ARPANET

The **Advanced Research Projects Agency Network** (**ARPANET**) was the first wide-area packet-switched network with distributed control and one of the first computer networks to implement the TCP/IP protocol suite. Both technologies became the technical foundation of the Internet. The ARPANET was established by the Advanced Research Projects Agency (ARPA) of the United States Department of Defense.

ASCII

ASCII abbreviated from **American Standard Code for Information Interchange**, is a character encoding standard for electronic communication. ASCII codes represent text in computers, telecommunications equipment, and other devices. Because of technical limitations of computer systems at the time it was invented, ASCII has just 128 code points, of which only 95 are printable characters, which severely limited its scope. Many computer systems instead use Unicode, which has millions of code points, but the first 128 of these are the same as the ASCII set.

Since it is a seven-bit code, it can at the most represent 128 characters. it currently defines 95 printable characters including 26 upper case letters (A to Z), 26 lower case letters, 10 numerals (0 to 9), and 33 special characters including mathematical symbols, punctuation marks and space characters. They represent text in, telecommunications equipment, and devices. These include numbers, upper and lowercase English letters, functions, punctuation symbols, and some other symbols. In total, there are 256 ASCII characters, and can be broadly divided into three categories:

1. **ASCII control characters (0-31 and 127)**
2. **ASCII printable characters (32-126) (most commonly referred to)**
3. **Extended ASCII characters (128-255)**

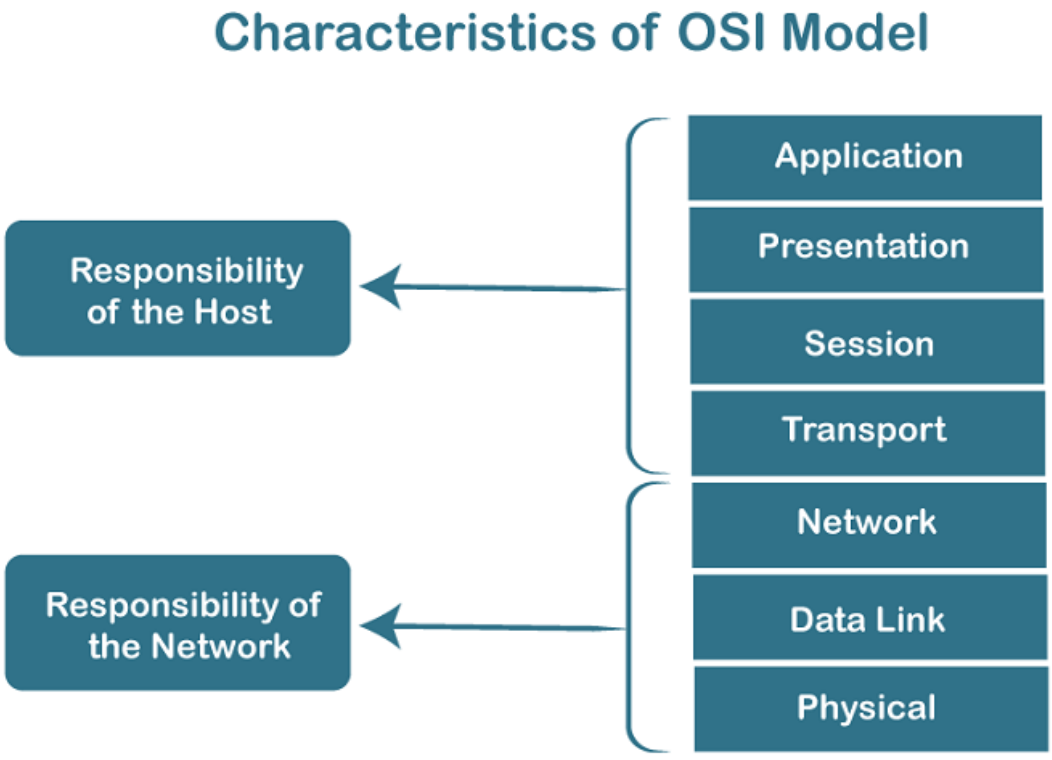
Unicode :

- Unicode provides a unique way to define every character in every spoken language of the world by assigning it a unique number. The Unicode standard is maintained by the Unicode Consortium and defines more than 1,40,000 characters from more than 150 modern and historic scripts along with emoji.
- Unicode can be defined with different character encoding like UTF-8, UTF-16, UTF-32, etc. Among these UTF-8 is the most popular as it used in over 90% of websites on the World Wide Web as well as on most modern Operating systems like Windows.

OSI Model

- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model:



- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is

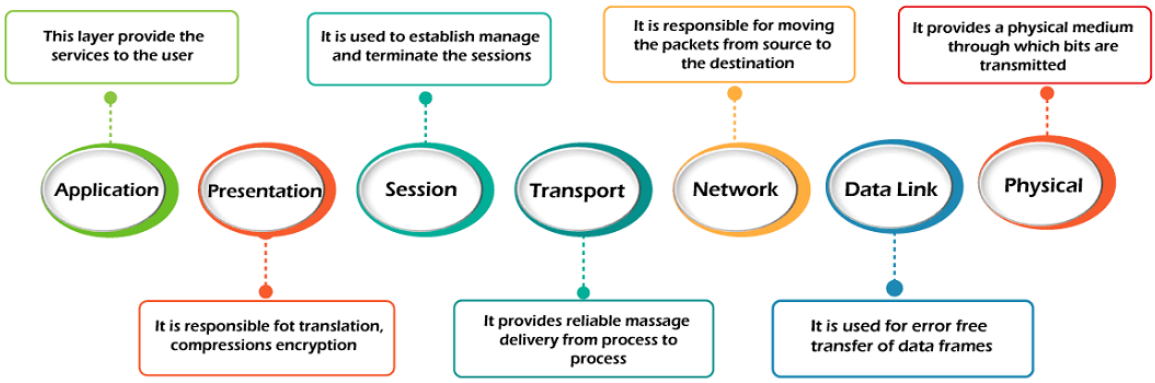
closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.

- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

7 Layers of OSI Model

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



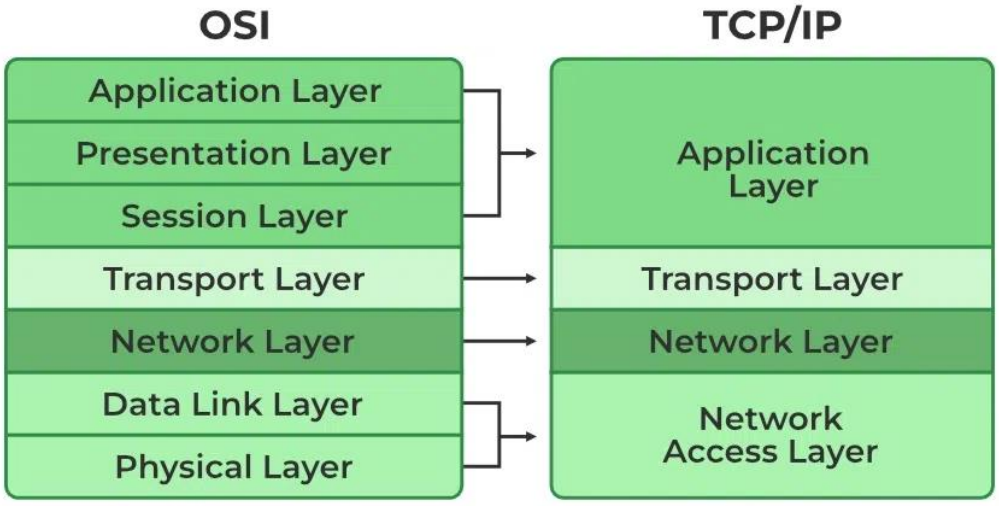
TCP/IP Model

TCP/IP was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model.

The number of layers is sometimes referred to as five or four. We'll study five layers. The Physical Layer and Data Link Layer are referred to as one single layer as the 'Physical Layer' or 'Network Interface Layer' in the 4-layer reference.
Layers of TCP/IP Model

1. Application Layer
2. Transport Layer(TCP/UDP)
3. Network/Internet Layer(IP)
4. Data Link Layer (MAC)
5. Physical Layer

The diagrammatic comparison of the **TCP/IP and OSI** model is as follows:



De facto and de jure

De facto and **de jure** are Latin expressions used in legal contexts to describe the nature of state government. The terms are closely related, but have different meanings:

- De facto describes practices that exist in reality, even though they are not officially recognized by laws.
- De jure describes practices that are legally recognized, regardless of whether the practice exists in reality.

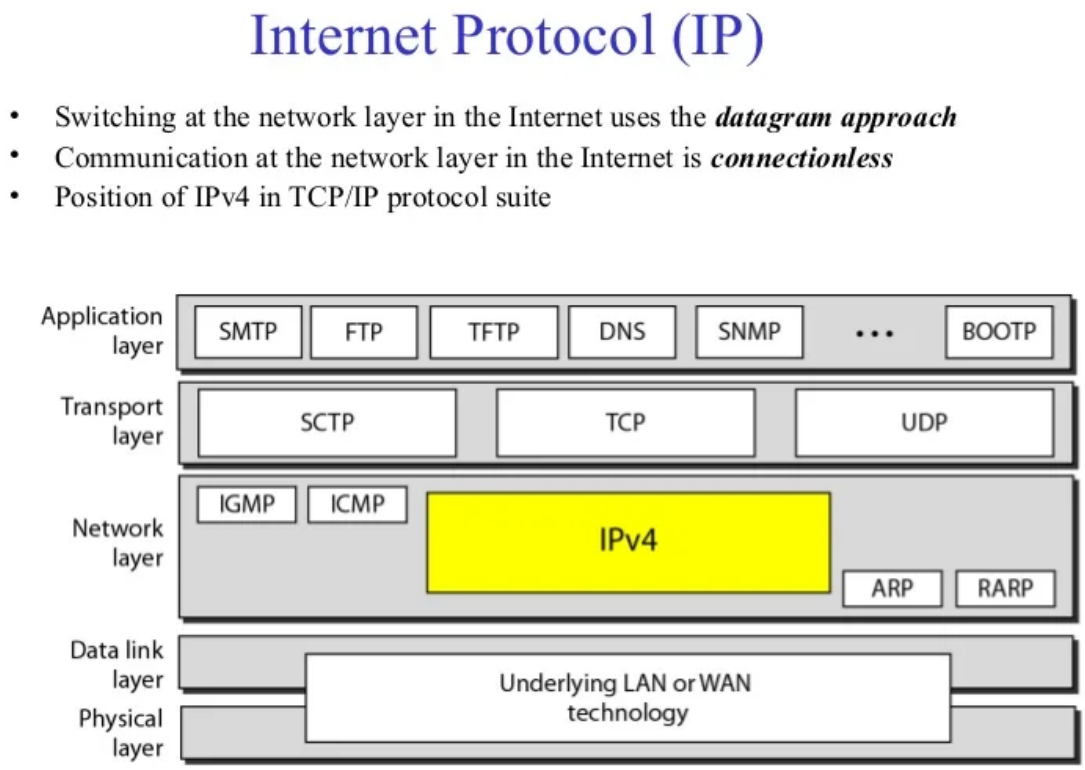
Standard creation committees

Standard creation committees are organizations that develop and publish standards in various fields. Some examples are:

- **ISO** (International Standards Organization)
- **ITU-T** (International Telecommunication Union - Telecommunication Standards Sector)
- **ANSI** (American National Standards Institute)
- **IEEE** (Institute of Electrical and Electronics Engineers)
- **EIA** (Electronic Industries Association)

