Circuit Switching

In circuit switching network resources (bandwidth) is divided into pieces and bit delay is constant during a connection. The dedicated path/circuit established between sender and receiver provides a guaranteed data rate. Data can be transmitted without any delays once the circuit is established.
Telephone system network is the one of example of Circuit switching
eg :
Each of the six rectangles represents a carrier switching office (end office, toll office, etc.). In this example, each office has three incoming lines and three outgoing lines. When a call passes through a switching office, a physical connection is (conceptually) established between the line on which the call came in and one of the output lines, as shown by the dotted lines.

Phases of Circuit Switch Connection

- **Circuit Establishment** : In this phase, a dedicated circuit is established from the source to the destination through a number of intermediate switching centres. The sender and receiver transmits communication signals to request and acknowledge establishment of circuits.
- **Data Transfer** : Once the circuit has been established, data and voice are transferred from the source to the destination. The dedicated connection remains as long as the end parties communicate.
- **Circuit Disconnection** : When data transfer is complete, the connection is relinquished. The disconnection is initiated by any one of the user. Disconnection involves removal of all intermediate links from the sender to the receiver.

Advantages of Circuit Switching:
It has the following advantages :

1. The main advantage of circuit switching is that a committed transmission channel is established between the computers which gives a guaranteed data ratee.
2. In circuit switching there is no delay in data flow because of the dedicated transmission path.

Disadvantages of Circuit Switching:
It has the following disadvantages :

1. It takes long time to establish connection.
2. More bandwidth is required in setting up of dedicated channels.
3. It cannot be used to transmit any other data even if the channel is free as the connection is dedicated in circuit switching.

Formulas in Circuit Switching :

Transmission rate = Link Rate or Bit rate / no. of slots = R/h bps
Transmission time = size of file / transmission rate = x / (R/h) = (x*h)/R second
Total time to send packet to destination = Transmission time + circuit setup time

Example 1 : How long it takes to send a file of ‘x bits’ from host A to host B over a circuit switched network that uses TDM with ‘h slots’ and have a bit rate of ‘R Mbps’, circuit establish time is k seconds.Find total time?

Explanation :
Transmission rate = Link Rate or Bit rate / no. of slots = R/h bps
Transmission time = size of file/ transmission rate = x / (R/h) = (x*h)/R

Total time = transmission time + circuit setup time = (x*h)/R secs + k secs

Example 2 : If a link transmits F frames/sec and each slot has B bits then find the transmission rate?

Explanation :
Since it is not mention how many slots in each frame we take one frame has one slot.
Transmission rate is amount of data send in 1 second.
Transmission rate = F * B bits/sec

Packet Switching

- **Packet switching** is a method of transferring the data to a network in form of packets. In order to transfer the file fast and efficient manner over the network and minimize the transmission latency, the data is broken into small pieces of variable length, called **Packet**.
- At the destination, all these small-parts (packets) has to be reassembled, belonging to the same file. A packet composes of payload and various control information. No pre-setup or reservation of resources is needed.
- Packet Switching uses **Store and Forward** technique while switching the packets; while forwarding the packet each hop first store that packet then forward. This technique is very beneficial because packets may get discarded at any hop due to some reason
- Packet-Switched networks were designed to overcome the *weaknesses* of Circuit-Switched networks since circuit-switched networks were not very effective for small messages.

Advantage of Packet Switching over Circuit Switching :

- More efficient in terms of bandwidth, since the concept of reserving circuit is not there.
- Minimal transmission latency.
- More reliable as destination can detect the missing packet.
- More fault tolerant because packets may follow different path in case any link is down,

Unlike Circuit Switching.

- Cost effective and comparatively cheaper to implement.

Disadvantage of Packet Switching over Circuit Switching :

- Packet Switching don’t give packets in order, whereas Circuit Switching provides ordered delivery of packets because all the packets follow the same path.
- Since the packets are unordered, we need to provide sequence numbers to each packet.
- Complexity is more at each node because of the facility to follow multiple path.
- Transmission delay is more because of rerouting.
- Packet Switching is beneficial only for small messages, but for bursty data (large messages) Circuit Switching is better.

Modes of Packet Switching :

1. **Connection-oriented Packet Switching (Virtual Circuit)**
2. **Connectionless Packet Switching (Datagram)**

Delays in Packet switching :

1. Transmission Delay
2. Propagation Delay
3. Queuing Delay
4. Processing Delay

Transmission Delay :
Time taken to put a packet onto link. In other words, it is simply time required to put data bits on the wire/communication medium. It depends on length of packet and bandwidth of network.

Transmission Delay = Data size / bandwidth = (L/B) second

Propagation delay :
Time taken by the first bit to travel from sender to receiver end of the link. In other words, it is simply the time required for bits to reach the destination from the start point. Factors on which Propagation delay depends are Distance and propagation speed.

Propagation delay = distance/transmission speed = d/s

Queuing Delay :
Queuing delay is the time a job waits in a queue until it can be executed. It depends on congestion. It is the time difference between when the packet arrived Destination and when the packet data was processed or executed. It may be caused by mainly three reasons i.e. originating switches, intermediate switches or call receiver servicing switches.

Average Queuing delay = (N-1)L/(2*R)

where N = no. of packets
L=size of packet
R=bandwidth

Processing Delay :
Processing delay is the time it takes routers to process the packet header. Processing of packets helps in detecting bit-level errors that occur during transmission of a packet to the destination. Processing delays in high-speed routers are typically on the order of microseconds or less.
In simple words, it is just the time taken to process packets.

Total time *or* **End-to-End time**

= Transmission delay + Propagation delay+ Queuing delay
+ Processing delay

For M hops and N packets –

Total delay
= M*(Transmission delay + propagation delay)+
(M-1)*(Processing delay + Queuing delay) +
(N-1)*(Transmission delay)

For N connecting link in the circuit –
Transmission delay = N*L/R
Propagation delay = N*(d/s)

Difference b/w Circuit vs Packet-Switching

Circuit Switching	**Packet Switching**
In circuit switching there are 3 phases: i) Connection Establishment. ii) Data Transfer. iii) Connection Released.	In Packet switching directly data transfer takes place .
In circuit switching, each data unit know the entire path address which is provided by the source.	In Packet switching, each data unit just know the final destination address intermediate path is decided by the routers.

In Circuit switching, data is processed at source system only	In Packet switching, data is processed at all intermediate node including source system.
Delay between data units in circuit switching is uniform.	Delay between data units in packet switching is not uniform.
Resource reservation is the feature of circuit switching because path is fixed for data transmission.	There is no resource reservation because bandwidth is shared among users.
Circuit switching is more reliable.	Packet switching is less reliable.
Wastage of resources are more in Circuit Switching	Less wastage of resources as compared to Circuit Switching
It is not a store and forward technique.	It is a store and forward technique.
Transmission of the data is done by the source.	Transmission of the data is done not only by the source, but also by the intermediate routers.
Congestion can occur during connection establishment time, there might be a case will requesting for channel the channel is already occupied.	Congestion can occur during data transfer phase, large number of packets comes in no time.
Circuit switching is not convenient for handling bilateral traffic.	Packet switching is suitable for handling bilateral traffic.
In Circuit switching, charge depend on time and distance, not on traffic in the network.	In Packet switching, charge is based on the number of bytes and connection time.
Recording of packet is never possible in circuit switching.	While recording of packet is possible in packet switching.

Data Link Layer Design Issues

Data-link layer is the second layer after physical layer. The data link layer is responsible for maintaining the data link between two hosts or nodes.

This layer converts the raw transmission facility provided by the physical layer to a reliable and error-free link.

The main functions and the design issues of this layer are

- Providing services to the network layer
- Framing
- Error Control
- Flow Control

1. Services to the Network Layer

The data link layer uses the services offered by the physical layer.The primary function of this layer is to provide a well defined service interface to network layer above it.

The types of services provided can be of three types −

- Unacknowledged connectionless service
- Acknowledged connectionless service
- Acknowledged connection - oriented service

2. Framing

The data link layer encapsulates each data packet from the network layer into frames that are then transmitted.

A frame has three parts, namely −

- Frame Header
- Payload field that contains the data packet from network layer
- Trailer
- Flag − It marks the beginning and end of the frame.

Breaking up the bit stream into frames is more difficult than it at first appears. A good design must make it easy for a receiver to find the start of new frames while using little of the channel bandwidth. We will look at four methods:

1. **Byte count.**

   The first framing method uses a field in the header to specify the number of bytes in the frame. When the data link layer at the destination sees the byte count, it knows how many bytes follow and hence where the end of the frame is

   Disadvantage

   a side effect is that the length of a frame now depends on the contents of the data it carries.

   the destination will get out of synchronization. It will then be unable to locate the correct start of the next frame. Even if the checksum is incorrect so the destination knows that the frame is bad, it still has no way of telling where the next frame starts.

2. **Flag bytes with byte stuffing.**

   A byte is stuffed in the message to differentiate from the delimiter. This is also called character-oriented framing.

   The data link layer on the receiving end removes the escape bytes before giving the data to the network layer. This technique is called byte stuffing.

   The second framing method gets around the problem of resynchronization after an error by having each frame start and end with special bytes. Often the same byte, called a flag byte, is used as both the starting and ending delimiter.

Used when frames consist of character. If data contains ED then, byte is stuffed into data to diffentiate it from ED(end delimeter).

The byte-stuffing scheme depicted in Fig. 3-4 is a slight simplification of the one used in PPP (Point-to-Point Protocol), which is used to carry packets over communications links.

Disadvantage

It is very costly and obsolete method.

A side effect is that the length of a frame now depends on the contents of the data it carries.

FLAG	Header	Payload field	Trailer	FLAG

Two consecutive flag bytes indicate the end of one frame and the start of the next frame.

If the receiver ever loses synchronization it can just search for two flag bytes to find the end of the current frame and the start of the next frame.

3. **Flag bits with bit stuffing.**

A pattern of bits of arbitrary length is stuffed in the message to differentiate from the delimiter. This is also called bit – oriented framing.

It was developed for the once very popular HDLC (Highlevel Data Link Control) protocol. Each frame begins and ends with a special bit pattern, 01111110 or 0x7E in hexadecimal.

This pattern is a flag byte.

Whenever the sender’s data link layer encounters five consecutive 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream.

This bit stuffing is analogous to byte stuffing, in which an escape byte is stuffed into the outgoing character stream before a flag byte in the data.

It also ensures a minimum density of transitions that help the physical layer maintain synchronization. USB (Universal Serial Bus) uses bit stuffing for this reason.

When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically destuffs (i.e., deletes) the 0 bit.

4. **Physical layer coding violations.**

3. Error Control

Error control is done to prevent duplication of frames. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

For unacknowledged connectionless service it might be fine if the sender just kept outputting frames without regard to whether they were arriving properly. But for reliable, connection-oriented service it would not be fine at all.

when frames may be transmitted multiple times there is a danger that the receiver will accept the same frame two or more times and pass it to the network layer more than once. To prevent this from happening, it is generally necessary to assign sequence numbers to outgoing frames, so that the receiver can distinguish retransmissions from originals.

The data link layer ensures error free link for data transmission. The issues it caters to with respect to error control are −

- Dealing with transmission errors
- Sending acknowledgement frames in reliable connections
- Retransmitting lost frames
- Identifying duplicate frames and deleting them
- Controlling access to shared channels in case of broadcasting

4. Flow Control

Flow control is done to prevent the flow of data frame at the receiver end. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

Two approaches are commonly used. In the first one, feedback-based flow control, the receiver sends back information to the sender giving it permission to send more data, or at least telling the sender how the receiver is doing. In the second one, rate-based flow control, the protocol has a built-in mechanism that limits the rate at which senders may transmit data, without using feedback from the receiver.

There will be frame losses even if the transmission is error-free. The two common approaches for flow control are −

- Feedback based flow control
- Rate based flow control

Error-Correcting Codes OR FEC (Forward Error Correction)

We will examine four different error-correcting codes:

1. Hamming codes.
2. Binary convolutional codes.

3. Reed-Solomon codes.
4. Low-Density Parity Check codes

A frame consists of m data (i.e., message) bits and r redundant (i.e. check) bits.

In a **block code**, the r check bits are computed solely as a function of the m data bits with which they are associated, as though the m bits were looked up in a large table to find their corresponding r check bits.

In a **systematic code**, the m data bits are sent directly, along with the check bits, rather than being encoded themselves before they are sent.

In a **linear code**, the r check bits are computed as a linear function of the m data bits.

An n-bit unit containing data and check bits is referred to as an nbit codeword. The code rate, or simply rate, is the fraction of the codeword that carries information that is not redundant, or m/n.

The number of bit positions in which two codewords differ is called the **Hamming distance** (Hamming, 1950). Its significance is that if two codewords are a **Hamming distance d** apart, it will require d single-bit errors to convert one into the other.

All 2m possible data messages are legal, but due to the way the check bits are computed, not all of the 2n possible codewords are used. In fact, when there are r check bits, only the small fraction of 2m /2n or 1/2r of the possible messages will be legal codewords.

$$\mathbf{(m + r + 1) \leq 2r}$$

In Hamming codes the bits of the codeword are numbered consecutively, starting with bit 1 at the left end, bit 2 to its immediate right, and so on. The bits that are powers of 2 (1, 2, 4, 8, 16, etc.) are check bits. The rest (3, 5, 6, 7, 9, etc.) are filled up with the m data bits.

If the check results are not all zero, however, an error has been detected. The set of check results forms the **error syndrome** that is used to **pinpoint** and correct the error

The second code we will look at is a convolutional code. This code is the only one we will cover that is not a block code. In a convolutional code, an encoder processes a sequence of input bits and generates a sequence of output bits.

.The number of previous bits on which the output depends is called the constraint length of the code. Convolutional codes are specified in terms of their rate and constraint length.

systematic block codes:

1. Parity.
2. Checksums.
3. Cyclic Redundancy Checks (CRCs).

1. Parity

Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

- One extra bit called as **parity bit** is sent along with the original data bits.
- Parity bit helps to check if any error occurred in the data during the transmission.
- **Even Parity**
- 1 is added to the block if it contains odd number of 1's, and
- 0 is added if it contains even number of 1's

This scheme makes the total number of 1's even, that is why it is called even parity checking.

<u>Advantage-</u>

- This technique is guaranteed to detect an odd number of bit errors (one, three, five and so on).
- If odd number of bits flip during transmission, then receiver can detect by counting the number of 1's.

<u>Limitation-</u>

- This technique can not detect an even number of bit errors (two, four, six and so on).
- If even number of bits flip during transmission, then receiver can not catch the error.

2. **Checksum**

Checksum is an error detection method**.**

Error detection using checksum method involves the following steps-

At sender side,

- If m bit checksum is used, the data unit to be transmitted is divided into segments of m bits.
- All the m bit segments are added.
- The result of the sum is then complemented using 1's complement arithmetic.
- The value so obtained is called as **checksum**.
- The data along with the checksum value is transmitted to the receiver.

At receiver side,

- If m bit checksum is being used, the received data unit is divided into segments of m bits.
- All the m bit segments are added along with the checksum value.

- The value so obtained is complemented and the result is checked.

OR

In checksum error detection scheme, the data is divided into k segments each of m bits.

- In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.
- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.

3. CRC or a polynomial code

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

FSM (Finite state machine)

- Finite state machine is used to recognize patterns.
- Finite automata machine takes the string of symbol as input and changes its state accordingly. In the input, when a desired symbol is found then the transition occurs.
- While transition, the automata can either move to the next state or stay in the same state.
- FA has two states: accept state or reject state. When the input string is successfully processed and the automata reached its final state then it will accept.

Simplest Protocol

In simplest protocol data travels in single direction with neither flow control nor error control.

