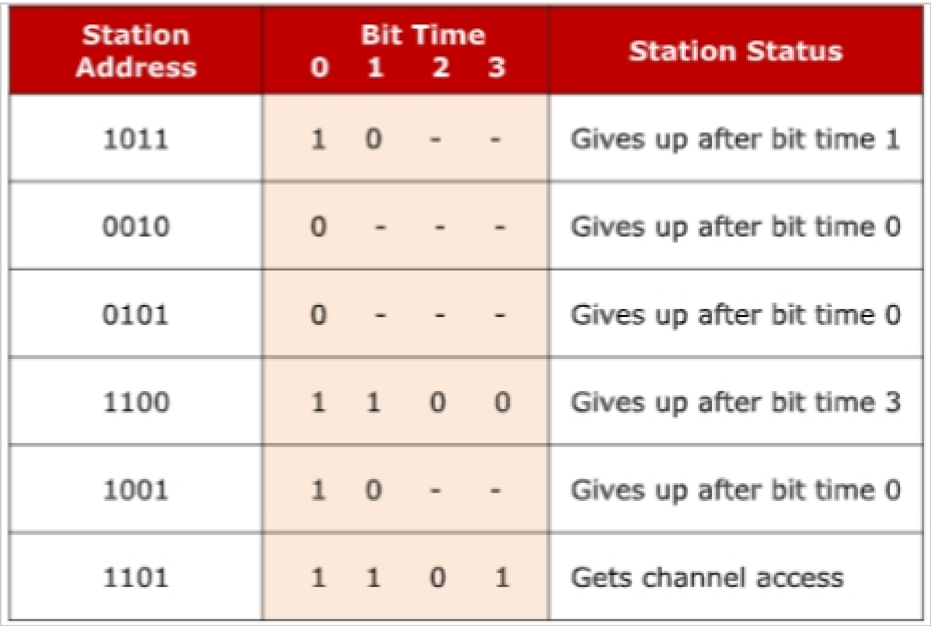
Suppose that six stations contend for channel access which have the addresses: 1011, 0010, 0101, 1100, 1001 and 1101.

The iterative steps are −

- All stations broadcast their most significant bit, i.e. 1, 0, 0, 1, 1, 1. Stations 0010 and 0101 sees 1 bit in other stations, and so they give up competing for the channel.

- The stations 1011, 1100, 1001 and 1101 continue. They broadcast their next bit, i.e. 0, 1, 0, 1. Stations 1011 and 1001 sees 1 bit in other stations, and so they give up competing for the channel.
- The stations 1100 and 1101 continue. They broadcast their next bit, i.e. 0, 0. Since both of them have same bit value, both of them broadcast their next bit.
- The stations 1100 and 1101 broadcast their least significant bit, i.e. 0 and 1. Since station 1101 has 1 while the other 0, station 1101 gets the access to the channel.
- After station 1101 has completed frame transmission, or there is a time-out, the next contention cycle starts.