Communication protocol

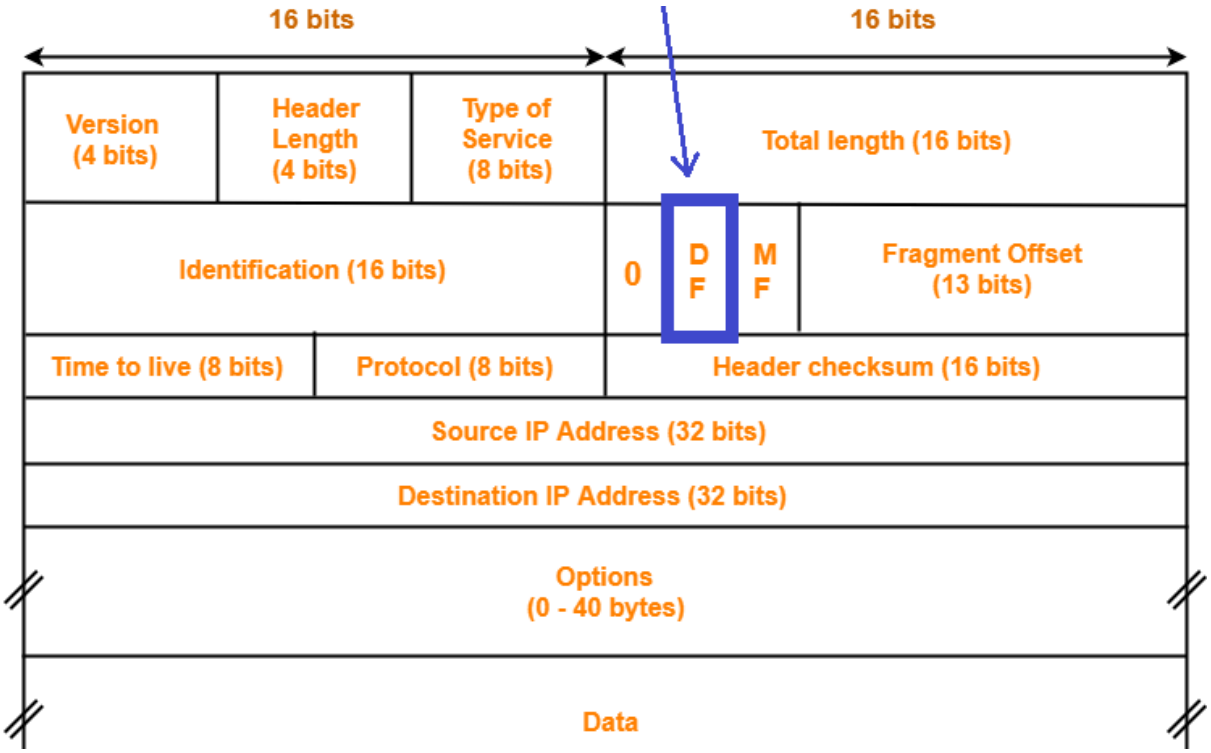
A **communication protocol** is a system of rules that allows two or more entities of a communications system to transmit information via any variation of a physical quantity. The protocol defines the rules, syntax, semantics,
and synchronization of communication and possible error recovery methods. Protocols may be implemented by hardware, software, or a combination of both.



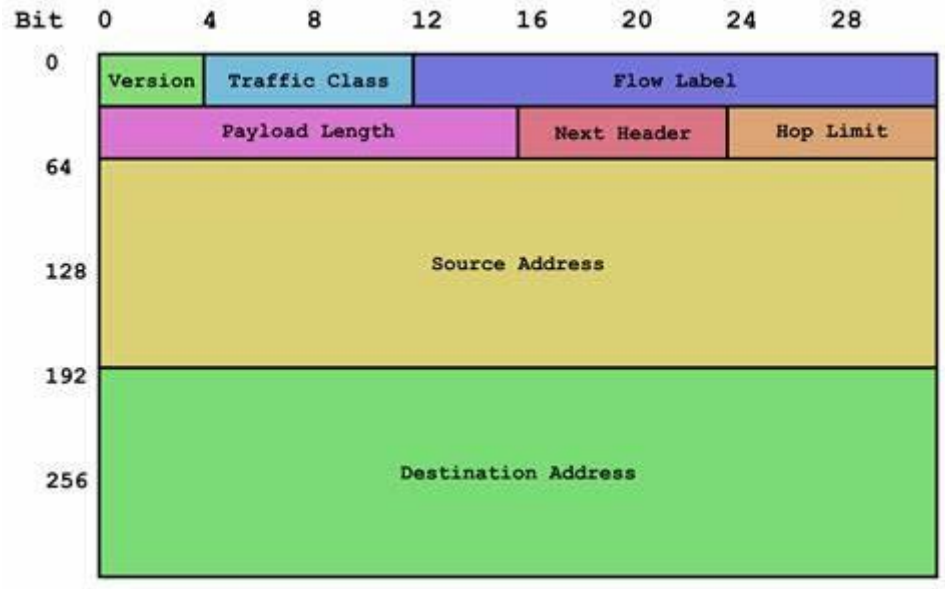
IP Header:

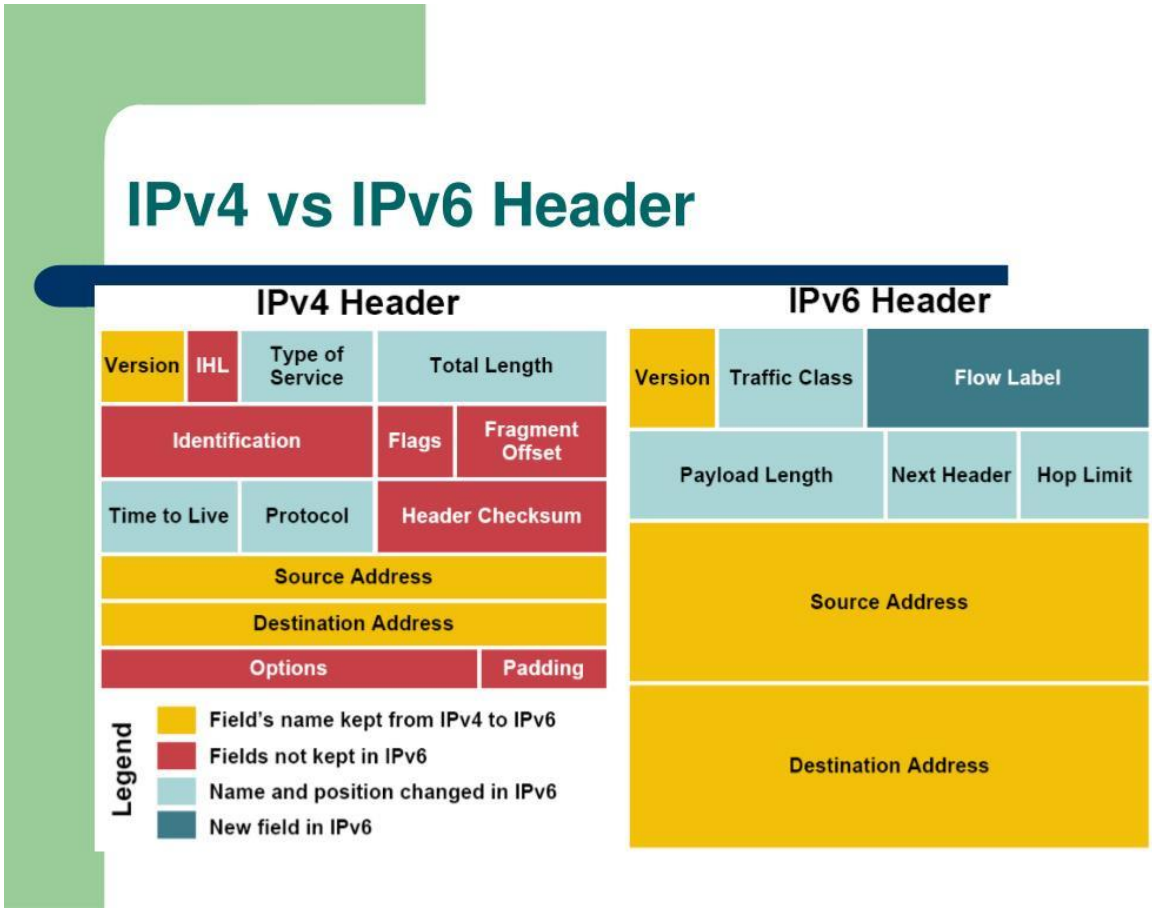
An **IP header** is header information at the beginning of an Internet Protocol (IP) packet. An IP packet is the smallest message entity exchanged via the Internet Protocol across an IP network. IP packets consist of a header for addressing and routing, and a payload for user data. The header contains information about IP version, source IP address, destination IP address, time-to-live, etc. The payload of an IP packet is typically a datagram or segment of the higher-level transport layer protocol, but may be data for an internet layer (e.g., ICMP or ICMPv6) or link layer (e.g., OSPF) instead.