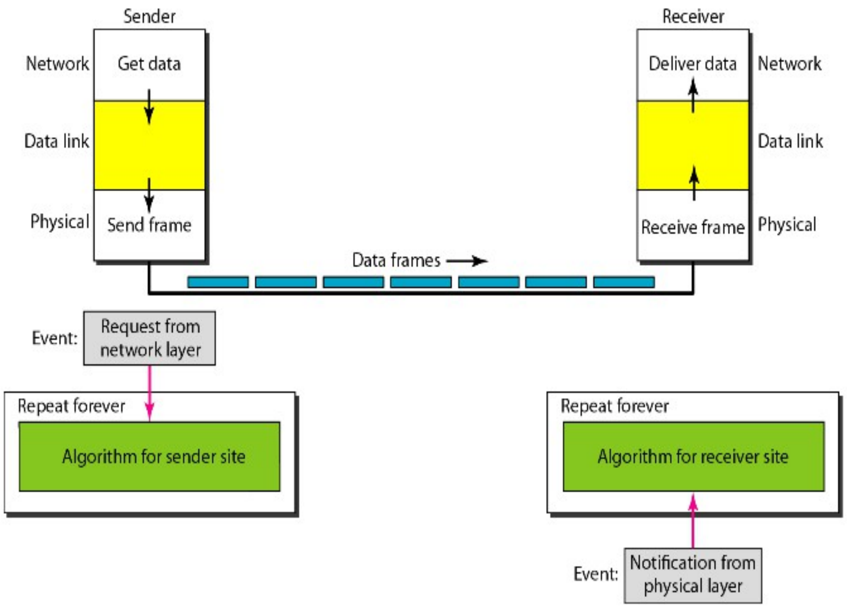
2) We assume that data link layer can accept as many as packet in no time.

3) In data link layer, at receiver side it removes header and passes the data to network layer.

4) At sender side, data link layer gets data from network layer.

5) At receiver side, data link layer passes data to network layer.

Figure 11.6 *The design of the simplest protocol with no flow or error control*



Stop and Wait Protocol

- Sender sends a data packet / single frame to the receiver.
- Sender stops and waits for the acknowledgement for the sent packet from the receiver.
- Receiver receives and processes the data packet.
- Receiver sends an acknowledgement to the sender.
- After receiving the acknowledgement, sender sends the next data packet to the receiver.
- This process of sending a frame & waiting for an acknowledgment continues as long as the sender has data to send.

- Sender puts the data packet on the transmission link.
- Data packet propagates towards the receiver's end.
- Data packet reaches the receiver and waits in its buffer.
- Receiver processes the data packet.
- Receiver puts the acknowledgement on the transmission link.
- Acknowledgement propagates towards the sender's end.
- Acknowledgement reaches the sender and waits in its buffer.
- Sender processes the acknowledgement.

Sender States : The sender is initially in the ready state, but it can move between the ready and blocking state

Ready State

When the sender is in this state, it is only waiting for a packet from the network layer. If a packet comes from the network layer, the sender creates a frame, saves a copy of the frame, starts the only timer and sends the frame. The sender then moves to the blocking state.

Blocking State

When the sender is in this state, three events can occur:

a. If a time-out occurs, the sender resends the saved copy of the frame and restarts the timer.
b. If a corrupted ACK arrives, it is discarded.

c. If an error-free ACK arrives, the sender stops the timer and discards the saved copy of the frame. It then moves to the ready state.

Receiver

The receiver is always in the ready state. Two events may occur:

a. If an error-free frame arrives, the message in the frame is delivered to the network layer and an ACK is sent.

b. If a corrupted frame arrives, the frame is discarded

Total time taken in sending one data packet= $(\text{Transmission delay} + \text{Propagation delay} + \text{Queuing delay} + \text{Processing delay})_{\text{packet}} + (\text{Transmission delay} + \text{Propagation delay} + \text{Queuing delay} + \text{Processing delay})_{\text{ACK}}$

Assume-

- Queuing delay and processing delay to be zero at both sender and receiver side.
- Transmission time for the acknowledgement to be zero since it’s size is very small.

Total time taken in sending one data packet $=(\text{Transmission delay} + \text{Propagation delay})_{\text{packet}} + (\text{Propagation delay})_{\text{ACK}}$

$$\text{Efficiency } (\eta) = \frac{1}{1 + 2 \text{ x } \left(\frac{\text{Propagation delay}}{(\text{Transmission delay})_{\text{packet}}} \right)}$$

$$\text{Efficiency } (\eta) = \frac{1}{1 + 2 \text{ x } \left(\frac{\text{Distance}}{\text{speed}} \right) \text{ x } \left(\frac{\text{Bandwidth}}{\text{Packet length}} \right)}$$

From here, we can observe-

- Efficiency (η) $\propto$ 1 / Distance between sender and receiver
- Efficiency (η) $\propto$ 1 / Bandwidth
- Efficiency (η) $\propto$ Transmission speed
- Efficiency (η) $\propto$ Length of data packet

Throughput-

- Number of bits that can be sent through the channel per second is called as its throughput.

  Throughput=Effeciency * Bandwidth

  Round Trip Time = 2 x Propagation delay

Advantages-

The advantages of stop and wait protocol are-

- It is very simple to implement.
- The incoming packet from receiver is always an acknowledgement.

Limitations-

The limitations of stop and wait protocol are-

- It makes the transmission process extremely slow.

- It does not use the bandwidth entirely as each single packet and acknowledgement uses the entire time to traverse the link.

If the data packet sent by the sender gets lost, then-

- Sender will keep waiting for the acknowledgement for infinite time.
- Receiver will keep waiting for the data packet for infinite time.

If acknowledgement sent by the receiver gets lost, then-

- Sender will keep waiting for the acknowledgement for infinite time.
- Receiver will keep waiting for another data packet for infinite time.

Efficiency may also be referred by the following names-

- **Line Utilization**
- **Link Utilization**
- **Sender Utilization**
- **Utilization of Sender**

Throughput may also be referred by the following names-

- **Bandwidth Utilization**
- **Effective Bandwidth**
- **Maximum data rate possible**
- **Maximum achievable throughput**

Stop and Wait protocol performs better for LANs than WANs.

- Efficiency of the protocol is inversely proportional to the distance between sender and receiver.
- So, the protocol performs better where the distance between sender and receiver is less.
- The distance is less in LANs as compared to WANs.

Piggybacking

A technique called piggybacking is used to improve the efficiency of the bidirectional protocols. When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B; when a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A.

The major **advantage** of piggybacking is better use of available channel bandwidth.

The major **disadvantage** of piggybacking Additional complexity and If the data link layer waits too long before transmitting the acknowledgment, then re-transmission of frame would take place.

CSMA

CSMA / CD stands for Carrier Sense Multiple Access / Collision Detection.

How it works

Step-01: Sensing the Carrier-

- Any station willing to transmit the data senses the carrier.
- **If it finds the carrier free, it starts transmitting its data packet otherwise not.**
- Each station can sense the carrier only at its point of contact with the carrier.
- It is not possible for any station to sense the entire carrier.
- Thus, there is a huge possibility that a station might sense the carrier free even when it is actually not.

Step-02: Detecting the Collision-

In CSMA / CD,

- It is the responsibility of the transmitting station to detect the collision.
- For detecting the collision, CSMA / CD implements the following condition.
- This condition is followed by each station-

  Formula

- **Transmission delay = Length of data packet (L) / Bandwidth (B)**
- **Propagation delay = Distance between the two stations (D) / Propagation speed (V)**

Two cases are possible-

Case-01:

If no collided signal comes back during the transmission,

- It indicates that no collision has occurred.
- The data packet is transmitted successfully.

Case-02:

If the collided signal comes back during the transmission,

- It indicates that the collision has occurred.

- The data packet is not transmitted successfully.
- Step-03 is followed.

Step-03: Releasing Jam Signal-

- Jam signal is a 48 bit signal.
- It is released by the transmitting stations as soon as they detect a collision.
- It alerts the other stations not to transmit their data immediately after the collision.
- Otherwise, there is a possibility of collision again with the same data packet.
- Ethernet sends the jam signal at a frequency other than the frequency of data signals.
- This ensures that jam signal does not collide with the data signals undergone collision.

Step-04: Waiting For Back Off Time-

- After the collision, the transmitting station waits for some random amount of time called as **back off time**.
- After back off time, it tries transmitting the data packet again.
- If again the collision occurs, then station again waits for some random back off time and then tries again.
- The station keeps trying until the back off time reaches its limit.
- After the limit is reached, station aborts the transmission.
- Back off time is calculated using **Back Off Algorithm**.

Back Off Time-

In CSMA / CD protocol,

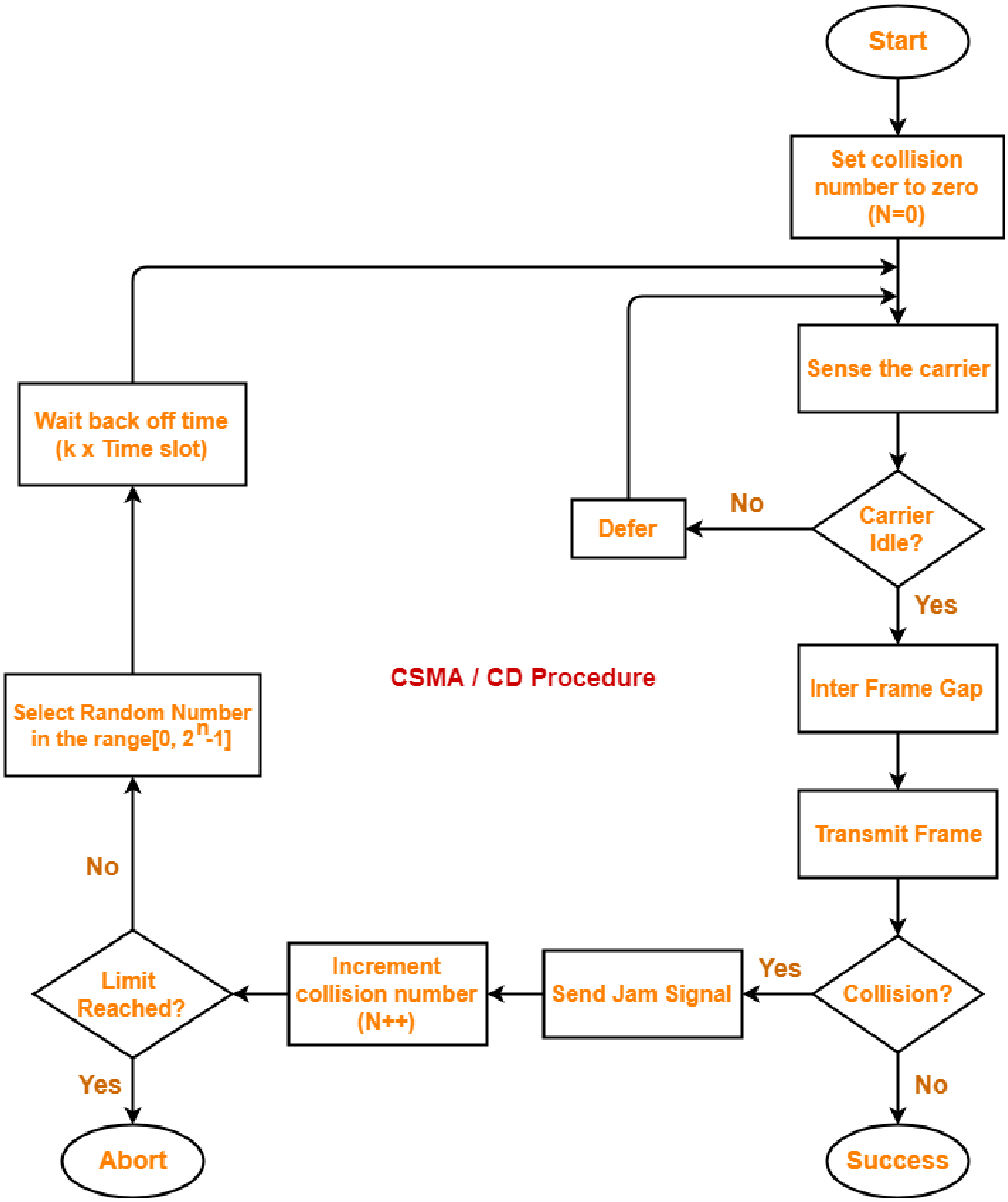
- After the occurrence of collision, station waits for some random back off time and then retransmits.
- This waiting time for which the station waits before retransmitting the data is called as **back off time**.
- Back Off Algorithm is used for calculating the back off time.

Back Off Algorithm-

After undergoing the collision,

- Transmitting station chooses a random number in the range [0, 2^n-1] if the packet is undergoing collision for the n^{th} time.
- If station chooses a number k, then-

Flowchart



OR

The **first carrier sense protocol** that we will study here is called **1-persistent CSMA** (Carrier Sense Multiple Access).

When a station has data to send, it first listens to the channel to see if anyone else is transmitting at that moment. If the channel is idle, the stations sends its data .

if the channel is busy, the station just waits until it becomes idle. Then the station transmits a frame. If a collision occurs, the station waits a random amount of time and starts all over again. The protocol is called 1-persistent because the station transmits with a probability of 1 when it finds the channel idle.

the propagation delay has an important effect on collisions. There is a chance that just after a station begins sending, another station will become ready to send and sense the channel. If the first station's signal has not yet reached the second one, the latter will sense an idle channel and will also begin sending, resulting in a collision. This chance depends on the number of frames that fit on the channel, or the **bandwidth-delay product** of the channel.

A **second carrier** sense protocol is **nonpersistent CSMA**. In this protocol, a conscious attempt is made to be less greedy than in the previous one. As before, a station senses the channel when it wants to send a frame, and if no one else is sending, the station begins doing so itself .this algorithm leads to better channel utilization but longer delays than 1-persistent CSMA

The **last protocol** is **p-persistent CSMA**. It applies to slotted channels and works as follows. When a station becomes ready to send, it senses the channel. If it is idle, it transmits with a probability p. With a probability q = 1 − p, it defers until the next slot. If that slot is also idle, it either transmits or defers again, with probabilities p and q. This process is repeated until either the frame has been transmitted or another station has begun transmitting .

CSMA with Collision Detection

This protocol, known as CSMA/CD ,is the basis of the classic Ethernet LAN .

One-Bit Sliding Window Protocol

- A window of size 1 is maintained by both sender and receiver. For the sender, it isor 1. For the receiver, it is or 1. If , if a new frame is to be transmitted, the sender stamps it with sends it and sets .
- If the sender timed out before receiving ACK, which could be due to excessive delay, lost ACK or lost frame in the forward direction, the same frame is resent;
- The protocol can be implemented on a simplex channel since at any time transmission in only one direction is required.

Go-Back-N

Go-Back-N protocol, also called Go-Back-N Automatic Repeat reQuest, is a data link layer protocol that uses a sliding window method for reliable and sequential delivery of data frames.

Receiver maintains an acknowledgement timer.

Each time the receiver receives a new frame, it starts a new acknowledgement timer.
After the timer expires, receiver sends the cumulative acknowledgement for all the frames that are unacknowledged at that moment.

If for any particular frame, sender does not receive any acknowledgement, then it understands that along with that frame, all the following frames must also have been discarded by the receiver.

So, sender has to retransmit all the following frames too along with that particular frame. Thus, it leads to the retransmission of entire window.
That is why, the protocol has been named as “**Go back N**“.

The maximum number of frames that can be sent depends upon the size of the sending window. If the acknowledgment of a frame is not received within an agreed upon time period, all frames starting from that frame are retransmitted.

Thus in order to accommodate a sending window size of $2^n - 1$, a n-bit sequence number is chosen

Efficiency = Sender Window Size in Protocol / (1 + 2a)

$a = T_p / T_t$

Transmission delay (T_t)= Frame size / Bandwidth

Propagation delay (T_p)

Maximum data rate possible or Throughput= Efficiency x Bandwidth

Receiver window size is always 1 for any value of N.

Selective Repeat

Selective Repeat protocol or SR protocol is an implementation of a sliding window protocol.

In SR protocol,

- Sender window size = Receiver window size
- The size is of course greater than 1 otherwise the protocol will become **Stop and Wait ARQ**.
- If n bits are available for sequence numbers, then-

Sender window size = Receiver window size = $2^n/2 = 2^{n-1}$

- As receiver receives a new frame from the sender, it sends its acknowledgement.
- Receiver acknowledges each frame independently.
- If receiver receives a frame that is corrupted, then it does not silently discard that frame.