The procedure is illustrated as follows –



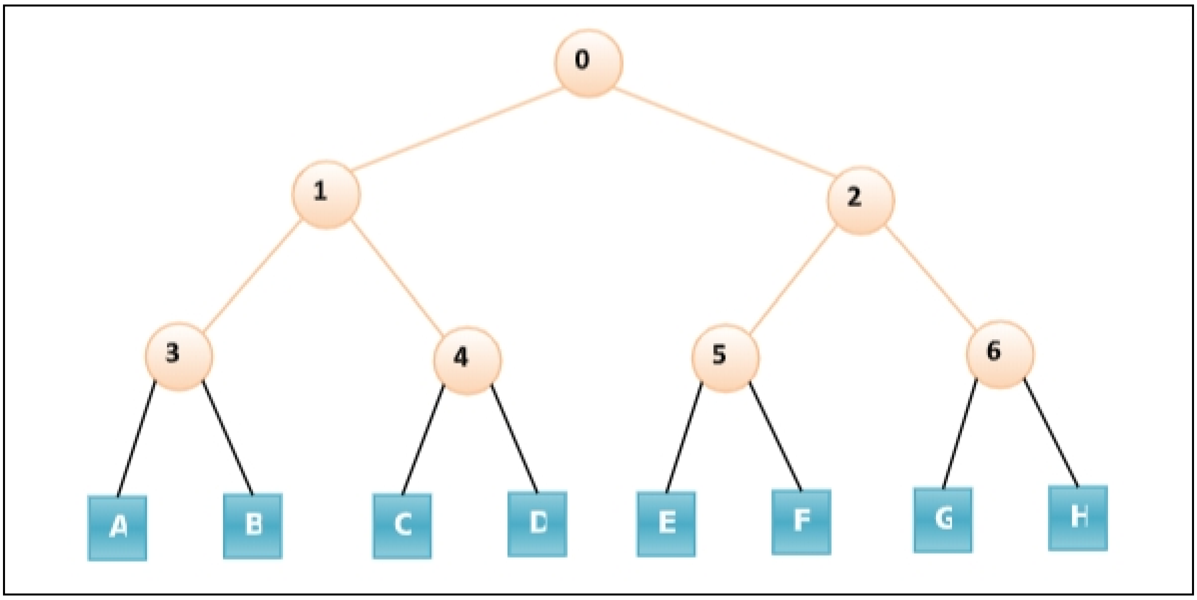
Station Address	Bit Time				Station Status
	0	1	2	3	
1011	1	0	-	-	Gives up after bit time 1
0010	0	-	-	-	Gives up after bit time 0
0101	0	-	-	-	Gives up after bit time 0
1100	1	1	0	0	Gives up after bit time 3
1001	1	0	-	-	Gives up after bit time 0
1101	1	1	0	1	Gets channel access

Limited Contention Protocols

These protocols combines the advantages of collision based protocols and collision free protocols. Under light load, they behave like ALOHA scheme. Under heavy load, they behave like bitmap protocols.

Adaptive Tree Walk Protocol

In adaptive tree walk protocol, the stations or nodes are arranged in the form of a binary tree as follows -



Initially all nodes (A, B ……. G, H) are permitted to compete for the channel. If a node is successful in acquiring the channel, it transmits its frame. In case of collision, the nodes are divided into two groups (A, B, C, D in one group and E, F, G, H in another group). Nodes belonging to only one of them is permitted for competing. This process continues until successful transmission occurs.

TOPIC: LIMITED CONTENTION PROTOCOL

Limited Contention Protocols are the media access control (MAC) protocols that combines the advantages of collision based protocols and collision free protocols. They behave like slotted ALOHA under light loads and bitmap protocols under heavy loads.

Concept

In computer networks, when more than one station tries to transmit simultaneously via a shared channel, the transmitted data is garbled, an event called collision.

In collision based protocols like ALOHA, all stations are permitted to transmit a frame without trying to detect whether the transmission channel is idle or busy.

In slotted ALOHA, the shared channel is divided into a number of discrete time intervals called slots. Any station having a frame can start transmitting at the beginning of a slot. Since, this works very good under light loads, limited contention protocols behave like slotted ALOHA under low loads.

However, with the increase in loads, there occurs exponential growth in number of collisions and so the performance of slotted ALOHA degrades rapidly. So, under high loads, collision free protocols like bitmap protocols work best.

In collision free protocols, channel access is resolved in the contention period and so the possibilities of collisions are eliminated. In bit map protocol, the contention period is divided into N slots, where N is the total number of stations sharing the channel. If a station has a frame to send, it sets the corresponding bit in the slot. So, before transmission, each station knows whether the other stations want to transmit. Collisions are avoided by mutual agreement among the contending stations on who gets the channel. Limited contention protocols behave like slotted ALOHA under low loads.

Working Principle

Limited contention protocols divide the contending stations into groups, which may or not be disjoint.

At slot 0, only stations in group 0 can compete for channel access. At slot 1, only stations in group 1 can compete for channel access and so on.