IPv4:

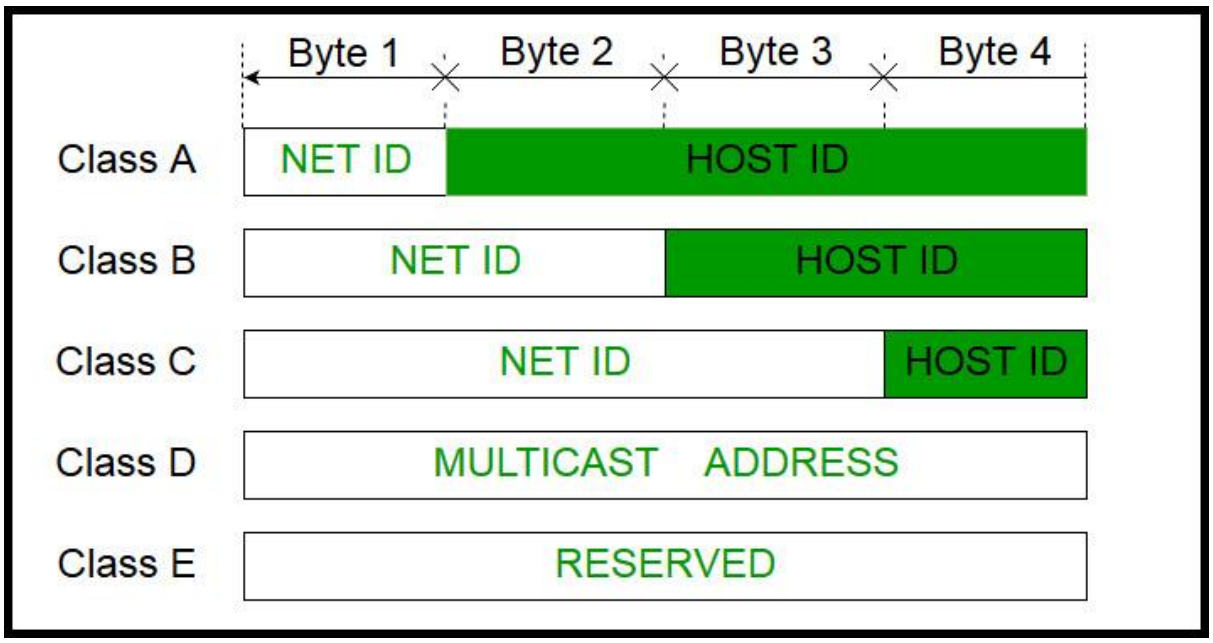

16 bits
16 bits
Version (4 bits)
Header Length (4 bits)
Type of Service (8 bits)
Total length (16 bits)
Identification (16 bits)
0
D F
M F
Fragment Offset (13 bits)
Time to live (8 bits)
Protocol (8 bits)
Header checksum (16 bits)
Source IP Address (32 bits)
Destination IP Address (32 bits)
Options (0 - 40 bytes)
Data

IPv6:


Bit 0 4 8 12 16 20 24 28
0
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
64
Source Address
128
192
Destination Address
256



Classful IP Addressing

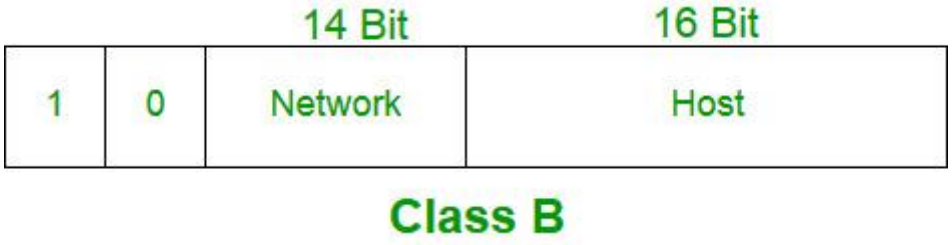


Class A

IP addresses belonging to class A ranges from 1.x.x.x – 126.x.x.x

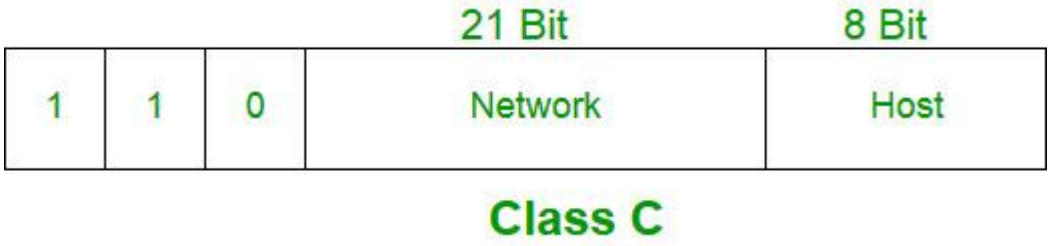
Class B

IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.



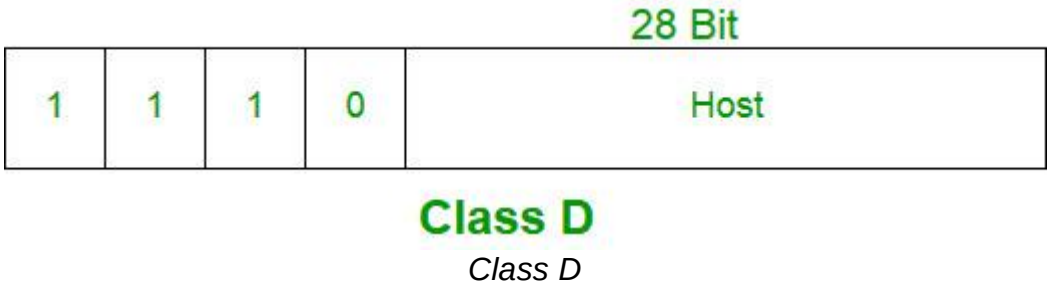
Class C

IP addresses belonging to class C range from 192.0.0.x – 223.255.255.x.