- Receiver handles the situation efficiently by sending a negative acknowledgement (NACK).
- Negative acknowledgement allows early retransmission of the corrupted frame.
- It also avoids waiting for the time out timer to expire at the sender side to retransmit the frame.
- Consider receiver receives a frame whose sequence number is not what the receiver expects.
- Then, it does not discard that frame rather accepts it and keeps it in its window.
- Receiver window is implemented as a linked list.
- When receiver receives a new frame, it places the new frame at the end of the linked list.
- When the received frames are out of order, receiver performs the sorting.
- Sorting sorts the frames in the correct order.
- Receiver does not reject the out of order frames.
- Receiver accepts the out of order frames and sort them later.
- Thus, only the missing frame has to be sent by the sender.
- For sending the missing frame, sender performs searching and finds the missing frame.
- Then, sender selectively repeats that frame.
- Thus, only the selected frame is repeated and not the entire window.
- That is why, the protocol has been named as “**Selective Repeat Protocol**“.

Efficiency = Sender Window Size in Protocol / (1 + 2a)

Ethernet

Ethernet is one of the standard LAN technologies used for building wired LANs.

It is defined under IEEE 802.3.

Two kinds of Ethernet exist: **classic Ethernet**, which solves the multiple access problem using the techniques we have studied in this chapter; and **switched Ethernet**, in which devices called switches are used to connect different computers. It is important to note that, while they are both referred to as Ethernet, they are quite different.

Classic Ethernet is the original form and ran at rates from **3 to 10 Mbps**.

Switched Ethernet is what Ethernet has become and runs at **100, 1000, and 10,000 Mbps**, in forms called fast Ethernet, gigabit Ethernet, and 10 gigabit Ethernet.

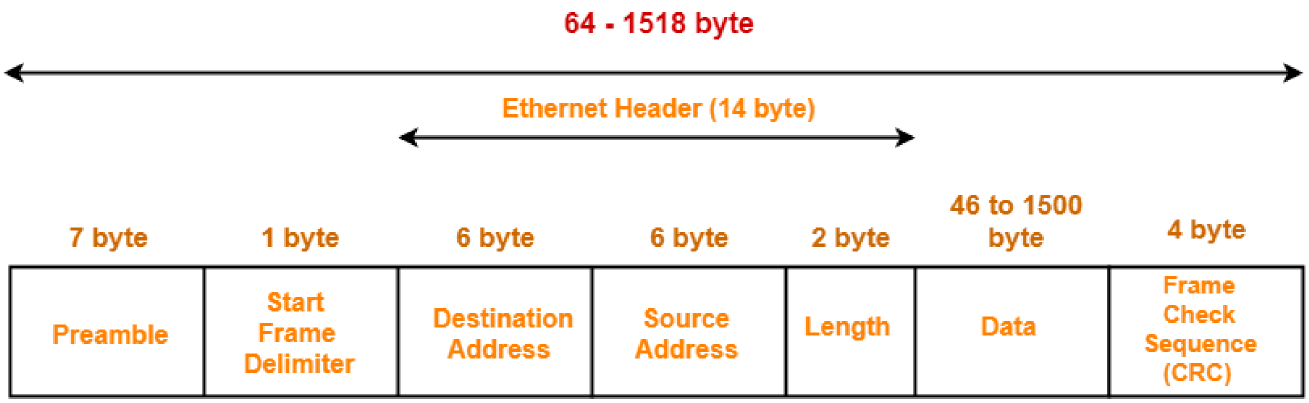
They called the system Ethernet after the luminiferous ether, through which electromagnetic radiation was once thought to propagate.

The Xerox Ethernet was so successful that DEC, Intel, and Xerox drew up a standard in 1978 for a 10-Mbps Ethernet, called the DIX standard. With a minor change, the DIX standard became the IEEE 802.3 standard in 1983

The first variety, popularly called thick Ethernet, resembled a yellow garden hose, with markings every 2.5 meters to show where to attach computers. It was succeeded by thin Ethernet, which bent more easily and made connections using industry-standard BNC connectors. Thin Ethernet was much cheaper and easier to install, but it could run for only 185 meters per segment (instead of 500 m with thick Ethernet), each of which could handle only 30 machines (instead of 100).

Each version of Ethernet has a maximum cable length per segment (i.e., unamplified length) over which the signal will propagate. To allow larger networks, multiple cables can be connected by repeaters.

IEEE 802.3 defines the following Ethernet frame format-



IEEE 802.3 Ethernet Frame Format

0-46 : PAD

1. Preamble-

- It is a 7 byte field that contains a pattern of alternating 0's and 1's.
- It alerts the stations that a frame is going to start.
- It also enables the sender and receiver to establish bit synchronization.

2. Start Frame Delimiter (SFD)-

- It is a 1 byte field which is always set to 10101011.
- The last two bits "11" indicate the end of Start Frame Delimiter and marks the beginning of the frame.

3. Destination Address-

- It is a 6 byte field that contains the MAC address of the destination for which the data is destined.

4. Source Address-

- It is a 6 byte field that contains the MAC address of the source which is sending the data.

5. Length-

- It is a 2 byte field which specifies the length (number of bytes) of the data field.
- This field is required because Ethernet uses variable sized frames.

The following three fields collectively represents the **Ethernet Header**–

- Destination Address (6 bytes)
- Source Address (6 bytes)
- Length (2 bytes)
- Thus, Ethernet Header Size = 14 bytes.

6. Data-

- It is a variable length field which contains the actual data.
- It is also called as a **payload field**.
- The length of this field lies in the range [46 bytes , 1500 bytes].
- Thus, in a Ethernet frame, minimum data has to be 46 bytes and maximum data can be 1500 bytes.

For detecting the collisions, CSMA / CD requires-

Minimum length of data packet = 2 x Propagation delay x Bandwidth

7. Frame Check Sequence (CRC)-

- It is a 4 byte field that contains the CRC code for error detection.

Advantages of Using Ethernet-

- It is simple to understand and implement.
- Its maintenance is easy.
- It is cheap.

Limitations of Using Ethernet-

- It can not be used for real time applications.
- Real time applications require the delivery of data within some time limit.
- Ethernet is not reliable because of high probability of collisions.
- High number of collisions may cause a delay in delivering the data to its destination.
- It can not be used for interactive applications.
- Interactive applications like chatting requires the delivery of even very small amount of data.
- Ethernet requires that minimum length of the data must be 46 bytes.
- It can not be used for client server applications.
- Client server applications require that server must be given higher priority than clients.
- Ethernet has no facility to set priorities.

Distance < = (Length x speed) / (2 x bandwidth)

Routing Algorithms-

- The routing algorithm is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on. If the network uses datagrams internally, this decision must be made anew for every arriving data packet since the best route may have changed since last time.
- Routing algorithms are meant for determining the routing of packets in a node.
- Routing algorithms are classified as-
  1. Static Routing Algorithms
  2. Dynamic Routing Algorithms : Distance Vector Routing is a dynamic routing algorithm.

Connection-Oriented Protocols

TCP is an example of a **connection-oriented protocol**. It requires a logical **connection** to be established between the two processes before data is exchanged. The **connection** must be maintained during the entire time that communication is taking place, then released afterwards.

Eg : **MPLS (MultiProtocol Label Switching)**

Connection-oriented Service	**Connection-less Service**

1.	Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
2.	Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.
3.	Connection-oriented Service is necessary.	Connection-less Service is not compulsory.
4.	Connection-oriented Service is feasible.	Connection-less Service is not feasible.
5.	In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.
6.	Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give the guarantee of reliability.
7.	In connection-oriented Service, Packets follow the same route.	In connection-less Service, Packets do not follow the same route.
8.	Connection-oriented Services requires a bandwidth of high range.	Connection-less Service requires a bandwidth of low range.

Datagram Network

In datagram networks, each data packet or datagram is routed independently from the source to the destination even if they belong to the same message. The network treats the packet as if it exists alone.

Since the datagrams are treated as independent units, no dedicated path is fixed for data transfer. Each datagram is routed by the intermediate routers using dynamically changing routing tables.

Datagram communication is generally guided by User Datagram Protocol or UDP.

Virtual-circuit Network

Virtual Circuit is the computer network providing connection-oriented service. It is a connection-oriented network.

In virtual circuit resource are reserve for the time interval of data transmission between two nodes. This network is a highly reliable medium of transfer. Virtual circuits are costly to implement.

r. No.	Key	Virtual Circuits	Datagram Networks
1	Definition	Virtual Circuit is the connection oriented service in which there is a implementation of resources like buffers, CPU, bandwidth, etc., used by virtual circuit for a data transfer session.	On other hand Datagram is the connection less service where no such resources are required for the data transmission.

r. No.	Key	Virtual Circuits	Datagram Networks
2	Path	In Virtual circuits as all the resources and bandwidth get reserved before the transmission, the path which is utilized or followed by first data packet would get fixed and all other data packets will use the same path and consume same resources.	On other hand in case Datagram network, the path is not fixed as data packets are free to decide the path on any intermediate router on the go by dynamically changing routing tables on routers.
3	Header	As there is same path followed by all the data packets, a common and same header is being used by all the packets.	On other hand different headers with information of other data packet is being used in Datagram network.
4	Complexity	Virtual Circuit is less complex as compared to that of Datagram network.	However on other hand Datagram network are more complex as compared to Virtual circuit.
5	Reliability	Due to fixed path and assurance of fixed resources, Virtual Circuits are more reliable for data transmission as compared to Datagram network.	On other hand Datagram network due to dynamic resource allocation and follow dynamic path is more prone to error and is less reliable than Virtual circuits.
6	Example and Cost	Virtual circuits are costlier in installation and maintenance and are widely used by ATM (Asynchronous Transfer Mode) Network, which is used for the Telephone calls.	On the other hand Datagram network are cheaper as compared to the Virtual Circuits and are mainly used by IP network, which is used for Data services like Internet.

The latter case is sometimes called **session routing** because a route remains in force for an entire session (e.g., while logged in over a VPN).

Routing algorithms can be grouped into two major classes: **nonadaptive and adaptive.**

Adaptive routing algorithm

Adaptive routing algorithm is also called as dynamic routing algorithm. In this algorithm, the routing decisions are made based on network traffic and topology. The parameters which are used in adaptive routing algorithms are distance, hop, estimated transit time and count.

Adaptive routing algorithm is of three types –

- Centralized algorithm
- Isolation algorithm
- Distributed algorithm

Non-Adaptive Routing algorithm :

Non-adaptive routing algorithm is also called as static routing algorithm. In a non-adaptive routing algorithm, the routing decisions are not made based on network traffic and topology. This algorithm is used by static routing. Non-adaptive routing algorithms are simple as compared to Adaptive routing algorithm in terms of complexity.

Non-adaptive routing algorithm is of two types –

- Flooding
- Random walks

S.NO	Adaptive Routing algorithm	Non-Adaptive Routing algorithm
1.	This algorithm creates a routing table based on network conditions.	Whereas this algorithm creates a static table in order to determine when to send packets and which node.
2.	This algorithm is used by dynamic routing.	Whereas this algorithm is used by static routing.
3.	In adaptive routing algorithm, the routing decisions are made based on network traffic and topology.	Whereas in a non-adaptive routing algorithm, the routing decisions are not made based on network traffic and topology.
4.	Adaptive routing algorithms are more complex as compared to non-adaptive routing algorithms in terms of complexity.	While non-adaptive routing algorithms are simple in terms of complexity.
5.	In adaptive routing algorithm, the routing decisions are not static tables.	While in non-adaptive routing algorithm, the routing decisions are static tables.
6.	Adaptive routing algorithm is categorized into distributed, centralized and isolation algorithm.	Whereas non-adaptive routing algorithm is categorized into random walks and flooding.
7.	Adaptive routing algorithm is more used as compared to non-adaptive.	Whereas non-adaptive routing algorithm is comparatively less used.

Shortest Path Algorithms

These paths are the ones that we want a distributed routing algorithm to find, even though not all routers may know all of the details of the network. The idea is to build a graph of the network, with each node of the graph representing a router and each edge of the graph representing a communication line, or link. To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph.

Distance Vector Algorithm –

1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
    - It receives a distance vector from a neighbor containing different information than before.
    - It discovers that a link to a neighbor has gone down.

Advantages of Distance Vector routing –

- It is simpler to configure and maintain than link state routing.

Disadvantages of Distance Vector routing –

- It is slower to converge than link state.
- It is at risk from the count-to-infinity problem.
- It creates more traffic than link state since a hop count change must be propagated to all routers and processed on each router. Hop count updates take place on a periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.
- For larger networks, distance vector routing results in larger routing tables than link state since each router must know about all other routers. This can also lead to congestion on WAN links.

Link State Routing –
Link state routing is the second family of routing protocols. While distance vector routers use a distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using a shortest path computation.

Features of link state routing protocols –

- **Link state packet –** A small packet that contains routing information.
- **Link state database –** A collection information gathered from link state packet.
- **Shortest path first algorithm (Dijkstra algorithm) –** A calculation performed on the database results into shortest path
- **Routing table –** A list of known paths and interfaces.

What is IPv4?

IP stands for **Internet Protocol** and **v4** stands for **Version Four** (IPv4). IPv4 was the primary version brought into action for production within the ARPANET in 1983.

IPv4 is a connectionless protocol used for packet-switched networks. It operates on a best effort delivery model, in which neither delivery is guaranteed, nor proper sequencing or avoidance of duplicate delivery is assured.

IP version four addresses are 32-bit integers which will be expressed in hexadecimal notation. Example- 192.0.2.126 could be an IPv4 address.

An IPv4 datagram consists of a header part and a body or payload part. The header has a 20-byte fixed part and a variable-length optional part. The bits are transmitted from left to right and top to bottom, with the high-order bit of the Version field going first.

Parts of IPv4

- **Network part:**
  The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that's assigned.
- **Host Part:**
  The host part uniquely identifies the machine on your network. This a part of the IPv4 address is assigned to every host.

  For each host on the network, the network part is the same, however, the host half must vary.
- **Subnet number:**
  This is the nonobligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

Characteristics of IPv4

- IPv4 could be a 32-Bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields are twelve and the length of the header filed is twenty.
- It has Unicast, broadcast, and multicast style of addresses.
- IPv4 supports VLSM (Virtual Length Subnet Mask).
- IPv4 uses the Post Address Resolution Protocol to map to mack address.
- RIP may be a routing protocol supported by the routed daemon.
- Networks ought to be designed either manually or with DHCP.
- Packet fragmentation permits from routers and causing host.

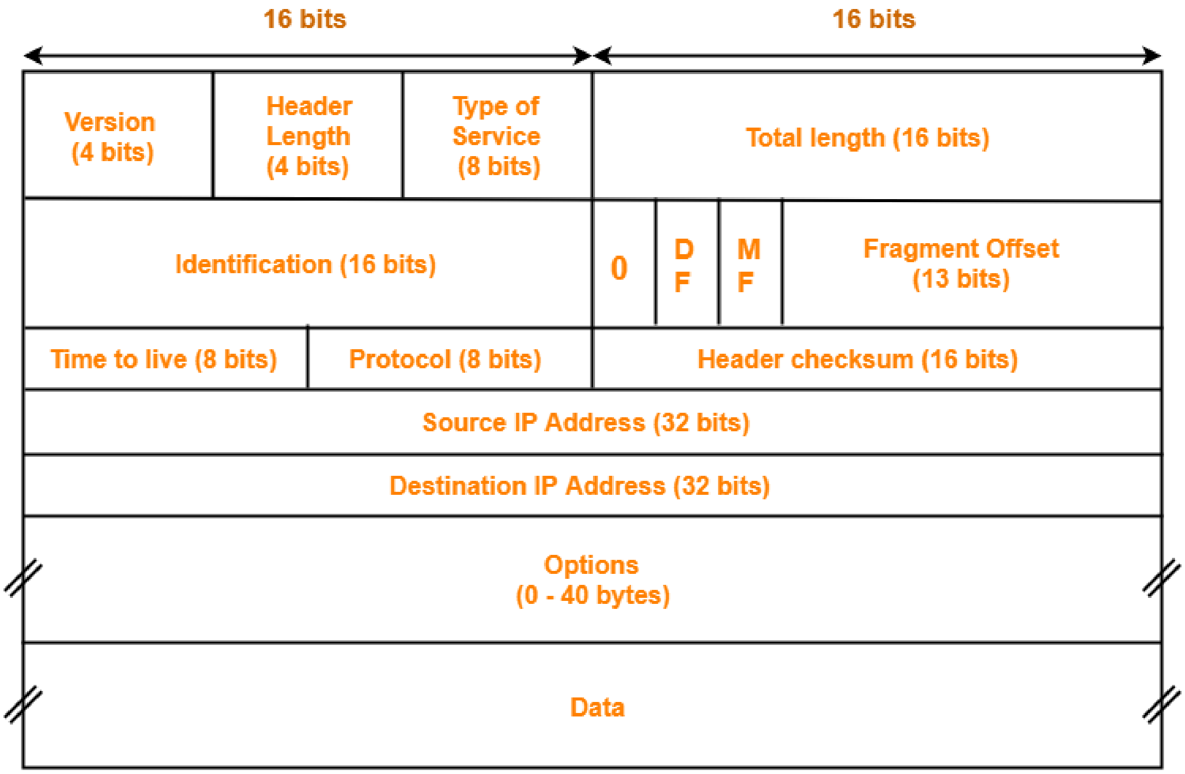
Advantages of IPv4

- IPv4 security permits encryption to keep up privacy and security.
- IPV4 network allocation is significant and presently has quite 85000 practical routers.
- It becomes easy to attach multiple devices across an outsized network while not NAT.
- This is a model of communication so provides quality service also as economical knowledge transfer.
- IPV4 addresses are redefined and permit flawless encoding.
- Routing is a lot of scalable and economical as a result of addressing is collective more effectively.