In this process, if a station successfully acquires the channel, then it transmits its data frame. If there is a collision or there are no stations competing for a given slot in a group, the stations of the next group can compete for the slot.

By dynamically changing the number of groups and the number of stations allotted in a group according to the network load, the protocol changes from slotted ALOHA under low loads to bit map protocol under high loads.

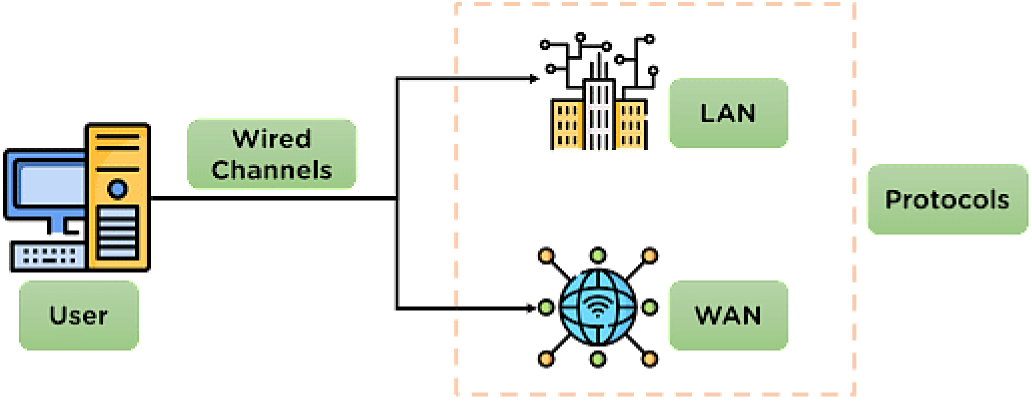
Under low loads, only one group is there containing all stations, which is the case of slotted ALOHA. As the load increases, more groups are added and the size of each group is reduced. When the load is very high, each group has just one station, i.e. only one station can compete at a slot, which is the case of bit map protocol.

The performance of limited contention protocol is highly dependent upon the algorithm to dynamically adjust the group configurations to the changes in network environment.

Example − An example of limited contention protocol is Adaptive Tree Walk Protocol

TOPIC: ETHERNET

What Is Ethernet?



Ethernet is designed for the transmission of data over the channel using wired technology and is used for high-speed data transmission. It is also responsible for applying some protocols for smooth and efficient data transmission over the network.

Ethernet uses cables to transmit data in a network model, such as LAN and, in some cases, WAN. It is more reliable and secure, providing better network connectivity.

Why Use Ethernet?

Ethernet technology is used for establishing connections and is preferred for network channels. It is used in industry networks, college campuses, and medical institutions because it provides services to the data being transmitted.

- Ethernet provides high-speed data transmission in the network.
- It establishes a secure connection for transferring data in the network.
- Ethernet is reliable, as the possibility of outside interference is very low as cable data is difficult to hack into.

Types of Ethernet

Depending on the network requirements, the type of ethernet networks applied in the communication also varies. The different types of ethernet connections are mentioned below:

- Fast Ethernet: This Ethernet type is used for transferring data around the network at a speed of 100 Mbps through twisted-pair cables or optical cables. This type of data transmitted can be done without applying protocols.

- Gigabit Ethernet: This type of Ethernet also uses optical and twisted pair cables for data transmission at 1000 Mbps. This is also one of the most preferred Ethernet networks.

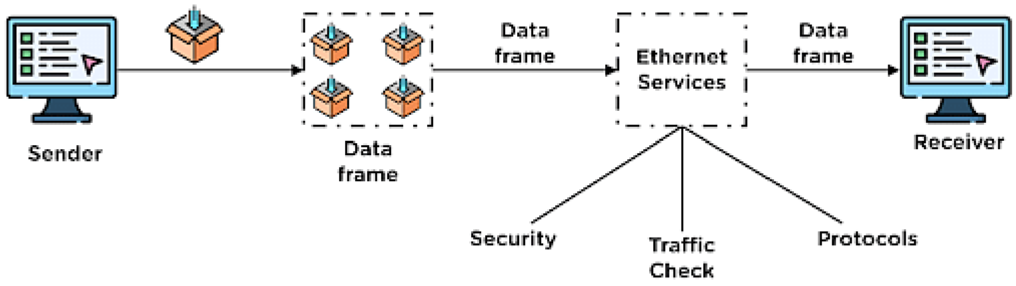
- Switched Ethernet: This Ethernet type installs network devices such as switches or hubs to improve the network transmission. The transmission range for this type ranges from 1000Mbps to 10Gbps.