Class D

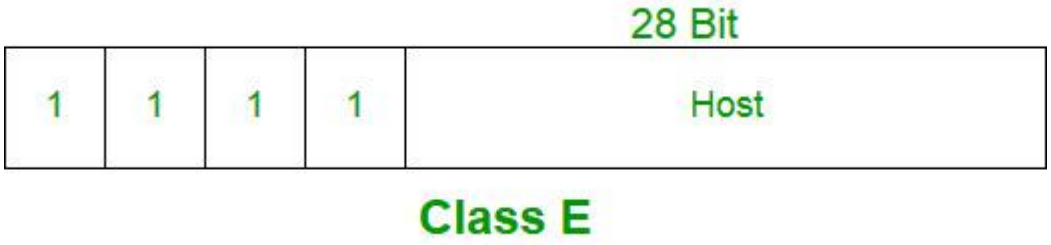
Class D does not possess any subnet mask. IP addresses belonging to class D range from 224.0.0.0 – 239.255.255.255.



Class D

Class E

IP addresses of class E range from 240.0.0.0 – 255.255.255.254. This class doesn't have any subnet mask. The higher-order bits of the first octet of class E are always set to 1111.



Range of Special IP Addresses

169.254.0.0 – 169.254.0.16 : Link-local addresses
127.0.0.0 – 127.0.0.8 : Loop-back addresses
0.0.0.0 – 0.0.0.8: used to communicate within the current network.

Subnet Mask

Suppose we have a Class A network that means we have 16 million hosts in a network. The task we have to do is:

1. Maintenance of such a huge network
2. Security for the network – For example, we have 4 departments in a company and all of the 4 departments need not access the whole network.

For this we need subnetting i.e., dividing a huge network into smaller network. Now every department will have their own network .

In case of addressing without subnetting, the process of reaching an address is done by 3 steps –

1. Identification of the network
2. Identification of the host
3. Identification of the process

In case of addressing with subnetting, the process of reaching an address is done by 4 steps –

1. Identification of the network
2. Identification of the subnet
3. Identification of the host
4. Identification of the process

A packet is received which has destination address -200.1.2.20 . Then how the router will identify that which subnet it belongs to . It'll be done using *Subnet Mask*. A **subnet mask** is a 32-bit number which is used to identify the subnet of an IP address. The subnet mask is combination of 1's and 0's. 1's represents network and subnet ID while 0's
represents the host ID. For this case, subnet mask is,

11111111.11111111.11111111.11000000

or

255.255.255.192

So in order to get the network which the destination address belongs to we have to **bitwise &** with subnet mask.