- Data communication across the network becomes a lot of specific in multicast organizations.

Disadvantages of IPv4

- Limits net growth for existing users and hinders the use of the net for brand new users.
- Internet Routing is inefficient in IPv4.
- IPv4 has high System Management prices and it's labor intensive, complex, slow & frequent to errors.
- Security features are nonobligatory.
- Difficult to feature support for future desires as a result of adding it on is extremely high overhead since it hinders the flexibility to attach everything over IP.



IPv4 Header

VERSION: Version of the IP protocol (4 bits), which is 4 for IPv4

HLEN/IHL: IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.

Type of service/Differentiated Service: Low Delay, High Throughput, Reliability (8 bits)

Total Length: Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.

The Total length includes everything in the datagram—both header and data. The maximum length is 65,535 bytes. At present, this upper limit is tolerable, but with future networks, larger datagrams may be needed.

Identification: Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)

Flags: 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)

Fragment Offset: Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.

Time to live: Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.

Protocol: Name of the protocol to which the data is to be passed (8 bits)

Header Checksum: 16 bits header checksum for checking errors in the datagram header

Source IP address: 32 bits IP address of the sender

Destination IP address: 32 bits IP address of the receiver

Option: Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.

Due to the presence of options, the size of the datagram header can be of variable length (20 bytes to 60 bytes).

Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

IP Addressing

- IP Address is short for Internet Protocol Address.
- It is a unique address assigned to each computing device in an IP network.
- ISP assigns IP Address to all the devices present on its network.
- Computing devices use IP Address to identify and communicate with other devices in the IP network

Types Of IP Address-

IP Addresses may be of the following two types-

1. Static IP Address
2. Dynamic IP Address

1. Static IP Address-

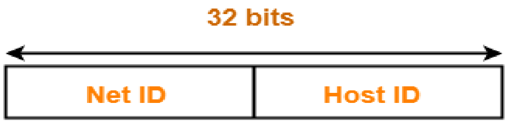
- Static IP Address is an IP Address that once assigned to a network element always remains the same.
- They are configured manually.

2. Dynamic IP Address-

- Dynamic IP Address is a temporarily assigned IP Address to a network element.
- It can be assigned to a different device if it is not in use.
- DHCP or PPPoE assigns dynamic IP addresses.

IP Address Format-

- IP Address is a 32 bit binary address written as 4 numbers separated by dots.
- The 4 numbers are called as **octets** where each octet has 8 bits.
- The octets are divided into 2 components- Net ID and Host ID.



Format of an IP Address

1. **Network ID** represents the IP Address of the network and is used to identify the network.
2. **Host ID** represents the IP Address of the host and is used to identify the host within the network.

IP Addressing-

There are two systems in which IP Addresses are classified-

1. Classful Addressing System
2. Classless Addressing System

Classful Addressing-

In Classful Addressing System, IP Addresses are organized into following 5 classes-

1. Class A
2. Class B
3. Class C
4. Class D
5. Class E

Class A (Prefix 0 fixed)

Range : [0,127]

In class A IP Address,

- The first 8 bits are used for the Network ID.
- The remaining 24 bits are used for the Host ID.

Total number of IP Addresses available in class A

= Numbers possible due to remaining available 31 bits(1st bit is fixed 0) = 2^{31}

Total number of networks available in class A

= Numbers possible due to remaining available 7 bits in the Net ID – 2= 2^7– 2= 126

Total number of hosts that can be configured in class A

= Numbers possible due to available 24 bits in the Host ID – 2 = 2^{24} – 2

Default Mask = 255.0.0.0

Range of 1st octet = [0, 127]
But 2 networks are reserved and unused.
So, Range of 1st octet = [1, 126]

Use- Class A is used by organizations requiring very large size networks like NASA, Pentagon etc.

Class B (Prefix 10 fixed)

Range : [128,191]

In class B IP Address,

- The first 16 bits are used for the Network ID.
- The remaining 16 bits are used for the Host ID.

Total number of IP Addresses available in class B

= Numbers possible due to remaining available 30 bits(1st bit is fixed 0) = 2^{30}

Total number of networks available in class B

= Numbers possible due to remaining available 14 bits in the Net ID = 2^{14}

Total number of hosts that can be configured in class B

= Numbers possible due to available 16 bits in the Host ID – 2 = $2^{16} - 2$

Default Mask = 255.255.0.0

Range of 1st octet = [128, 191]

Use- Class B is used by organizations requiring medium size networks like IRCTC, banks etc.

Class C (Prefix 110 fixed)

Range : [192,223]

In class C IP Address,

- The first 24 bits are used for the Network ID.
- The remaining 8 bits are used for the Host ID.

Total number of IP Addresses available in class C

= Numbers possible due to remaining available 29 bits(1st 3 bit is fixed 110) = 2^{29}

Total number of networks available in class C

= Numbers possible due to remaining available 21 bits in the Net ID = 2^{21}

Total number of hosts that can be configured in class C

= Numbers possible due to available 8 bits in the Host ID – 2 = $2^{8} - 2$

Default Mask = 255.255.255.0

So, Range of 1st octet = [192, 223]

Use- Class C is used by organizations requiring small to medium size networks.For example- engineering colleges, small universities, small offices etc.

Class D (Prefix 1110 fixed)

Range : [224,239]

Class D is not divided into Network ID and Host ID.

Total number of IP Addresses available in class D

= Numbers possible due to remaining available 28 bits(1st 4 bit is fixed 1110) = 2^{28}

So,Range of 1st octet = [224, 239]

Use- Class D is reserved for multicasting.

- In multicasting, there is no need to extract host address from the IP Address.
- This is because data is not destined for a particular host.

Class E (Prefix 1111 fixed)

Range : [240,255]

Class E is not divided into Network ID and Host ID.

Total number of IP Addresses available in class E

= Numbers possible due to remaining available 28 bits(1st 4 bit is fixed 1111) = 2^{28}

So,Range of 1st octet = [240,255]

Use- Class E is reserved for future or experimental purposes.

Subnet Mask Use-

Subnet mask is used to determine to which network the given IP Address belongs to.

- Host use its subnet mask to determine whether the other host it wants to communicate with is present within the same network or not.
- If the destination host is present within the same network, then source host sends the packet directly to the destination host.
- If the destination host is present in some other network, then source host routes the packet to the default gateway (router).
- Router then sends the packet to the destination host.

Casting in Networking-

Transmitting data (stream of packets) over the network is termed as **casting**.

Types of Casting

1. Unicast
2. Broadcast
    1. Limited Broadcast
    2. Direct Broadcast
3. Multicast

1. Unicast-

- Transmitting data from one source host to one destination host is called as **unicast**.
- It is a one to one transmission.

2. Broadcast-

- Transmitting data from one source host to all other hosts residing in the same or other network is called as **broadcast**.
- It is a one to all transmission.

Based on recipient's network, it is classified as-

1. Limited Broadcast/ Destination Address
    1. Transmitting data from one source host to all other hosts residing in the same network is called as **limited broadcast**.
    2. Limited Broadcast Address for any network = All 32 bits set to 1
       = 11111111.11111111.11111111.11111111= 255.255.255.255
2. Direct Broadcast
    1. Transmitting data from one source host to all other hosts residing in some other network is called as **direct broadcast**.
    2. Network ID is the IP Address of the network where all the destination hosts are present. Host ID bits are all set to 1.

3. Multicast-

Transmitting data from one source host to a particular group of hosts having interest in receiving the data is called as **multicast**.

- It is a one to many transmission.

MAC Address Vs IP Address-

The following table summarizes the differences between MAC Address and IP Address-

MAC Address	IP Address

It stands for Media Access Control Address.	It stands for Internet Protocol Address.
MAC Address identifies the physical address of a computer on the internet.	IP Address identifies the connection of a computer on the internet.
Manufacturer of NIC card assigns the MAC Address.	Network Administrator or ISP assigns the IP Address.
Reverse Address Resolution Protocol (RARP) is used for resolving physical (MAC) Address into IP address.	Address Resolution Protocol (ARP) is used for resolving IP Address into physical (MAC) address.

Classless Addressing-

- Classless Addressing is an improved IP Addressing system.
- It makes the allocation of IP Addresses more efficient.
- It replaces the older classful addressing system based on classes.
- It is also known as **Classless Inter Domain Routing (CIDR)**.

CIDR Block-

When a user asks for specific number of IP Addresses,

- CIDR dynamically assigns a block of IP Addresses based on certain rules.
- This block contains the required number of IP Addresses as demanded by the user.
- This block of IP Addresses is called as a **CIDR block**.

Rules For Creating CIDR Block-

CIDR block is created based on the following 4 rules-

- All the IP Addresses in the CIDR block must be contiguous.
- The size of the block must be presentable as power of 2.
- Size of the block is the total number of IP Addresses contained in the block.
- First IP Address of the block must be divisible by the size of the block.

CIDR Notation-

CIDR IP Addresses look like-

a.b.c.d / n

- They end with a slash followed by a number called as IP network prefix.
- IP network prefix tells the number of bits used for the identification of network.
- Remaining bits are used for the identification of hosts in the network.

Subnetting

In networking,

- The process of dividing a single network into multiple sub networks is called as **subnetting**.
- The sub networks so created are called as **subnets**.

Advantages-

The two main advantages of subnetting a network are-

- It improves the security.
- The maintenance and administration of subnets is easy.

Subnet ID-

- Each subnet has its unique network address known as its **Subnet ID**.
- The subnet ID is created by borrowing some bits from the Host ID part of the IP Address.
- The number of bits borrowed depends on the number of subnets created.

Types of Subnetting-

Subnetting of a network may be carried out in the following two ways-

1. Fixed Length Subnetting
   - Fixed length subnetting also called as **classful subnetting** divides the network into subnets where-
   - All the subnets are of same size.
   - All the subnets have equal number of hosts.
   - All the subnets have same subnet mask.
2. Variable Length Subnetting
   - Variable length subnetting also called as **classless subnetting** divides the network into subnets where-
   - All the subnets are not of same size.
   - All the subnets do not have equal number of hosts.
   - All the subnets do not have same subnet mask.

Disadvantages of Subnetting-

- Subnetting leads to loss of IP Addresses.
- Subnetting leads to complicated communication process.

Use of Subnet Mask-

- Subnet mask is used to determine to which subnet the given IP Address belongs to.

Ipv6

IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. It uses 128-bit addresses; a shortage of these addresses is not likely any time in the foreseeable future .

. Its major goals were:

1. Support billions of hosts, even with inefficient address allocation.
2. Reduce the size of the routing tables.
3. Simplify the protocol, to allow routers to process packets faster.
4. Provide better security (authentication and privacy).
5. Pay more attention to the type of service, particularly for real-time data.
6. Aid multicasting by allowing scopes to be specified.
7. Make it possible for a host to roam without changing its address.
8. Allow the protocol to evolve in the future.
9. Permit the old and new protocols to coexist for years.

The design of IPv6 presented a major opportunity to improve all of the features in IPv4 that fall short of what is now wanted.

Three Address Types

- **Unicast**—For a single interface.

  A unicast address defines a single interface (computer or router). The packet sent to a unicast address will be routed to the intended recipient.

- **Multicast**—For a set of interfaces on the same physical medium. A packet is sent to all interfaces associated with the address.

  A multicast address also defines a group of computers. However, there is a difference between anycasting and multicasting. In anycasting, only one copy of the packet is sent to one of the members of the group; in multicasting each member of the group receives a copy

- **Anycast**—For a set of interfaces on different physical media. A packet is sent to only one of the interfaces associated with this address, not to all the interfaces.

  An anycast address defines a group of computers that all share a single address. A packet with an anycast address is delivered to only one member of the group, the most reachable one

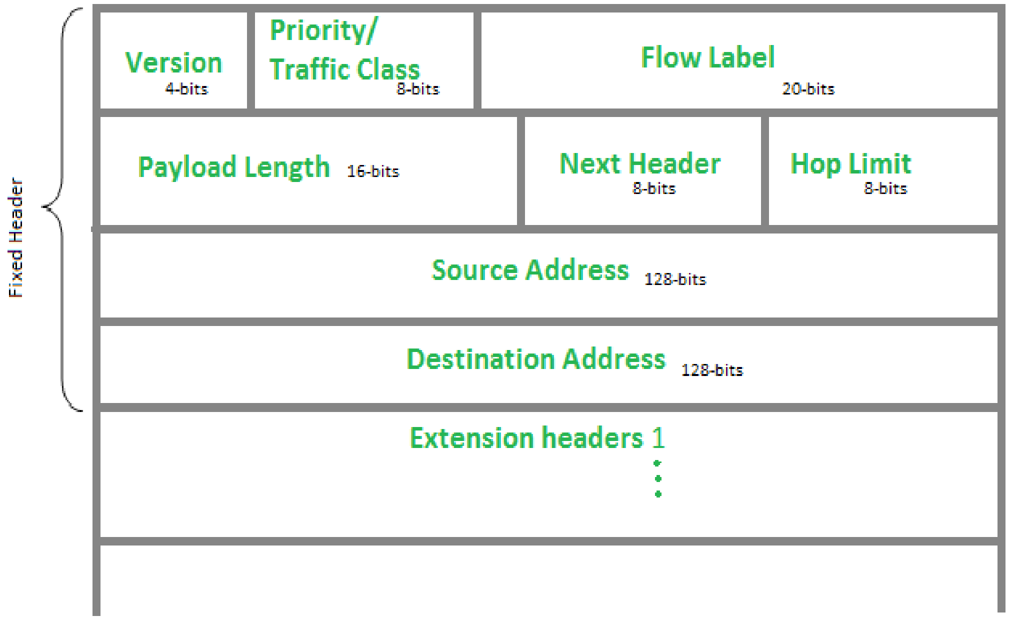
Advantages :

First and foremost, IPv6 has longer addresses than IPv4. They are 128 bits long, which solves the problem that IPv6 set out to solve: providing an effectively unlimited supply of Internet addresses

The second major improvement of IPv6 is the simplification of the header.

The third major improvement is better support for options

A fourth area in which IPv6 represents a big advance is in security



They are written as eight groups of four hexadecimal digits with colons between the groups, like this: 8000:0000:0000:0000:0123:4567:89AB:CDEF

ICMP

Since IP does not have a inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide an error control. It is used for reporting errors and management queries. It is a supporting protocol and used by networks devices like routers for sending the error messages and operations information.
e.g. the requested service is not available or that a host or router could not be reached.

ARP

The acronym ARP stands for Address Resolution Protocol which is one of the most important protocols of the Network layer in the OSI model.