Working of Ethernet Network

The Ethernet network is designed to work in the 1st layer (physical layer) and 2nd layer (Data Link Layer) of the OSI model.

Ethernet divides the transmission of data into two parts: packets and frames.

- Packet–Refers to a unit of data in the network.
- Frame–Refers to the collection of data packets being transmitted.



The data to be transmitted is converted into data packets in the network and then transferred to the channel. At a point, multiple data packets are collected to form a data frame, which is then transmitted further in the network channel.

During data transmission, Ethernet applies various services over the data being transmitted, such as security checks, traffic control services & other protocols.

Advantages and Disadvantages of Ethernet

Advantages	Disadvantages
1. The cost of installing an Ethernet connection is affordable.	Ethernet networks are more suited for short-distance connections.
2. Provides high-speed data transmission for data in the network.	Troubleshooting faults in the ethernet connection is difficult.
3. It maintains data quality and also provides a secure channel for data transmission.	Increased cases of network traffic in the network channel.

Ethernet vs Internet

Network Model

Ethernet	*Internet*
Ethernet is preferred for small distance network connections, such as schools, hospitals, etc.	Internet connections are available for all distance network channels.

Network Security and Reliability

Ethernet	*Internet*
Ethernet connections are secure and are less prone to external interference and provide data security.	The Internet is an open format network connection, so it is affected more because of external interference.

Network Control

Ethernet	*Internet*
Ethernet is less complex due to being wired in connection and provides much better transmission of data.	The Internet is a connection of multiple networks, so it requires a regular inspection from network administrators.

IEEE 802.11 Architecture

The IEEE 802.11 standard, commonly known as Wi-Fi, outlines the architecture and defines the MAC and physical layer specifications for wireless LANs (WLANs). Wi-Fi uses high-frequency radio waves instead of cables for connecting the devices in LAN. Given the mobility of WLAN nodes, they can move unrestricted within the network coverage zone. The 802.11 structure is designed to accommodate mobile stations that participate actively in network decisions. Furthermore, it can seamlessly integrate with 2G, 3G, and 4G networks.

The Wi-Fi standard represents a set of wireless LAN standards developed by the Working Group of IEEE LAN/MAN standards committee (IEEE 802). The term 802.11x is also used to denote the set of standards. Various specifications and amendments include 802.11a, 802.11b, 802.11e, 802.11g, 802.11n etc.