11111111.11111111.11111111.11000000

&& 11001000.00000001.00000010.00010100

11001000.00000001.00000010.00000000

The address belongs to,

11001000.00000001.00000010.00000000

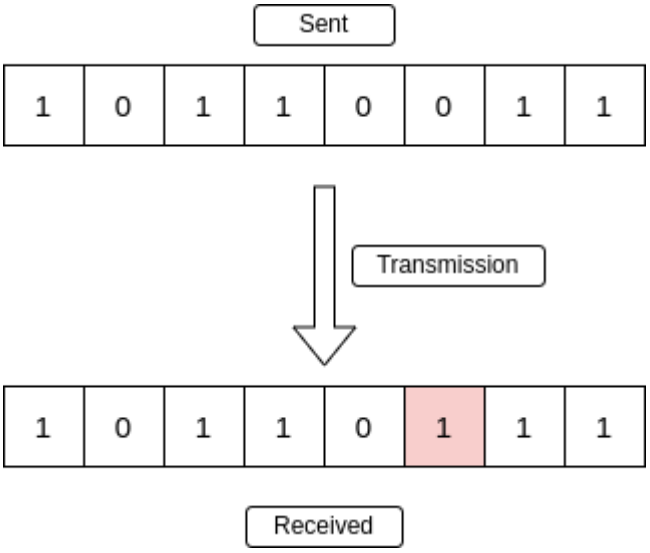
or

200.1.2.0

Error Detection in Computer Networks

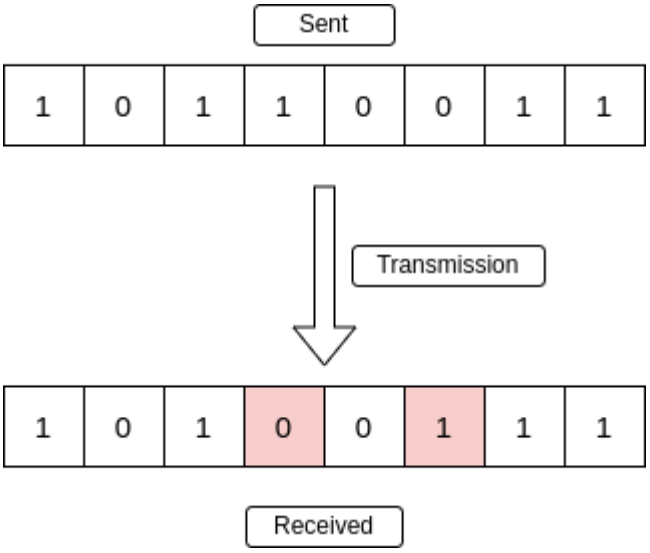
Types of Errors

Single-Bit Error



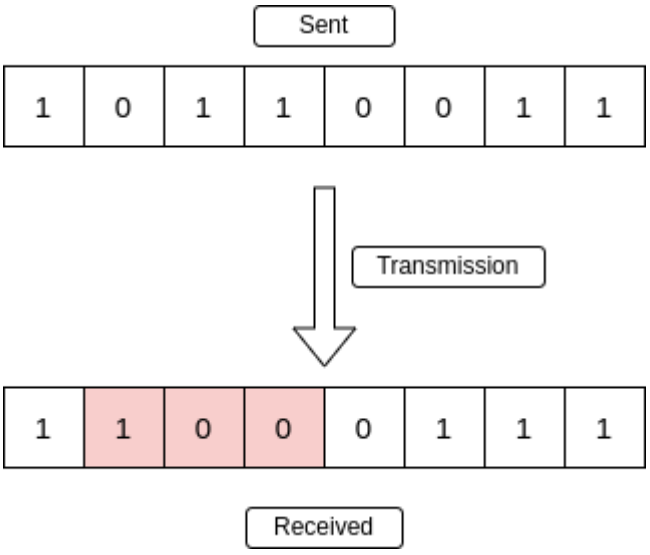
Single-Bit Error

Multiple-Bit Error



Multiple-Bit Error

Burst Error



Burst Error

Error Detection Methods

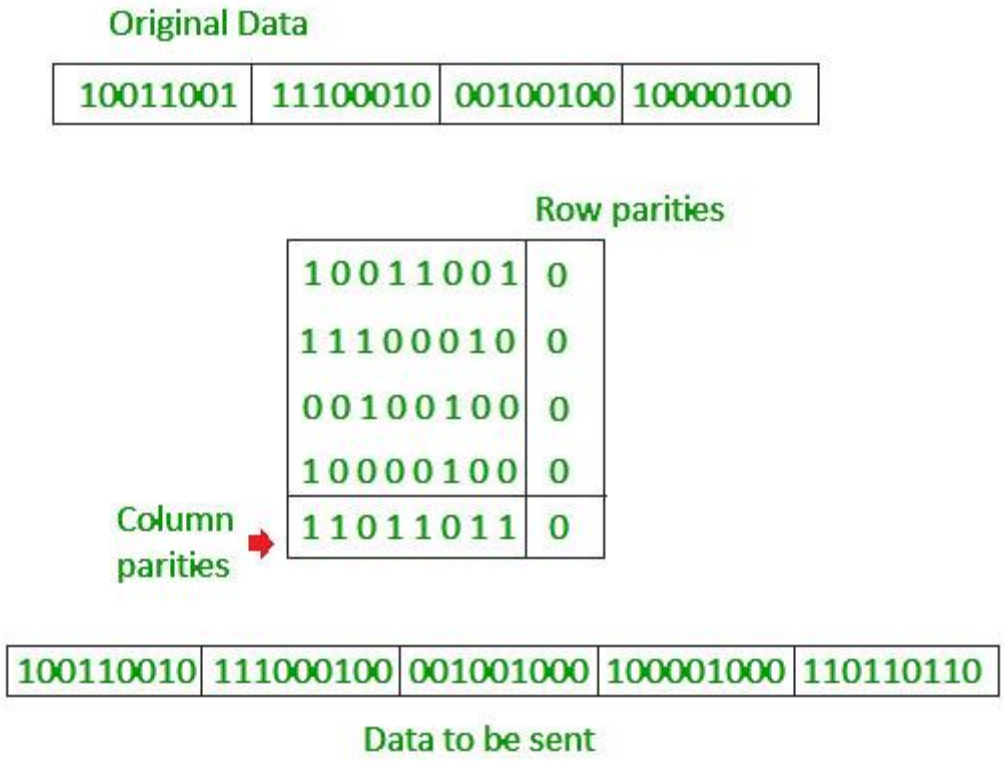
Simple Parity Check

Simple-bit parity is a simple error detection method that involves adding an extra bit to a data transmission. It works as:

- 1 is added to the block if it contains an odd number of 1's, and
- 0 is added if it contains an even number of 1's

Two-dimensional Parity Check

Two-dimensional Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end, these are compared with the parity bits calculated on the received data.



Checksum

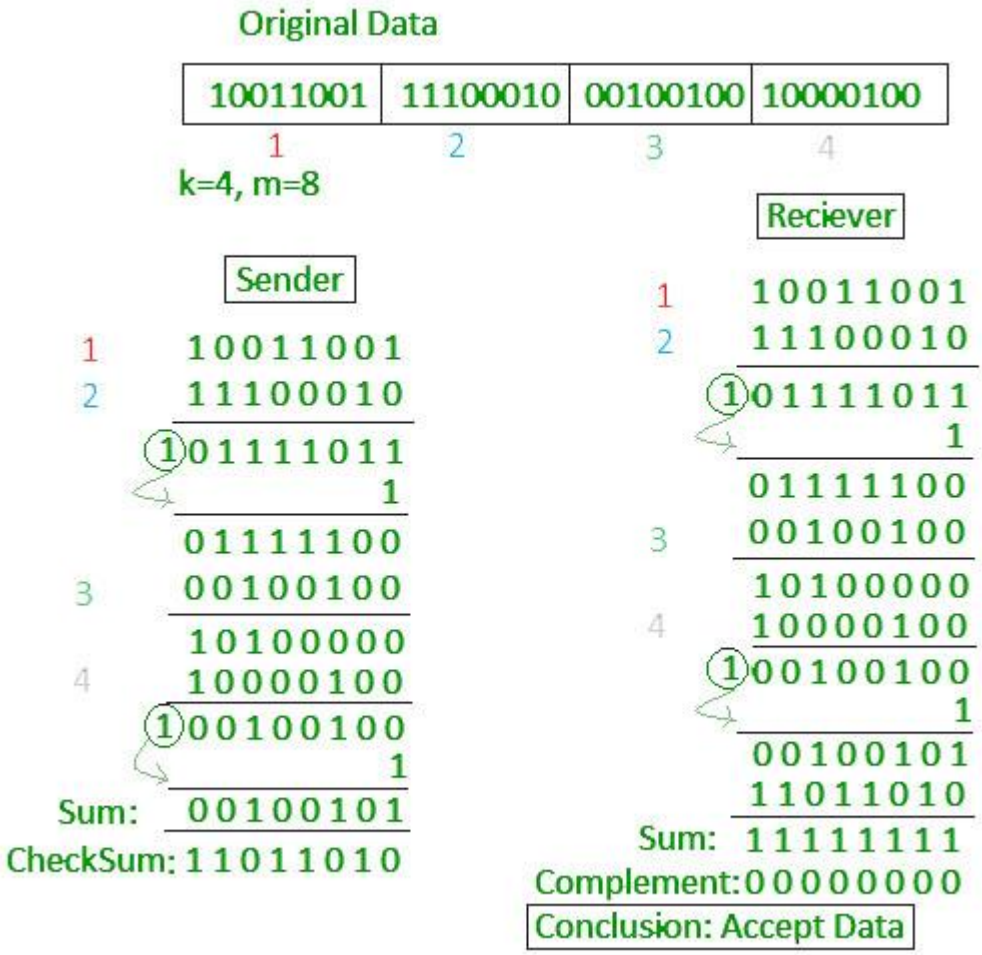
Checksum error detection is a method used to identify errors in transmitted data. The process involves dividing the data into equally sized segments and using a 1's complement to calculate the sum of these segments. The calculated sum is then sent along with the data to the receiver. At the receiver's end, the same process is repeated and if all zeroes are obtained in the sum, it means that the data is correct.

Checksum – Operation at Sender's Side

- Firstly, the data is divided into k segments each of m bits.
- On 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.