The important terms associated with ARP are :

1. **ARP Cache:** After resolving MAC address, the ARP sends it to the source where it stores in a table for future reference. The subsequent communications can use the MAC address from the table
2. **ARP Cache Timeout:** It indicates the time for which the MAC address in the ARP cache can reside
3. **ARP request:** This is nothing but broadcasting a packet over the network to validate whether we came across destination MAC address or not.
    1. The physical address of the sender.
    2. The IP address of the sender.
    3. The physical address of the receiver is FF:FF:FF:FF:FF:FF or 1's.
    4. The IP address of the receiver
4. **ARP response/reply:** It is the MAC address response that the source receives from the destination which aids in further communication of the data.

DHCP

Dynamic Host Configuration Protocol(DHCP) is an application layer protocol which is used to provide:

1. Subnet Mask (Option 1 – e.g., 255.255.255.0)
2. Router Address (Option 3 – e.g., 192.168.1.1)
3. DNS Address (Option 6 – e.g., 8.8.8.8)
4. Vendor Class Identifier (Option 43 – e.g., 'unifi' = 192.168.1.9 ##where unifi = controller)

DHCP is based on a client-server model and based on discovery, offer, request, and ACK.

DHCP **port number** for server is 67 and for the client is 68. It is a Client server protocol which uses UDP services. IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called DORA process, but there are 8 DHCP messages in the process.

Services provided to upper layer

The software and/or hardware within the transport layer that does the work is called the transport entity.

UDP Protocol-

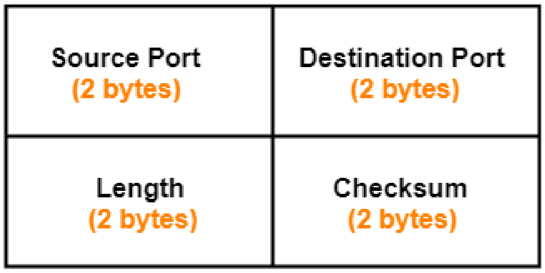
- UDP is short for **User Datagram Protocol**.
- It is the simplest transport layer protocol.
- It has been designed to send data packets over the Internet.
- It simply takes the datagram from the network layer, attaches its header and sends it to the user.

Characteristics of UDP-

- It is a connectionless protocol.
- It is a stateless protocol.
- It is an unreliable protocol.
- It is a fast protocol.
- It offers the minimal transport service.
- It is almost a null protocol.
- It does not guarantee in order delivery.
- It does not provide congestion control mechanism.
- It is a good protocol for data flowing in one direction.

Need of UDP-

- TCP proves to be an overhead for certain kinds of applications.
- The **Connection Establishment** Phase, **Connection Termination** Phase etc of TCP are time consuming.
- To avoid this overhead, certain applications which require fast speed and less overhead use UDP



Source Port (2 bytes)	Destination Port (2 bytes)
Length (2 bytes)	Checksum (2 bytes)

UDP Header

1. Source Port-

- Source Port is a 16 bit field.
- It identifies the port of the sending application.

2. Destination Port-

- Destination Port is a 16 bit field.
- It identifies the port of the receiving application.

3. Length-

- Length is a 16 bit field.
- It identifies the combined length of UDP Header and Encapsulated data.

Length = Length of UDP Header + Length of encapsulated data

4. Checksum-

- **Checksum** is a 16 bit field used for error control.
- It is calculated on UDP Header, encapsulated data and IP pseudo header.
- Checksum calculation is not mandatory in UDP.

Applications Using UDP-

Following applications use UDP-

- Applications which require one response for one request use UDP. Example- **DNS**.
- Routing Protocols like RIP and OSPF use UDP because they have very small amount of data to be transmitted.
- Trivial **File Transfer Protocol** (TFTP) uses UDP to send very small sized files.
- Broadcasting and multicasting applications use UDP.
- Streaming applications like multimedia, video conferencing etc use UDP since they require speed over reliability.
- Real time applications like chatting and online games use UDP.
- Management protocols like SNMP (Simple Network Management Protocol) use UDP.
- Bootp / DHCP uses UDP.
- Other protocols that use UDP are- Kerberos, Network Time Protocol (NTP), Network News Protocol (NNP), Quote of the day protocol etc.

TCP

Transmission Control Protocol-

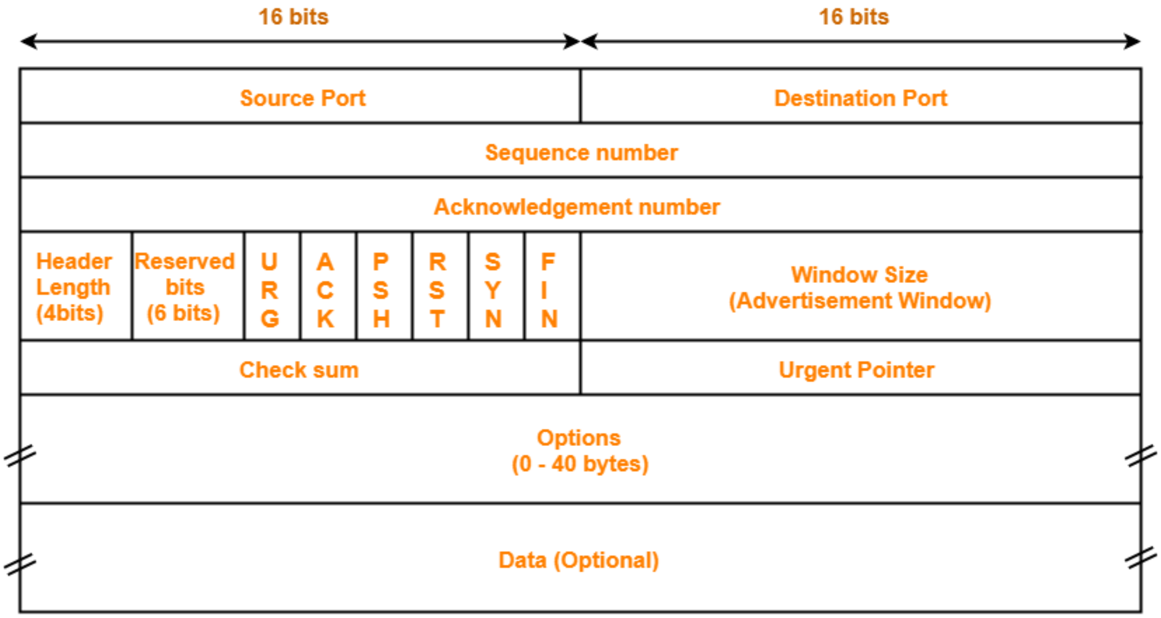
- TCP is short for **Transmission Control Protocol**.
- It is a transport layer protocol.
- It has been designed to send data packets over the Internet.
- It establishes a reliable end to end connection before sending any data.

Characteristics:

- TCP is a reliable protocol.
- TCP is a connection oriented protocol.
- TCP handles both congestion and flow control.
- TCP ensures in-order delivery.
- TCP connections are full duplex.
- TCP is a byte stream protocol.

- TCP provides error checking & recovery mechanism.
- TCP works in collaboration with Internet Protocol.
- TCP can use both selective & cumulative acknowledgements.

TCP Header



TCP Header

1. Source Port-

- Source Port is a 16 bit field.
- It identifies the port of the sending application.

2. Destination Port-

- Destination Port is a 16 bit field.
- It identifies the port of the receiving application.

3. Sequence Number-

- Sequence number is a 32 bit field.
- TCP assigns a unique sequence number to each byte of data contained in the TCP segment.
- This field contains the sequence number of the first data byte.

4. Acknowledgement Number-

- Acknowledgment number is a 32 bit field.
- It contains sequence number of the data byte that receiver expects to receive next from the sender.
- It is always sequence number of the last received data byte incremented by 1.

5. Header Length-

- Header length is a 4 bit field.
- It contains the length of TCP header.
- It helps in knowing from where the actual data begins.

Minimum and Maximum Header length-

The length of TCP header always lies in the range-
[20 bytes , 60 bytes]

6. Reserved Bits-

- The 6 bits are reserved.
- These bits are not used.

7. URG Bit-

URG bit is used to treat certain data on an urgent basis.

8. ACK Bit-

ACK bit indicates whether acknowledgement number field is valid or not.

9. PSH Bit-

PSH bit is used to push the entire buffer immediately to the receiving application.

10. RST Bit-

RST bit is used to reset the TCP connection.

11. SYN Bit-

SYN bit is used to synchronize the sequence numbers.

12. FIN Bit-

FIN bit is used to terminate the TCP connection.

13. Window Size-

- Window size is a 16 bit field.
- It contains the size of the receiving window of the sender.
- It advertises how much data (in bytes) the sender can receive without acknowledgement.
- Thus, window size is used for **Flow Control**.

14. Checksum-

- Checksum is a 16 bit field used for error control.
- It verifies the integrity of data in the TCP payload.
- Sender adds CRC checksum to the checksum field before sending the data.
- Receiver rejects the data that fails the CRC check.

15. Urgent Pointer-

- Urgent pointer is a 16 bit field.
- It indicates how much data in the current segment counting from the first data byte is urgent.
- Urgent pointer added to the sequence number indicates the end of urgent data byte.
- This field is considered valid and evaluated only if the URG bit is set to 1.

16. Options-

- Options field is used for several purposes.
- The size of options field vary from 0 bytes to 40 bytes.

Options field is generally used for the following purposes-

1. Time stamp
2. Window size extension
3. Parameter negotiation
4. Padding

A. Time Stamp-

When wrap around time is less than life time of a segment,

- Multiple segments having the same sequence number may appear at the receiver side.
- This makes it difficult for the receiver to identify the correct segment.
- If time stamp is used, it marks the age of TCP segments.
- Based on the time stamp, receiver can identify the correct segment.

B. Window Size Extension-

- Options field may be used to represent a window size greater than 16 bits.
- Using window size field of TCP header, window size of only 16 bits can be represented.
- If the receiver wants to receive more data, it can advertise its greater window size using this field.
- The extra bits are then appended in Options field.

C. Parameter Negotiation-

Options field is used for parameters negotiation.

Example- During connection establishment,

- Both sender and receiver have to specify their maximum segment size.
- To specify maximum segment size, there is no special field.
- So, they specify their maximum segment size using this field and negotiates.

D. Padding-

- Addition of dummy data to fill up unused space in the transmission unit and make it conform to the standard size is called as padding.
- Options field is used for padding.

The TCP Service Model

TCP service is obtained by both the sender and the receiver creating end points, called sockets.Each socket has a socket number (address) consisting of the IP address of the host and a 16-bit number local to that host, called a **port .**

A port is the TCP name for a TSAP. For TCP service to be obtained, a connection must be explicitly established between a socket on one machine and a socket on another machine .

Port numbers below 1024 are reserved for standard services that can usually only be started by privileged users (e.g., root in UNIX systems). They are called well-known ports.

Connection Establishment

For establishing a connection,

- Client sends a request segment to the server.(SYN bit set to 1)
- Request segment consists only of TCP Header with an empty payload.
- Then, it waits for a reply segment from the server.

1. Initial Sequence Number-

- Client sends the initial sequence number to the server.
- It is contained in the sequence number field.

- It is a randomly chosen 32 bit value.

2. SYN Bit Set To 1-

Client sets SYN bit to 1 which indicates the server-

- This segment contains the initial sequence number used by the client.
- It has been sent for synchronizing the sequence numbers.

3. Maximum Segment Size (MSS)-

- Client sends its MSS to the server.
- It dictates the size of the largest data chunk that client can send and receive from the server.
- It is contained in the Options field.

4. Receiving Window Size-

- Client sends its receiving window size to the server.
- It dictates the limit of unacknowledged data that can be sent to the client.
- It is contained in the window size field.

Step-02: SYN + ACK-

After receiving the request segment,

- Server responds to the client by sending the reply segment.
- It informs the client of the parameters at the server side.

After receiving the request segment,

- Server responds to the client by sending the reply segment.
- It informs the client of the parameters at the server side.

Reply segment contains the following information in TCP header-

1. Initial sequence number
2. SYN bit set to 1
3. Maximum segment size
4. Receiving window size
5. Acknowledgment number
6. ACK bit set to 1

1. Initial Sequence Number-

- Server sends the initial sequence number to the client.
- It is contained in the sequence number field.
- It is a randomly chosen 32 bit value.

2. SYN Bit Set To 1-

Server sets SYN bit to 1 which indicates the client-

- This segment contains the initial sequence number used by the server.
- It has been sent for synchronizing the sequence numbers.

3. Maximum Segment Size (MSS)-

- Server sends its MSS to the client.
- It dictates the size of the largest data chunk that server can send and receive from the client.
- It is contained in the Options field.

4. Receiving Window Size-

- Server sends its receiving window size to the client.
- It dictates the limit of unacknowledged data that can be sent to the server.
- It is contained in the window size field.

5. Acknowledgement Number-

- Server sends the initial sequence number incremented by 1 as an acknowledgement number.
- It dictates the sequence number of the next data byte that server expects to receive from the client.

6. ACK Bit Set To 1-

- Server sets ACK bit to 1.
- It indicates the client that the acknowledgement number field in the current segment is

valid.

Step-03: ACK-

After receiving the reply segment,

- Client acknowledges the response of server.
- It acknowledges the server by sending a pure acknowledgement.

TCP Retransmission-

After establishing the connection,

- Sender starts transmitting TCP segments to the receiver.
- A TCP segment sent by the sender may get lost on the way before reaching the receiver.
- This causes the receiver to send the acknowledgement with same ACK number to the sender.
- As a result, sender retransmits the same segment to the receiver.
- This is called as **TCP retransmission**.

Sender discovers that the TCP segment is lost when-

1. Either Time Out Timer expires
2. Or it receives three duplicate acknowledgements

TCP Connection Termination-

A TCP connection is terminated using FIN segment where FIN bit is set to 1.

Consider-

- There is a well established TCP connection between the client and server.
- Client wants to terminate the connection.

The following steps are followed in terminating the connection-

Step-01:

For terminating the connection,

- Client sends a FIN segment to the server with FIN bit set to 1.
- Client enters the FIN_WAIT_1 state.
- Client waits for an acknowledgement from the server.

Step-02:

After receiving the FIN segment,

- Server frees up its buffers.
- Server sends an acknowledgement to the client.
- Server enters the CLOSE_WAIT state.

Step-03:

After receiving the acknowledgement, client enters the FIN_WAIT_2 state.

Now,

- The connection from client to server is terminated i.e. one way connection is closed.
- Client can not send any data to the server since server has released its buffers.
- Pure acknowledgements can still be sent from the client to server.
- The connection from server to client is still open i.e. one way connection is still open.
- Server can send both data and acknowledgements to the client.

Step-04:

Now, suppose server wants to close the connection with the client.

For terminating the connection,

- Server sends a FIN segment to the client with FIN bit set to 1.
- Server waits for an acknowledgement from the client.

Step-05:

After receiving the FIN segment,

- Client frees up its buffers.
- Client sends an acknowledgement to the server (not mandatory).
- Client enters the TIME_WAIT state.

TIME_WAIT State-

- The TIME_WAIT state allows the client to resend the final acknowledgement if it gets lost.
- The time spent by the client in TIME_WAIT state depends on the implementation.
- The typical values are 30 seconds, 1 minute and 2 minutes.
- After the wait, the connection gets formally closed.

Transport Layer Services :

1. Process-to-process communication:

The first duty of a transport-layer protocol is to provide process-to-process communication. A process is an application-layer entity (running program) that uses the services of the transport layer. Before we discuss how process-to-process communication can be accomplished, we need to understand the difference between host-to-host communication and process-to-process communication.

.To define the processes, we need second identifiers, called **port numbers.** In the TCP/IP protocol suite, the port numbers are integers between 0 and 65,535 (16 bits). The client program defines itself with a port number, called the **ephemeral port number**. The word ephemeral means “short-lived” and is used because the life of a client is normally short. An ephemeral port number is recommended to be greater than 1023 for some client/server programs to work properly.