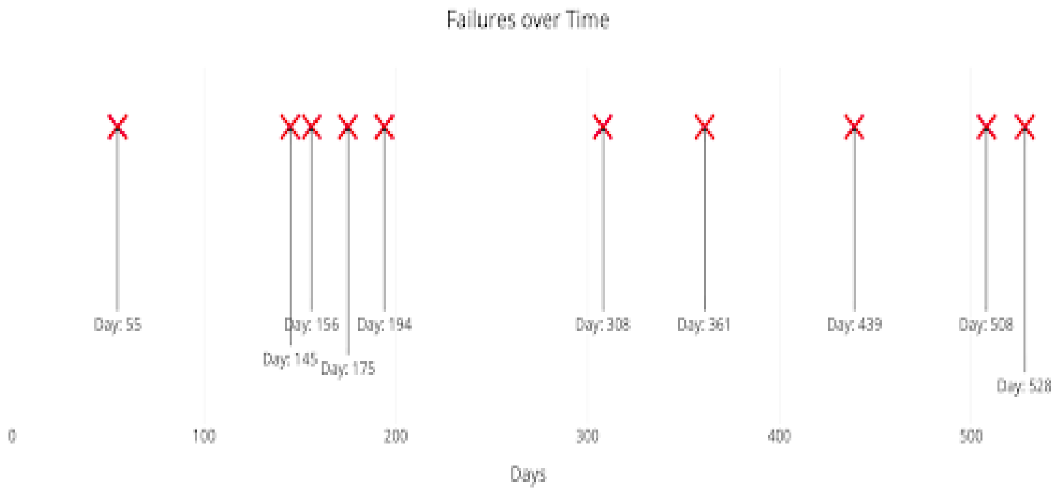
TOPIC:HDLC queuing MODELS

Poisson process

A Poisson process, or Poisson point process, describes a process where certain events occur at a constant rate, but at random and independently of each other.

A Poisson process is a model for a series of discrete events where the average time between events is known, but the exact timing of events is random. The arrival of an event is independent of the event before (waiting time between events is memoryless).

For example, suppose we own a website that our content delivery network (CDN) tells us goes down on average once per 60 days, but one failure doesn't affect the probability of the next. All we know is the average time between failures. The failures are a Poisson process that looks like:



Poisson process with an average time between events of 60 days.

We know the average time between events, but the events are randomly spaced in time. We might have back-to-back failures, but we could also go years between failures because the process is stochastic.

A Poisson process meets the following criteria:

Poisson Process Criteria

- Events are independent of each other. The occurrence of one event does not affect the probability another event will occur.
- The average rate (events per time period) is constant.

Common examples of Poisson processes are customers calling a help center, visitors to a website, radioactive decay in atoms, photons arriving at a space telescope and movements in a stock price.

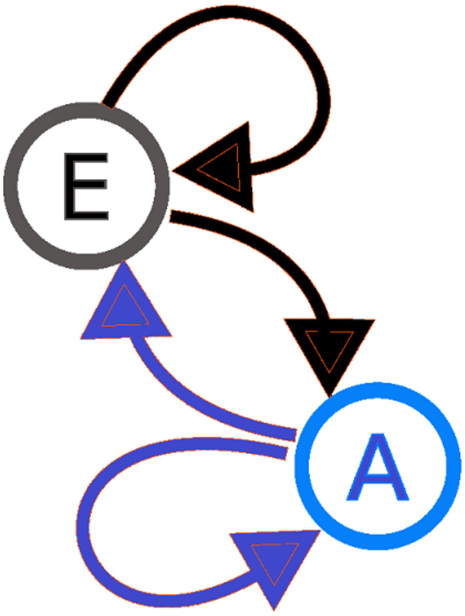
Topic: Marcov chain

Marcov chain: A **Markov chain** or **Markov process** is a stochastic model describing a sequence of possible events in which the probability of each event depends only on the state attained in the previous event. Informally, this may be thought of as, "What happens next depends only on the state of affairs *now*."

Markov chains. These are the simplest type of Markov model and are used to represent systems where all states are observable. Markov chains show all possible states, and between states, they show the transition rate, which is the probability of moving from one state to another per unit of time. Applications of this type of model include prediction of market crashes, speech recognition and search engine algorithms.

Markov chains, named after **Andrey Markov**, a stochastic model that depicts a sequence of possible events where predictions or probabilities for the next state are based solely on its previous event state, not the states before.

In simple words, the probability that n+1th steps will be x depends only on the nth steps not the complete sequence of steps that came before n. This property is known as Markov Property or Memorylessness. Let us explore our Markov chain with the help of a diagram, are Markov Process



A diagram representing a two-state(here, E and A) Markov process. Here the arrows originated from the current state and point to the future state and the number associated with the arrows indicates the probability of the Markov process changing from one state to another state. For instance, if the Markov process is in state E, then the probability it changes to state A is 0.7, while the probability it remains in the same state is 0.3. Similarly, for any process in state A, the probability to change to Estate is 0.4 and the probability to remain in the same state is 0.6.

Topic:Queuing theory

A queueing model is **constructed so that queue lengths and waiting time can be predicted**. Queueing theory is generally considered a branch of operations research because the results are often used when making business decisions about the resources needed to provide a service.