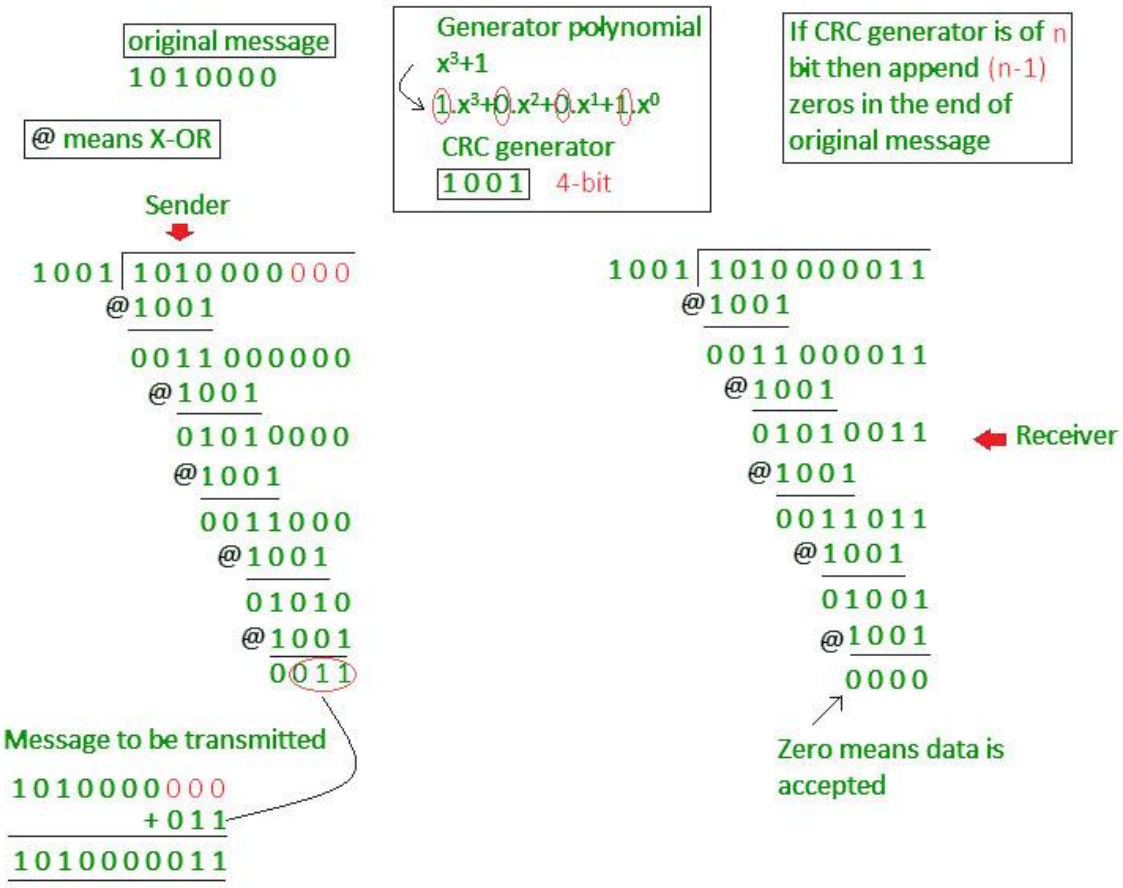
Checksum – Operation at Receiver's Side

- 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.



Cyclic Redundancy Check (CRC)

- Unlike the 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 the 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.



Error Correction

Error Correction codes are used to detect and correct the errors when data is transmitted from the sender to the receiver.

Error Correction can be handled in two ways:

- **Backward error correction:** Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.
- **Forward error correction:** In this case, the receiver uses the error-correcting code which automatically corrects the errors.

Hamming Code

Hamming code is a set of error-correction codes that can be used to **detect and correct the errors** that can occur when the data is moved or stored from the sender to the receiver.

Redundant bits – Redundant bits are extra binary bits that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer.

The number of redundant bits can be calculated using the following formula:

$2^r \geq m + r + 1$

where, r = redundant bit, m = data bit

Suppose the number of data bits is 7, then the number of redundant bits can be calculated using: = $2^4 \geq 7 + 4 + 1$ Thus, the number of redundant bits= 4 **Parity bits**

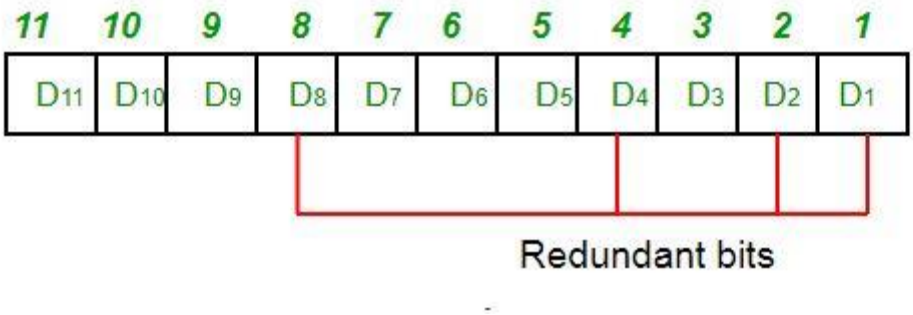
Position	R8	R4	R2	R1
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
10	1	0	1	0
11	1	0	1	1

R1 -> 1,3,5,7,9,11
R2 -> 2,3,6,7,10,11
R3 -> 4,5,6,7
R4 -> 8,9,10,11

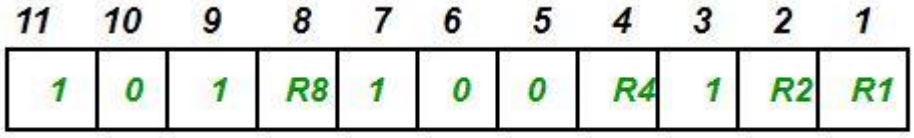
Determining the position of redundant bits – These redundancy bits are placed at positions that correspond to the power of 2.
As in the above example:

- The number of data bits = 7
- The number of redundant bits = 4

- The total number of bits = 11
- The redundant bits are placed at positions corresponding to power of 2 - 1, 2, 4, and 8



- Suppose the data to be transmitted is 1011001, the bits will be placed as follows:



R1: bits 1, 3, 5, 7, 9, 11

- To find the redundant bit R1, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R1 is an even number the value of R1 (parity bit's value) = 0