The server process must also define itself with a port number. This port number, however, cannot be chosen randomly

one solution would be to send a special packet and request the port number of a specific server, but this creates more overhead. TCP/IP has decided to use universal port numbers for servers; these are called **well-known port numbers**. There are some exceptions to this rule; for example, there are clients that are assigned well-known port numbers. Every client process knows the well-known port number of the corresponding server process.

2. ICANN Ranges

ICANN has divided the port numbers into three ranges: well-known, registered, and dynamic (or private) .

- **Well-known ports.** The ports ranging from 0 to 1023 are assigned and controlled by ICANN. These are the well-known ports.
- **Registered ports.** The ports ranging from 1024 to 49,151 are not assigned or controlled by ICANN. They can only be registered with ICANN to prevent duplication.
- **Dynamic ports.** The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used as temporary or private port numbers.

Two Connections :

The two connections in FTP have different lifetimes. The control connection remains connected during the entire interactive FTP session.

When a user starts an FTP session, the control connection opens. While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred. FTP uses two well-known TCP ports: port 21 is used for the control connection, and port 20 is used for the data connection.

Control Connection

For sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files, etc., FTP makes use of control connection. The control connection is initiated on port number 21.

Data Connection

For sending the actual file, FTP makes use of data connection. A data connection is initiated on port number 20.
FTP sends the control information out-of-band as it uses a separate control connection. Some protocols send their request and response header lines and the data in the same TCP connection. For this reason, they are said to send their control information in-band. HTTP and SMTP are such examples.

Communication over Data Connection

.The heterogeneity problem is resolved by defining three attributes of communication: file type, data structure, and transmission mode.

File Type : FTP can transfer one of the following file types across the data connection: ASCII file, EBCDIC file, or image file.

Data Structures : FTP allows three types of data structures :

1. **File Structure –** In file-structure there is no internal structure and the file is considered to be a continuous sequence of data bytes.
2. **Record Structure –** In record-structure the file is made up of sequential records.
3. **Page Structure –** In page-structure the file is made up of independent indexed pages.

Transmission Mode: FTP can transfer a file across the data connection using one of the following three transmission modes:

1. **Stream mode :** The stream mode is the default mode; data are delivered from FTP to TCP as a continuous stream of bytes.

2. **Block mode or Compressed mode :** In the block mode, data can be delivered from FTP to TCP in blocks. In this case, each block is preceded by a 3-byte header. The first byte is called the block descriptor; the next two bytes define the size of the block in bytes.

FTP Security

The FTP protocol was designed when security was not a big issue. Although FTP requires a password, the password is sent in plaintext (unencrypted), which means it can be intercepted and used by an attacker.

The data transfer connection also transfers data in plaintext, which is insecure. To be secure, one can add a Secure Socket Layer between the FTP application layer and the TCP layer.In this case FTP is called SSL-FTP .

Advantages of FTP:

- **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.

- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
- **Back & forth movement:** FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.

TELNET

TELNET stands for **TE**rmina**L NET**work. It is a type of protocol that enables one computer to connect to local computer. It is a used as a standard **TCP/IP protocol** for virtual terminal service which is given by **ISO** .generic client/server pairs as remote logging applications. One of the original remote logging protocols is TELNET .

Computer which starts connection known as the **local computer**. Computer which is being connected to i.e. which accepts the connection known as **remote computer** .

TELNET here for two reasons:

1. The simple plaintext architecture of TELNET allows us to explain the issues and challenges related to the concept of remote logging, which is also used in SSH when it serves as a remote logging protocol.
2. Network administrators often use TELNET for diagnostic and debugging purposes.

Local versus Remote Logging :

When a user logs into a local system, it is called **local logging**. As a user types at a terminal or at a workstation running a terminal emulator, the keystrokes are accepted by the terminal driver. The terminal driver passes the characters to the operating system. The operating system, in turn, interprets the combination of characters and invokes the desired application program or utility.

when a user wants to access an application program or utility located on a remote machine, she performs **remote logging**. Here the TELNET client and server programs come into use. The user sends the keystrokes to the terminal driver where the local operating system accepts the characters but does not interpret them. The characters are sent to the TELNET client, which transforms the characters into a universal character set called **Network Virtual Terminal (NVT)** characters (discussed below) and delivers them to the local TCP/IP stack .

the characters cannot be passed directly to the operating system because the remote operating system is not designed to receive characters from a TELNET server; it is designed to receive characters from a terminal driver. The solution is to add a piece of software called a **pseudoterminal driver**, which pretends that the characters are coming from a terminal. The operating system then passes the characters to the appropriate application program.

NVT

If we want to access any remote computer in the world, we must first know what type of computer we will be connected to, and we must also install the specific terminal emulator used by that computer. TELNET solves this problem by defining a universal interface called the Network Virtual Terminal (NVT) character set.

NVT uses two sets of characters, one for data and one for control. **For data,** NVT normally uses what is called NVT ASCII. This is an 8-bit character set in which the seven lowest order bits are the same as US ASCII and the highest order bit is 0. To send control characters between computers (from client to server or vice versa), NVT uses an 8-bit character set in which the highest order bit is set to 1.

Options

TELNET lets the client and server negotiate options before or during the use of the service. Options are extra features available to a user with a more sophisticated terminal. Users with simpler terminals can use default features.

User Interface

The operating system (UNIX, for example) defines an interface with user-friendly commands

Command	**Meaning**
open	Connect to a remote computer
set	Set the operating parameters
close	Close the connection
status	Display the status information
display	Show the operating parameters
send	Send special characters
mode	Change to line or character mode
quit	Exit TELNET

DNS

DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

Asolute

An absolute URL typically takes the following form:

```
protocol://domain/path
```

The protocol is usually http://, but can also be https://, ftp://, gopher://, or file://. The domain is the name of the website. For example, the domain name of Indiana University's central web server is www.indiana.edu. The path includes directory and file information. You must use absolute URLs when referring to links on different servers.

Relative

Relative URLs can take a number of different forms. When referring to a file that occurs in the same directory as the referring page, a URL can be as simple as the name of the file. For example, if you want to create a link in your home page to the file foobar.html, which is in the same directory as your home page, you would use:

```
<a href="foobar.html">The Wonderful World of Foobar!</a>
```

If the file you want to link to is in a subdirectory of the referring page's directory, you need to enter only the directory information and the name of the file

Important application layer protocols are-

- **Domain Name Service (DNS)**
- **Hyper Text Transfer Protocol (HTTP)**
- **Simple Mail Transfer Protocol (SMTP)**
- **Post Office Protocol (POP)**
- **File Transfer Protocol (FTP)**

DNS

- DNS is short for **Domain Name Service** or **Domain Name System**.
- It is an application layer protocol.
- DNS is a host name to IP Address translation service.

- It converts the names we type in our web browser address bar to the IP Address of web servers hosting those sites.
- The need for Domain Name Service arises due to the following reasons-
  - **IP Addresses** are not static and may change dynamically.So, a mapping is required which maps the domain names to the IP Addresses of their web servers.
  - IP Addresses are a complex series of numbers.So, it is difficult to remember IP Addresses directly while it is easy to remember names.
- **DNS Resoultion**
  - DNS Resolution is a process of resolving a domain name onto an IP Address.
  - The steps involved in DNS Resolution are-
    - A user program sends a name query to a library procedure called the resolver.
    - Resolver looks up the local domain name cache for a match.
      - If a match is found, it sends the corresponding IP Address back.
      - If no match is found, it sends a query to the local DNS server.
    - DNS server looks up the name.
      - If a match is found, it returns the corresponding IP Address to the resolver.
      - If no match is found, the local DNS server sends a query to a higher level DNS server.
      - This process is continued until a result is returned.
    - DNS server looks up the name.
      - If a match is found, it returns the corresponding IP Address to the resolver.
      - If no match is found, the local DNS server sends a query to a higher level DNS server.
      - This process is continued until a result is returned.
    - After receiving a response, the DNS client returns the resolution result to the application.

Simple Mail Transfer Protocol(SMTP)

- SMTP is short for **Simple Mail Transfer Protocol.**
- It is an application layer protocol.
- It is used for sending the emails efficiently and reliably over the internet.
- The use of SMTP with extensions is called **ESMTP (Extended SMTP).**

Working-

- SMTP server is always on a listening mode.
- Client initiates a TCP connection with the SMTP server.
- SMTP server listens for a connection and initiates a connection on that port.
- The connection is established.
- Client informs the SMTP server that it would like to send a mail.
- Assuming the server is OK, client sends the mail to its mail server.
- Client’s mail server use DNS to get the IP Address of receiver’s mail server.
- Then, SMTP transfers the mail from sender’s mail server to the receiver’s mail server.

While sending the mail, SMTP is used two times-

1. Between the sender and the sender’s mail server
2. Between the sender’s mail server and the receiver’s mail server

Characteristics of SMTP-

- SMTP is a push protocol.
- SMTP uses TCP at the transport layer.
- SMTP uses port number 25.
- SMTP uses persistent TCP connections, so it can send multiple emails at once.
- SMTP is a connection oriented protocol.
- SMTP is an in-band protocol.
- SMTP is a stateless protocol.

Some SMTP extensions

Keyword	**Description**
AUTH	Client authentication
BINARYMIME	Server accepts binary messages
CHUNKING	Server accepts large messages in chunks
SIZE	Check message size before trying to send
STARTTLS	Switch to secure transport
UTF8SMTP	Internationalized addresses

Architecture

Pages are generally viewed with a program called a **browser.**

A piece of text, icon, image, and so on associated with another page is called a **hyperlink.**

the Web consists of a vast, worldwide collection of content in the form of Web pages, often just called **pages** for short .

The idea of having one page point to another, now called **hypertext,** was invented by a visionary M.I.T. professor of electrical engineering, Vannevar Bush, in 1945 (Bush, 1945). This was long before the Internet was invented.

The request-response protocol for fetching pages is a simple text-based protocol that runs over TCP, just as was the case for SMTP. It is called **HTTP (HyperText Transfer Protocol).** The content may simply be a document that is read off a disk, or the result of a database query and program execution .

The page is a **static page** if it is a document that is the same every time it is displayed.

In contrast, if it was generated on demand by a program or contains a program it is a **dynamic page**. A dynamic page may present itself differently each time it is displayed.

The solution chosen identifies pages in a way that solves all three problems at once. Each page is assigned a **URL (Uniform Resource Locator)** that effectively serves as the page's worldwide name.

URLs have **three parts/components:**

the protocol (also known as the scheme),

the DNS name of the machine on which the page is located, and

the path uniquely indicating the specific page (a file to read or program to run on the machine) .

OR

Host Name

The name of the machine on which the resource lives.

Filename

The pathname to the file on the machine.

Port Number

The port number to which to connect (typically optional).

Reference

A reference to a named anchor within a resource that usually identifies a specific location within a file (typically optional).

As an example, the URL of the page

http://www.cs.washington.edu/index.html

This URL consists of three parts: the protocol (http), the DNS name of the host (www.cs.washington.edu), and the path name (index.html).

1. The browser determines the URL (by seeing what was selected).
2. The browser asks DNS for the IP address of the server www.cs.washington.edu.
3. DNS replies with 128.208.3.88.
4. The browser makes a TCP connection to 128.208.3.88 on port 80, the well-known port for the HTTP protocol.
5. It sends over an HTTP request asking for the page /index.html.
6. The www.cs.washington.edu server sends the page as an HTTP response, for example, by sending the file /index.html.
7. If the page includes URLs that are needed for display, the browser fetches the other URLs using the same process. In this case, the URLs include multiple embedded images also fetched from www.cs.washington.edu, an embedded video from youtube.com, and a script from google-analytics.com.
8. The browser displays the page /index.html .
9. The TCP connections are released if there are no other requests to the same servers for a short period.

Name	**Used for**	**Example**
http	Hypertext (HTML)	http://www.ee.uwa.edu/~rob/
https	Hypertext with security	https://www.bank.com/accounts/
ftp	FTP	ftp://ftp.cs.vu.nl/pub/minix/README
file	Local file	file:///usr/suzanne/prog.c
mailto	Sending email	mailto:JohnUser@acm.org
rtsp	Streaming media	rtsp://youtube.com/montypython.mpg
sip	Multimedia calls	sip:eve@adversary.com
about	Browser information	about:plugins

The http protocol is the Web’s native language, the one spoken by Web servers. **HTTP** stands for HyperText Transfer Protocol.

The **ftp** protocol is used to access files by FTP, the Internet’s file transfer protocol. FTP predates the Web and has been in use for more than three decades. The Web makes it easy to obtain files placed on numerous FTP servers throughout the world by providing a simple, clickable interface instead of a command-line interface. This improved access to information is one reason for the spectacular growth of the Web.

To solve this kind of problem, URLs have been generalized into **URIs (Uniform Resource Identifiers)**. Some URIs tell how to locate a resource. These are the URLs. Other URIs tell the name of a resource but not where to find it. These URIs are called **URNs (Uniform Resource Names).** The rules for writing URIs are given in RFC 3986, while the different URI schemes in use are tracked by IANA.

A **plug-in** is a third-party code module that is installed as an extension to the browser .

Common examples are plug-ins for PDF, Flash, and Quicktime to render documents and play audio and video. Because plug-ins run inside the browser, they have access to the current page and can modify its appearance.

The Server Side

That server is given the name of a file to look up and return via the network. In both cases, the steps that the server performs in its main loop are:

1. Accept a TCP connection from a client (a browser).
2. Get the path to the page, which is the name of the file requested.
3. Get the file (from disk).
4. Send the contents of the file to the client.
5. Release the TCP connection.

These steps occur after the TCP connection and any secure transport mechanism (such as SSL/TLS, which will be described in Chap. 8) have been established.

1. Resolve the name of the Web page requested.
2. Perform access control on the Web page.
3. Check the cache.
4. Fetch the requested page from disk or run a program to build it.
5. Determine the rest of the response (e.g., the MIME type to send).
6. Return the response to the client.
7. Make an entry in the server log.

- **Difference between 1-persistent and Non-persistent CSMA :**

Basis	1-persistent CSMA	Non-persistent CSMA
Carrier Sense	When channel is idle it will send with probability 1.	When channel is idle it will send frame.
Waiting	It will continuously sense channel for transmission of frames.	It will wait for random amount of time to check carrier.

Basis	1-persistent CSMA	Non-persistent CSMA
Chance of Collision	In this method, there are highest number of collisions observed.	In this method, chance of collision are less than in 1-persistent.
Utilization	It’s utilization is above ALOHA because frames are sent only when channel is found in idle state.	It’s utilization is above 1-persistent because in this all stations constantly check for channel at same time.
Delay Low Load	It is small because frames are sent only in idle state.	It is longer than 1-persistent as it only checks randomly when channel is busy.
Delay High Load	It is high due to collision.	It is longer than 1-persistent because stations check randomly when channel is busy.

- **Difference between 1-persistent and p-persistent CSMA :**

Basis	1-persistent CSMA	p-persistent CSMA
Carrier Sense	When channel is idle it will send with probability 1.	When channel is idle it will send with probability p.
Waiting	It will continuously sense channel for transmission of frames.	It will wait for next time slot for transmission of frames.
Chance of Collision	In this method, there are highest number of collisions observed.	In this method, there are less chances of collision than in 1-persistent.
Utilization	It’s utilization is above ALOHA because frames are sent only when channel is found in idle state.	It’s utilization is dependent on probability p.
Delay low load	It is small because frames are sent only in idle state.	It is large when probability p is small because station will not send always in idle state of channel.
Delay high load	It is high due to collision.	It is large when probability p of sending is small when channel is found in idle state.

- **Difference b/w TDM and FDM**

S.NO	TDM	FDM
1.	TDM stands for Time division multiplexing.	FDM stands for Frequency division multiplexing.
2.	TDM works with digital signals as well as analog signals.	While FDM works with only analog signals.
3.	TDM has low conflict.	While it has high conflict.

4.	Wiring or chip of TDM is simple.	While it’s wiring or chip is complex rather than simple.
5.	TDM is efficient.	While it is inefficient.
6.	In TDM, time sharing takes place.	While in this, frequency sharing takes place.
7.	In TDM, synchronization pulse is necessary.	While in it Guard band is necessary.

- **Explain Distance Vector Routing**

  Distance Vector Routing is a dynamic routing algorithm.