M/M/1 Queueing Model

Basic Concepts

The **M/M/1 model** is a queueing process in which customers arrive at one server and wait in a queue (if necessary) until the server is available. Customers are serviced in the order in which they arrive (FIFO = first in, first out). The server services at most one customer at a time. There is no limit to the number of customers who can wait in the queue.

In the M/M/1 model, customer arrivals follow an exponential distribution at the rate of λ. Servicing also follows an exponential distribution with a service rate of μ.

The number of customers in the system = the number of customers (if any) waiting in the queue plus one if the server is occupied.

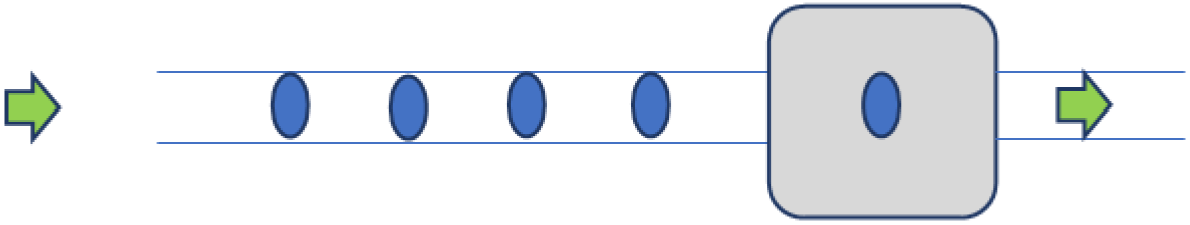


Figure 1 – M/M/1 queueing model

Little's Law is a theorem that determines the average number of items in a stationary queuing system, based on the average waiting time of an item within a system and the average number of items arriving at the system per unit of time.

The law provides a simple and intuitive approach for the assessment of the efficiency of queuing systems.

Formula for Little’s Law

Mathematically, Little’s Law is expressed through the following equation:

$$L = \lambda \text{ x } W$$

Where:

L – the average number of items in a queuing system

λ – the average number of items arriving at the system per unit of time

W – the average waiting time an item spends in a queuing system

Example of Little’s Law

John owns a small coffee shop. He wants to know the average number of customers queuing in his coffee shop, to decide whether he needs to add more space to accommodate more customers. Currently, his queuing area can accommodate no more than eight people.

John measured that, on average, 40 customers arrive at his coffee shop every hour. He also determined that, on average, a customer spends around 6 minutes in his store (or 0.1 hours). Given these inputs, John can find the average number of customers queuing in his coffee shop by applying Little’s Law:

$$L = 40 \text{ x } 0.1 = 4 \text{ customers}$$

Little’s Law shows that, on average, there are only four customers queuing in John’s coffee shop. Therefore, he does not need to create more space in the store to accommodate more queuing customers.

Queueing delay:

Let the packet is received by the destination, the packet will not be processed by the destination immediately. It has to wait in a queue in something called a buffer. So the amount of time it waits in queue before being processed is called queueing delay.

In general, we can’t calculate queueing delay because we don’t have any formula for that.

This delay depends upon the following factors:

- If the size of the queue is large, the queuing delay will be huge. If the queue is empty there will be less or no delay.
- If more packets are arriving in a short or no time interval, queuing delay will be large.

- The less the number of servers/links, the greater is the queuing delay.

M/M/s/K Queueing Model

Basic Concepts

The **M/M/s/K queueing model** is like the M/M/1/K model, except that there are *s* servers instead of 1.

It is sufficient to look at the case where $s \leq K$ (where *K* is the maximum size of the queue) since if $K < s$ then at most *K* of the *s* servers will ever be used. Also note that when $K = s$, there is no queueing since customers who arrive either get serviced immediately or go away permanently.

M/G/1 QUEUE

An **M/G/1 queue** is a queue model where arrivals are **M**arkovian (modulated by a Poisson process), service times have a **G**eneral distribution and there is a single server.