  - A router transmits its distance vector to each of its neighbors in a routing packet.
  - Each router receives and saves the most recently received distance vector from each of its neighbors.
  - A router recalculates its distance vector when:
  - It receives a distance vector from a neighbor containing different information than before.
  - It discovers that a link to a neighbor has gone down.

    Dx(y) = Estimate of least cost from x to y
    C(x,v) = Node x knows cost to each neighbor v
    Dx = [Dx(y): y ∈N] = Node x maintains distance vector
    Node x also maintains its neighbors' distance vectors
    – For each neighbor v, x maintains Dv = [Dv(y): y ∈N]

From time-to-time, each node sends its own distance vector estimate to neighbors.

- When a node x receives new DV estimate from any neighbor v, it saves v’s distance vector and it updates its own DV using B-F equation:

Dx(y) = min { C(x,v) + Dv(y), Dx(y) } for each node y ∈N

Advantages of Distance Vector routing –

- It is simpler to configure and maintain than link state routing.

Disadvantages of Distance Vector routing –

- It is slower to converge than link state.
- It is at risk from the count-to-infinity problem.
- It creates more traffic than link state since a hop count change must be propagated to all routers and processed on each router. Hop count updates take place on a periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.
- For larger networks, distance vector routing results in larger routing tables than

link state since each router must know about all other routers. This can also lead to congestion on WAN links.

- **Remote Procedure Call**

  Remote Procedure Call (RPC) is a powerful technique for constructing distributed, client-server based applications. It is based on extending the conventional local procedure calling so that the called procedure need not exist in the same address space as the calling procedure. The two processes may be on the same system, or they may be on different systems with a network connecting them.

  <u>**RPC ISSUES**</u>

- **Issues that must be addressed:**

1. RPC Runtime: RPC run-time system is a library of routines and a set of services that handle the network communications that underlie the RPC mechanism. In the course of an RPC call, client-side and server-side run-time systems' code handle **binding, establish communications over an appropriate protocol, pass call data between the client and server, and handle communications errors.**

2. Stub: The function of the stub is to **provide transparency to the programmer-written application code**.

On the client side, the stub handles the interface between the client's local procedure call and the run-time system, marshaling and unmarshaling data, invoking the RPC run-time protocol, and if requested, carrying out some of the binding steps.

On the server side, the stub provides a similar interface between the run-time system and the local manager procedures that are executed by the server.

3. Binding: How does the client know who to call, and where the service resides?

The most flexible solution is to use dynamic binding and find the server at run time when the RPC is first made. The first time the client stub is invoked, it contacts a name server to determine the transport address at which the server resides.

Binding consists of two parts:

- <u>Naming:</u>

  Remote procedures are named through interfaces. **An interface uniquely identifies a particular service, describing the types and numbers of its arguments**. It is similar in purpose to a type definition in programming languauges.

- <u>Locating:</u>

  Finding the transport address at which the server actually resides. Once we have the transport address of the service, we can send messages directly to the server.

  A Server having a service to offer exports an interface for it. Exporting an interface registers it with the system so that clients can use it.

A Client must import an (exported) interface before communication can begin.

ADVANTAGES

1. RPC provides **ABSTRACTION** i.e message-passing nature of network communication is hidden from the user.

2. RPC often omits many of the protocol layers to improve performance. Even a small performance improvement is important because a program may invoke RPCs often.

3. RPC enables the usage of the applications in the distributed environment, not only in the local environment.

4. With RPC code re-writing / re-developing effort is minimized.

5. Process-oriented and thread oriented models supported by RPC.

HTTP

HTTP headers let the client and the server pass additional information with an HTTP request or response. An HTTP header consists of its case-insensitive name followed by a colon (:), then by its value. Whitespace before the value is ignored.

Headers can be grouped according to their contexts:

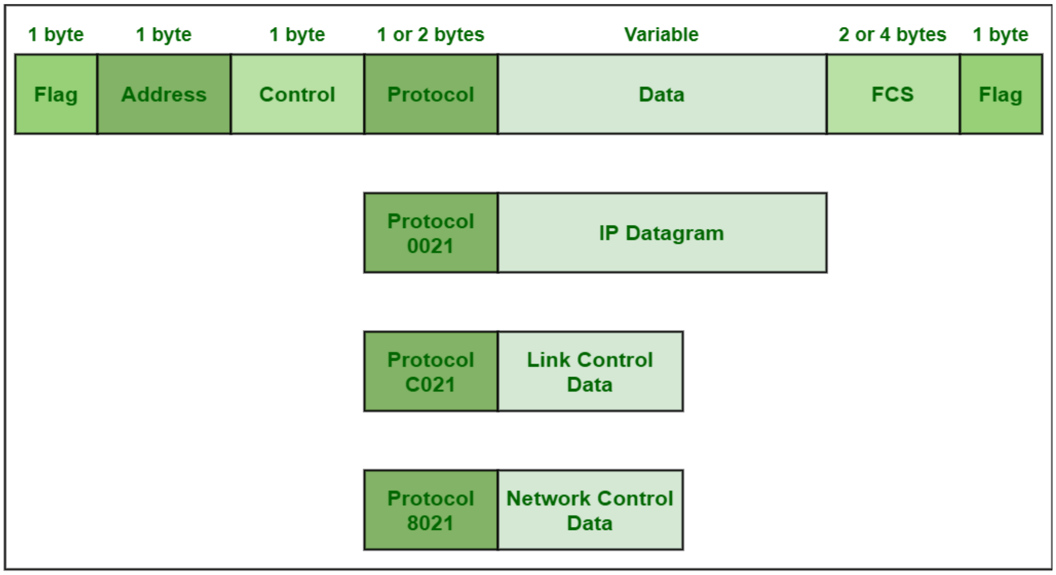
- General headers apply to both requests and responses, but with no relation to the data transmitted in the body.
- Request headers contain more information about the resource to be fetched, or about the client requesting the resource.
- Response headers hold additional information about the response, like its location or about the server providing it.
- Entity headers contain information about the body of the resource, like its content length or MIME type.

PPP

Point-to-Point Protocol (PPP) is generally the default RAS protocol in Windows and is most commonly used protocol of data link layer that is required to encapsulate higher network-layer protocols simply to pass over synchronous and asynchronous communication lines

PPP Frame Format :

PPP frame is generally required to encapsulate packets of information or data that simply includes either configuration information or data. PPP basically uses the same basic format as that of HDLC. PPP usually contains one additional field i.e. protocol field. This protocol field is present just after control field and before information or data field.



PPP Frame Format

Flag field –

PPP frame similar to HDLC frame, always begins and ends with standard HDLC flag. It always has a value of 1 byte i.e., 01111110 binary value.

1. **Address field –**
   Address field is basically broadcast address. In this, all 1's simply indicates that all of the stations are ready to accept frame. It has the value of 1 byte i.e., 11111111 binary value. PPP on the other hand, does not provide or assign individual station addresses.

2. **Control field –**
   This field basically uses format of U-frame i.e., Unnumbered frame in HDLC. In HDLC, control field is required for various purposes but in PPP, this field is set to 1 byte i.e., 00000011 binary value. This 1 byte is used for a connection-less data link.

3. **Protocol field –**
   This field basically identifies network protocol of the datagram. It usually identifies the kind of packet in the data field i.e., what exactly is being carried in data field. This field is of 1 or 2 bytes and helps in identifies the PDU (Protocol Data Unit) that is being encapsulated by PPP frame.

4. **Data field –**
   It usually contains the upper layer datagram. Network layer datagram is particularly encapsulated in this field for regular PPP data frames. Length of this field is not constant rather it varies.

5. **FCS field –**
   This field usually contains checksum simply for identification of errors. It can be either 16 bits 0r 32 bits in size. It is also calculated over address, control, protocol, and even information fields. Characters are added to frame for control and handling of errors.

Guard Bands OR why Guard bands are used in FDM

A guard band is a narrow frequency range that separates two ranges of wider frequency. This ensures that simultaneously used communication channels do not experience interference, which would result in decreased quality for both transmissions.

Guard bands are used in frequency division multiplexing (FDM).

- **Difference b/w ARP and RARP**

S.NO	ARP	RARP
1.	ARP stands for Address Resolution Protocol.	Whereas RARP stands for Reverse Address Resolution Protocol.
2.	Through ARP, (32-bit) IP address mapped into (48-bit) MAC address.	Whereas through RARP, (48-bit) MAC address of 48 bits mapped into (32-bit) IP address.
3.	In ARP, broadcast MAC address is used.	While in RARP, broadcast IP address is used.
4.	In ARP, ARP table is managed or maintained by local host.	While in RARP, RARP table is managed or maintained by RARP server.
5.	In Address Resolution Protocol, Receiver’s MAC address is fetched.	While in RARP, IP address is fetched.
6.	In ARP, ARP table uses ARP reply for its updation.	While in RARP, RARP table uses RARP reply for configuration of IP addresses .
7.	Hosts and routers uses ARP for knowing the MAC address of other hosts and routers in the networks.	While RARP is used by small users having less facilities.

- **Difference b/w OSI and TCP/IP layers**

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a

gateway between the network and end user.	communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers

- **Thick Ethernet LAN**

  Thick Ethernet was the first commercially available form of cabling supported by Ethernet. It is technically known as 10-BASE-5. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500 metres (1,600 ft). This type of cabling allows 100 stations to be connected to it by vampire taps. The stations share a single collision domain.

- **Thin Ethernet LAN**

Thin Ethernet, popularly known as cheapernet or thinnet, is among the family of Ethernet standards that uses thinner coaxial cable as a transmission media. It is technically known as 10-BASE-2. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 2 refers to the maximum segment length of about 200 metres (precisely 185 metres).

Features of Cable and Network

The salient features of 10-BASE-2 Ethernet cabling are −

- 10-BASE-2 use RG-58 A/U coaxial cable. It is thinner, more flexible, more economic and easier to install than the coaxial cable used in thick Ethernet.
- The cable has 10 Mbps transmission speed.
- The maximum segment length is 185 m and the minimum gap between stations is 50 cm.
- The maximum number of stations that can be connected is restricted to 30.
- Thinnet uses Manchester coding. A low-to-high transition in the middle of the bit period is encoded as binary 0 while a high-to-low transition in the middle of the bit period is encoded as binary 1.
- It uses BNC T-connector for connecting with the stations network interface card (NIC) and also for joining cables.
- The thin coaxial cable is terminated by a 50 ohm resistor at both the ends.

Thick Ethernet	Thin Ethernet
It is technically known as 10-BASE-5.	It is technically known as 10-BASE-5.
The maximum segment length is 500 metres.	The maximum segment length is nearly 200 metres (185 m to be exact).
It uses the thick coaxial cable RG-8/U.	It uses the thinner coaxial cable RG-58/AU.
Connectors used are vampire taps.	Connectors used are BNC connectors.
It allows a maximum of 100 stations to be connected.	It allows a maximum of 30 stations to be connected

- **Concept Of Pipelining**

In Stop and Wait protocol, only 1 packet is transmitted onto the link and then sender waits for acknowledgement from the receiver. The problem in this setup is that efficiency is very less as we are not filling the channel with more packets after 1st packet has been put onto the link. Within the total cycle time of Tt + 2*Tp units, we will now calculate the maximum number of packets that sender can transmit on the link before getting an acknowledgement.

In Tt units ----> 1 packet is Transmitted.
In 1 units ----> 1/Tt packet can be Transmitted.
In Tt + 2*Tp units -----> (Tt + 2*Tp)/Tt
packets can be Transmitted
------> 1 + 2a [Using a = Tp/Tt]

Maximum packets That can be Transmitted in total cycle time = 1+2*a

Transmission Delay (Tt) – Time to transmit the packet from host to the outgoing link. If B is the Bandwidth of the link and D is the Data Size to transmit

Propagation Delay (Tp) – It is the time taken by the first bit transferred by the host onto the outgoing link to reach the destination. It depends on the distance d and the wave propagation speed s (depends on the characteristics of the medium).

Efficiency – It is defined as the ratio of total useful time to the total cycle time of a packet. For stop and wait protocol,

Effective Bandwidth(EB) or Throughput – Number of bits sent per second.

Capacity of link – If a channel is Full Duplex, then bits can be transferred in both the directions and without any collisions. Number of bits a channel/Link can hold at maximum is its capacity.

Loopback IP Addresses

The IP address range 127.0.0.0 – 127.255.255.255 is reserved for loopback, i.e. a Host's self-address, also known as localhost address.

This loopback IP address is managed entirely by and within the operating system.

Loopback addresses, enable the Server and Client processes on a single system to communicate with each other.

When a process creates a packet with destination address as loopback address, the operating system loops it back to itself without having any interference of NIC.

Data sent on loopback is forwarded by the operating system to a virtual network interface within operating system. This address is mostly used for testing purposes like client-server architecture on a single machine.

For example, if a host machine can successfully ping 127.0.0.2 or any IP from loopback range, implies that the TCP/IP software stack on the machine is successfully loaded and working.

- **Broadcasting**(Normal not Unicast...)

  Broadcasting in computer network is a group communication, where a sender sends data to receivers simultaneously. This is an all − to − all communication model where each sending device transmits data to all other devices in the network domain.

The ways of operation of broadcasting may be −

- A high level operation in a program, like broadcasting in Message Passing Interface.
- A low level networking operation, like broadcasting on Ethernet.

Advantages of Broadcasting

Broadcast helps to attain economies of scale when a common data stream needs to be delivered to all, by minimizing the communication and processing overhead. It ensures better utilization of resources and faster delivery in comparison to several unicast communication.

Disadvantages of Broadcasting

Broadcasting cannot accommodate a very large amount of devices. Also it does not allow personalisation of the messages according to the individual preferences of the devices.

- **TCP Sliding Window**

What is a TCP Window?

A TCP window is the amount of unacknowledged data a sender can send on a particular connection before it gets an acknowledgment back from the receiver, that it has received some of the data.

TCP Sliding Window

The working of the TCP sliding window mechanism can be explained as below.

- The sending device can send all packets within the TCP window size (as specified in the TCP header) without receiving an ACK, and should start a timeout timer for each of them.
- The receiving device should acknowledge each packet it received, indicating the sequence number of the last well-received packet. After receiving the ACK from the receiving device, the sending device slides the window to right side.

- The comparison of baseband and broadband in CSMA/CD schemes is as follows:

Different carrier sense (CS): Baseband detects the presence of transition between binary 1 and binary 0 on the channels, but broadband performs the actual carrier sense, just like the technique used in the telephone network.

Different collision detection (CD) techniques: Baseband compares the received signal with a collision detection (CD) threshold. If the received signal exceeds the threshold, it claims that the collision is detected. It may fail to detect a collision due to signal attenuation. Broadband performs a bit-by-bit comparison or lets the headend perform collision detection by checking whether higher signal strength is received at the headend. If the headend detects a collision, it sends a jamming signal to the outbound channel.

- **Max and Min frame size for Ethernet**

  The **minimum frame size** including the header and cyclic redundancy check (CRC) is 64 bytes. Jumbo frames can take the **maximum frame size** up to around 16K bytes.

- **how is connection oriented service is implemented at network layer**

  Connection-Oriented Service is basically a technique that is typically used to transport and send data at session layer.

  The data streams or packets are transferred or delivered to receiver in a similar order in which they have seen transferred by sender.

  It is actually a data transfer method among two devices or computers in a different network, that is designed and developed after telephone system.

  Whenever a network implements this service, it sends or transfers data or message from sender or source to receiver or destination in correct order and manner.

  This connection service is generally provided by protocols of both network layer (signifies different path for various data packets that belongs to same message) as well as transport layer (use to exhibits independence among packets rather than different paths that various packets belong to same message will follow).

- Advantages and Disadvantages of Optical Fibre

  The **advantages of optical fiber** include the following.

  - Bandwidth is higher than copper cables
  - Less power loss and allows data transmission for longer distances
  - The optical cable is resistance for electromagnetic interference
  - The size of the fiber cable is 4.5 times better than copper wires and
  - These cables are lighter, thinner, and occupy less area compare with metal wires.
  - Installation is very easy due to less weight.
  - The optical fiber cable is very hard to tap because they don't produce electromagnetic energy. These cables are very secure while carrying or transmitting data.

- A fiber optic cable is very flexible, easily bends, and opposes most acidic elements that hit the copper wire.

The **disadvantages of optical fiber** include the following

- The optical fiber cables are very difficult to merge & there will be a loss of the beam within the cable while scattering.
- The Installation of these cables is cost-effective. They are not as robust as the wires. Special test equipment is often required to the optical fiber.
- Fiber optic cables are compact and highly vulnerable while fitting
- These cables are more delicate than copper wires.
- Special devices are needed to check the transmission of fiber cable.

- Optimality Principle

Principle of Optimality

- Definition: A problem is said to satisfy the Principle of Optimality if the subsolutions of an optimal solution of the problem are themesleves optimal solutions for their subproblems.
- Examples:
  - The shortest path problem satisfies the Principle of Optimality.
  - This is because if a,x1,x2,...,xn,b is a shortest path from node a to node b in a graph, then the portion of xi to xj on that path is a shortest path from xi to xj.

- **Hub Bridge Router**

The key difference between hubs, switches and bridges is that hubs operate at Layer 1 of the OSI model, while bridges and switches work with MAC addresses at Layer 2. Hubs broadcast incoming traffic on all ports, whereas bridges and switches only route traffic towards their addressed destinations.

- **Difference b/w Data Element and Signal Element**

Data Element	Signal Element
1. A data element is the smallest entity that can represent a piece of information (a bit)	1. A signal element is the shortest unit of a digital signal.
2. Data elements are what we need to send 3. Data elements are being carried	2. signal elements are what we can send 3. signal elements are the carriers.

- **Count to Infinity Problem**

  1. One of the important issue in Distance Vector Routing is County of Infinity Problem.
  2. Counting to infinity is just another name for a routing loop.
  3. In distance vector routing, routing loops usually occur when an interface goes down.
  4. It can also occur when two routers send updates to each other at the same time.

- **QAM**

  Quadrature amplitude modulation (QAM) is a modulation scheme used for both digital and analog signals. QAM doubles the effective bandwidth by combining two amplitude-modulated signals into a single channel .

  Quadrature amplitude modulation (QAM) is a technique used to transmit two digital bit streams or two analog signals by modulating or changing the amplitudes of two carrier waves so that they differ in phase by 90 degrees, a quarter of a cycle, hence the name quadrature.

- **Significance of twisting in twisted pair cable**

  The flow of current generates an electromagnetic field of interference around the wire that creates noise the can impact signals being transmitted through surrounding wire and cable.

  In order to help eliminate this electromagnetic interference, the wire is twisted together to create a canceling effect.By twisting wires that carry an equal and opposite amount of current through them, the interference/noise produced by one wire is effectively canceled by the interference/noise produced by the other.A twisted pair also improves rejection of external electromagnetic interference from other equipment.

- **Flow Control in Data Link Layer**

  Flow control is design issue at Data Link Layer. It is technique that generally observes proper flow of data from sender to receiver. It is very essential because it is possible for sender to transmit data or information at very fast rate and hence receiver can receive this information and process it.

  Flow control in Data Link Layer simply restricts and coordinates number of frames or amount of data sender can send just before it waits for an acknowledgment from receiver.

  Flow control is actually set of procedures that explains sender about how much data or frames it can transfer or transmit before data overwhelms receiver.

  Approaches to Flow Control :

Flow Control is classified into two categories –

Feedback – based Flow Control

Rate – based Flow Control

Techniques of Flow Control in Data Link Layer :

There are basically two types of techniques being developed to control the flow of data –

Stop-and-Wait Flow Control

This method is the easiest and simplest form of flow control. In this method, basically message or data is broken down into various multiple frames, and then receiver indicates its readiness to receive frame of data. When acknowledgment is received, then only sender will send or transfer the next frame.

This process is continued until sender transmits EOT (End of Transmission) frame. In this method, only one of frames can be in transmission at a time. It leads to inefficiency i.e. less productivity if propagation delay is very much longer than the transmission delay.

Advantages –

- This method is very easiest and simple and each of the frames is checked and acknowledged well.
- It can also be used for noisy channels.
- This method is also very accurate.

Disadvantages –

- This method is fairly slow.
- In this, only one packet or frame can be sent at a time.
- It is very inefficient and makes the transmission process very slow.

Sliding Window Flow Control

This method is required where reliable in-order delivery of packets or frames is very much needed like in data link layer. It is point to point protocol that assumes that none of the other entity tries to communicate until current data or frame transfer gets completed. In this method, sender transmits or sends various frames or packets before receiving any acknowledgment.

In this method, both the sender and receiver agree upon total number of data frames after which acknowledgment is needed to be transmitted. Data Link Layer requires and uses this method that simply allows sender to have more than one unacknowledged packet “in-flight” at a time. This increases and improves network throughput.

Advantages –

- It performs much better than stop-and-wait flow control.
- This method increases efficiency.
- Multiples frames can be sent one after another.

Disadvantages –

- The main issue is complexity at the sender and receiver due to the transferring of multiple frames.
- The receiver might receive data frames or packets out the sequence.

- **Difference b/w data rate and signal rate**
- **Self Synchronization**

  A self-synchronizing digital signal includes timing information in the data being transmitted. This can be achieved if there are transitions in the signal that alert the receiver to the beginning, middle, or end of the pulse

- **why is header checksum of an ip packet computed at every hop from source to destination**

  This is because while traveling on network a data **packet** can become corrupt and there has to be a way at the receiving end to know that data is corrupted or not. This is the reason the **checksum** field is added to the **header**. At the **source** side, the **checksum** is **calculated** and set in **header** as a field

- **Why Selective repeat is better than Go Back N**
  - Selective repeat ARQ is efficient for noisy links whereas Go Back N ARQ is inefficient for the noisy link.
  - Selective Repeat ARQ is Complicated but Go Back N ARQ is less complicated than Selective Repeat ARQ
  - In Sender and Receiver Window Size is 2^(m-1) Go Back N ARQ Sender Windows Size is 2^(m)-1 and receiver window size is 1.
  - Selective Repeat ARQ / Selective Reject ARQ is a specific instance of the Automatic-Repeat-Request (ARQ) protocol used for communications. It may be used as a protocol for the delivery and acknowledgment of message units, or it may be used as a protocol for the delivery of subdivided message sub-units.
  -

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	If error rate is high, it wastes a lot of	Comparatively less bandwidth is

Basis for Comparison	Go-Back-N	Selective Repeat
Utilization	bandwidth.	wasted in retransmitting.
Complexity	Less complicated.	More complex as it require to apply extra logic and sorting and storage, at sender and receiver.
Window size	N-1	<= (N+1)/2
Sorting	Sorting is neither required at sender side nor at receiver side.	Receiver must be able to sort as it has to maintain the sequence of the frames.
Storing	Receiver do not store the frames received after the damaged frame until the damaged frame is retransmitted.	Receiver stores the frames received after the damaged frame in the buffer until the damaged frame is replaced.
Searching	No searching of frame is required neither on sender side nor on receiver	The sender must be able to search and select only the requested frame.
ACK Numbers	NAK number refer to the next expected frame number.	NAK number refer to the frame lost.
Use	It more often used.	It is less in practice because of its complexity.

Difference between flow control and congestion control

S.NO	Flow Control	Congestion Control
1.	In flow control, Traffics are controlled which are flow from sender to a receiver.	In this, Traffics are controlled entering to the network.
2.	Data link layer and Transport layer handle it.	Network layer and Transport layer handle it.
3.	In this, Receiver's data is prevented from being overwhelmed.	In this, Network is prevented from congestion.
4.	In flow control, Only sender is responsible for the traffic.	In this, Transport layer is responsible for the traffic.
5.	In this, Traffic is prevented by slowly sending by the sender.	In this, Traffic is prevented by slowly transmitting by the transport layer.
6.	In flow control, buffer overrun is restrained in the receiver.	In congestion control, buffer overrun is restrained in the intermediate systems in the network.

What is Congestion

Too many packets present in (a part of) the network causes packet delay and loss that degrades performance. This situation is called congestion

Causes of Congestion in Network

1. Outdated or non-compatible hardware
2. Too many devices
3. Bandwidth hogs
4. Poor network design and subnets

- **Difference b/w DPCM and PCM**

S.NO	PCM	DPCM
1.	PCM stands for Pulse Code Modulation.	While DPCM stands for Differential Pulse Code Modulation.
2.	In PCM, feedback is not provided.	While in DPCM, feedback is provided.
3.	It has good signal to noise ration.	While it has moderate signal o noise ratio.
4.	It is less efficient than DPCM.	While it is more efficient than PCM.
5.	For transmission channel, PCM needs high bandwidth(B).	Whereas DPCM needs less bandwidth(B) than PCM.
6.	PCM is complex than DPCM in terms of complexity.	While DPCM is simple in terms of complexity.
7.	In PCM, seven bits are transmitted per eight sample.	In DPCM, four bits are transmitted per six sample.
8.	In PCM, for transmitting bits rate varies from fifty five to sixty four.	While in DPCM, for transmitting bits rate varies from thirty two to forty eight.

- **Network Address Translation and IPv6**

Network Address Translation is a technique which allows for the composition of a network to be completely hidden from the outside world, with the entire network identified by a single IP address. Within the network, hosts and routers have addresses which are unique to that network, typically taked from the ranges designated as "private". In order to make sure that responses get back to the right hosts when packets are sent out into the Internet, the router will construct a table associating outgoing packets with private IP addresses; the address of the relevant table entry will be stored in the packet itself. This technique is controversial however; for one thing the field in the packet where the index into the table is stored is part of the TCP header, which violates the principles of modularity and encapsulation on which the "protocol stack" models are based.

- **3-way Handshaking Process**

  TCP traffic begins with a three-way handshake. In this TCP handshake process, a client needs to initiate the conversation by requesting a communication session with the Server:

  Step 1: In the first step, the client establishes a connection with a server. It sends a segment with SYN and informs the server about the client should start communication, and with what should be its sequence number.

  Step 2: In this step **s**erver responds to the client request with SYN-ACK signal set. ACK helps you to signify the response of segment that is received and SYN signifies what sequence number it should able to start with the segments.
  Step 3: In this final step, the client acknowledges the response of the Server, and they both create a stable connection will begin the actual data transfer process.

  TCP message types

Message	Description
Syn	Used to initiate and establish a connection. It also helps you to synchronize sequence numbers between devices.
ACK	Helps to confirm to the other side that it has received the SYN.
SYN-ACK	SYN message from local device and ACK of the earlier packet.
FIN	Used to terminate a connection.

- **Difference between BOOTP and DHCP**

  BOOTP stands for Bootstrap Protocol. and DHCP stands for Dynamic host configuration protocol. These protocols square measure used for getting the information science address of the host along side the bootstrap info. The operating of each protocols is totally different in some manner.Dynamic host configuration protocol is also the extended version of the Bootstrap Protocol.

  Let’s see that the difference between that BOOTP and DHCP:

S.NO	BOOTP	DHCP
1.	BOOTP stands for Bootstrap Protocol.	While DHCP stands for Dynamic host configuration protocol.
2.	BOOTP does not provide temporary	While DHCP provides temporary IP addressing for

	IP addressing.	only limited amount of time.
3.	BOOTP does not support DHCP clients.	While it support BOOTP clients.
4.	In BOOTP, manual-configuration takes place.	While in DHCP, auto-configuration takes place.
5.	BOOTP does not support mobile machines.	Whereas DHCP supports mobile machines.
6.	BOOTP can have errors due to manual-configuration.	Whereas in DHCP errors do not occure mostly due to auto-configuration.

- **WWW**

World Wide Web (WWW)

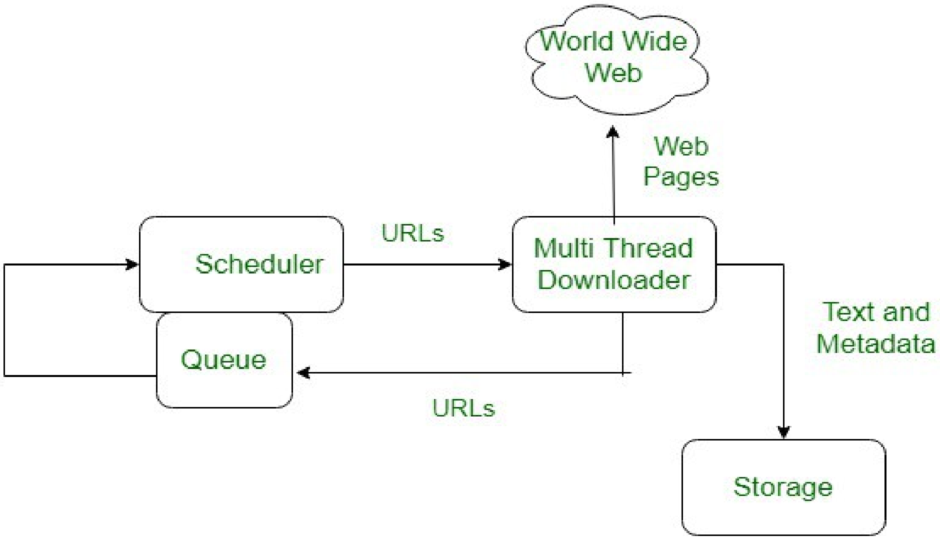
Last Updated: 22-07-2019

The **World Wide Web** abbreviated as WWW and commonly known as the web. The WWW was initiated by CERN (European library for Nuclear Research) in 1989.

History:
It is a project created, by Timothy Berner's Lee in 1989, for researchers to work together effectively at CERN. is an organisation, named World Wide Web Consortium (W3C), was developed for further development in web. This organisation is directed by Tim Berner's Lee, aka father of web.

System Architecture:
From user's point of view, the web consists of a vast, worldwide connection of documents or web pages. Each page may contain links to other pages anywhere in the world. The pages can be retrieved and viewed by using browsers of which internet explorer, Netscape Navigator, Google, Chrome, etc are the popular ones. The browser fetches the page requested interprets the text and formatting commands on it, and displays the page, properly formatted, on the screen.

The basic model of how the web works is shown in figure below. Here the browser is displaying a web page on the client machine. When the user clicks on a line of text that is linked to a page on the abd.com server, the browser follows the hyperlink by sending a message to the abd.com server asking it for the page.



Here the browser displaying web page om the client machine when the user clicks on a line of text that is linked to a page on abd.com, the vbrowser follows the hyperlink by sending a message to abd.com server asking it for the page.

Working of WWW:
The World Wide Web is based on several different technologies : Web browsers, Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP).

An Web browser is used to access webpages. Web browsers can be defined as programs which display text, data, pictures, animation and video on the Internet. Hyperlinked resources on the World Wide Web can be accessed using software interface provided by Web browsers. Initially Web browsers were used only for surfing the Web but now they have become more universal. Web browsers can be used for several tasks including conducting searches, mailing, transferring files, and much more. Some of the commonly used browsers are Internet Explorer, Opera Mini, Google Chrome.

Features of WWW:

- HyperText Information System
- Cross-Platform
- Distributed
- Open Standards and Open Source
- Uses Web Browsers to provide a single interface for many services
- Dynamic, Interactive and Evolving.
- "Web 2.0"

Components of Web
There are 3 components of web:

1. **Uniform Resource Locator (URL):** serves as system for resources on web.

2. **HyperText Transfer Protocol (HTTP):** specifies communication of browser and server.
3. **Hyper Text Markup Language (HTML):** defines structure, organisation and content of webpage.

- **Ping**

  Ping is not a client server application. Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP). In ping, there is no server that provides a service.

- **OSI Layers**

  SMTP is an **application** layer protocol used for e-mail transmission.
  TCP is a core **transport** layer protocol.
  BGP is a **network** layer protocol backing the core routing decisions on the Internet
  PPP is a **data link layer** protocol commonly used in establishing a direct connection between two networking nodes.

- In Ethernet when Manchester encoding is used, the bit rate is: **Half the baud rate**

- There are n stations in a slotted LAN. Each station attempts to transmit with a probability p in each time slot. What is the probability that ONLY one station transmits in a given time slot **$np(1-p)^{(n-1)}$**