R2: bits 2,3,6,7,10,11

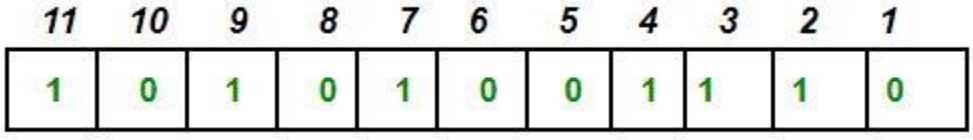
- To find the redundant bit R2, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R2 is odd the value of R2(parity bit's value)=1

R4: bits 4, 5, 6, 7

- To find the redundant bit R4, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R4 is odd the value of R4(parity bit's value) = 1

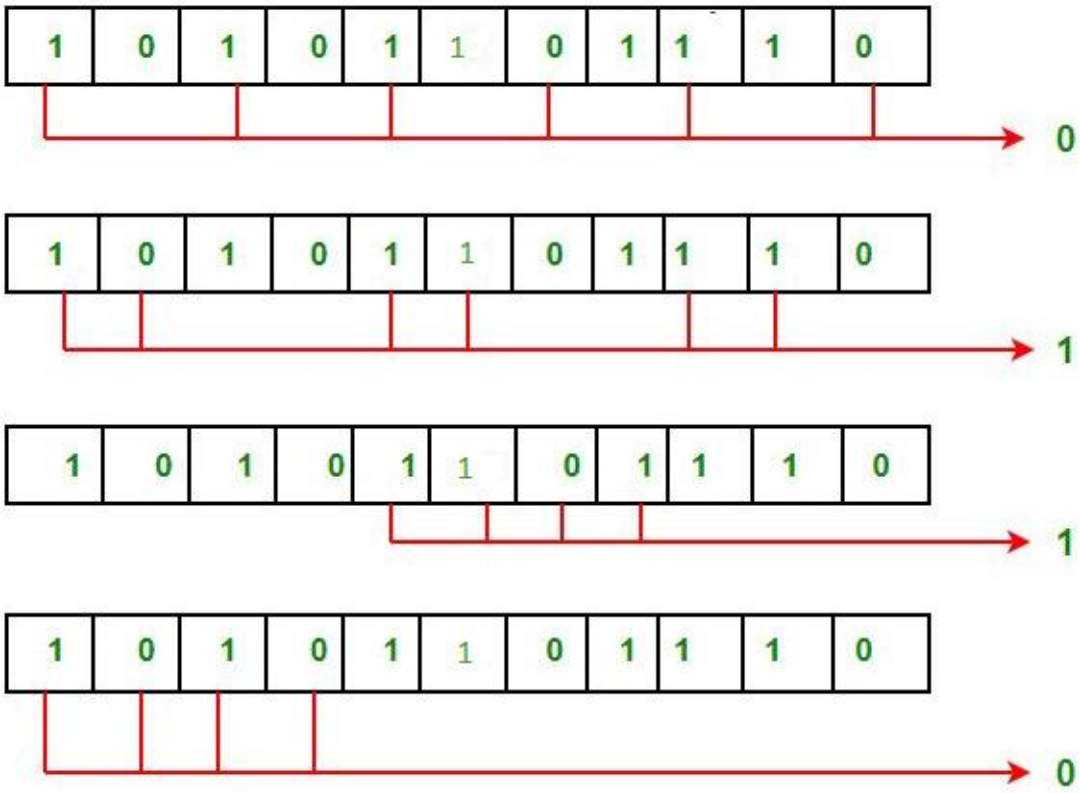
R8: bit 8,9,10,11

- To find the redundant bit R8, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R8 is an even number the value of R8(parity bit's value)=0.



Error detection and correction:

Suppose in the above example the 6th bit is changed from 0 to 1 during data transmission, then it gives new parity values in the binary number:



For all the parity bits we will check the number of 1's in their respective bit positions.

For R1: bits 1, 3, 5, 7, 9, 11. We can see that the number of 1's in these bit positions are 4 and that's even so we get a 0 for this.

For R2: bits 2,3,6,7,10,11 . We can see that the number of 1's in these bit positions are 5 and that's odd so we get a 1 for this.

For R4: bits 4, 5, 6, 7 . We can see that the number of 1's in these bit positions are 3 and that's odd so we get a 1 for this.

For R8: bit 8,9,10,11 . We can see that the number of 1's in these bit positions are 2 and that's even so we get a 0 for this.

The bits give the binary number 0110 whose decimal representation is 6. Thus, bit 6 contains an error. To correct the error the 6th bit is changed from 1 to 0.

Cable Type -Data Transfer-Max Dist

Cable Type	Data Transfer Rate	Maximum Distance
Ethernet	Up to 10 Gbps	Up to 100 m
Fiber Optic	Up to 100 Gbps	Up to 40 km
HDMI	Up to 48 Gbps	Up to 30 m
DVI	Up to 9.9 Gbps	Up to 15 m
CAT6	Up to 10 Gbps	Up to 100 m
CAT7	Up to 10 Gbps	Up to 100 m
CAT8	Up to 40 Gbps	Up to 30 m
RS485	Up to 10 Mbps	Up to 1200 m
CAT5 Twisted Pair	10-100 Mbps	Up to 100 m
Thin-net-Coax	10-100 Mbps	Up to 200 m
Multimode Fiber	100 Mbps	2 Km
Single-mode fiber	01-10 Gbps	40 Km

scale regarding storage capacity up to a yottabyte:

1. Bit (the smallest common measurement in computing)
2. Byte (eight bits)
3. Kilobyte (1024 bytes)
4. Megabyte (1024 Kilobytes)
5. Gigabyte (1024 Megabytes)
6. Terabyte (1024 Gigabytes)
7. Petabyte (1024 Terabytes)
8. Exabyte (1024 Petabytes)
9. Zettabyte (1024 Exabytes)
10. Yottabyte (1024 Zettabytes)

Some Host Facts:

1	Host to Host Layer	Application, Presentation, Transport, Session
2	Media Layer	Physical, Data Link, N/W Layer
3	Decomposition of Layer	Done in Data Link Layer
4	Point to Point connectivity	Done in Data Link Layer
5	Host to Host connectivity	Done in N/W Layer
6	End to End connectivity	Done in Transport Layer

TCP Flags List

Flag	Meaning
SYN	Packets that are used to initiate a connection.
ACK	Packets that are used to confirm that the data packets have been received, also used to confirm the initiation request and tear down requests
RST	Signify the connection is down or maybe the service is not accepting the requests
FIN	Indicate that the connection is being torn down. Both the sender and receiver send the FIN packets to gracefully terminate the connection
PSH	Indicate that the incoming data should be passed on directly to the application instead of getting buffered
URG	Indicate that the data that the packet is carrying should be processed immediately by the TCP stack. It can be used to provide out-of-band data transfer, such as signaling that a message is urgent and should be delivered before other data.

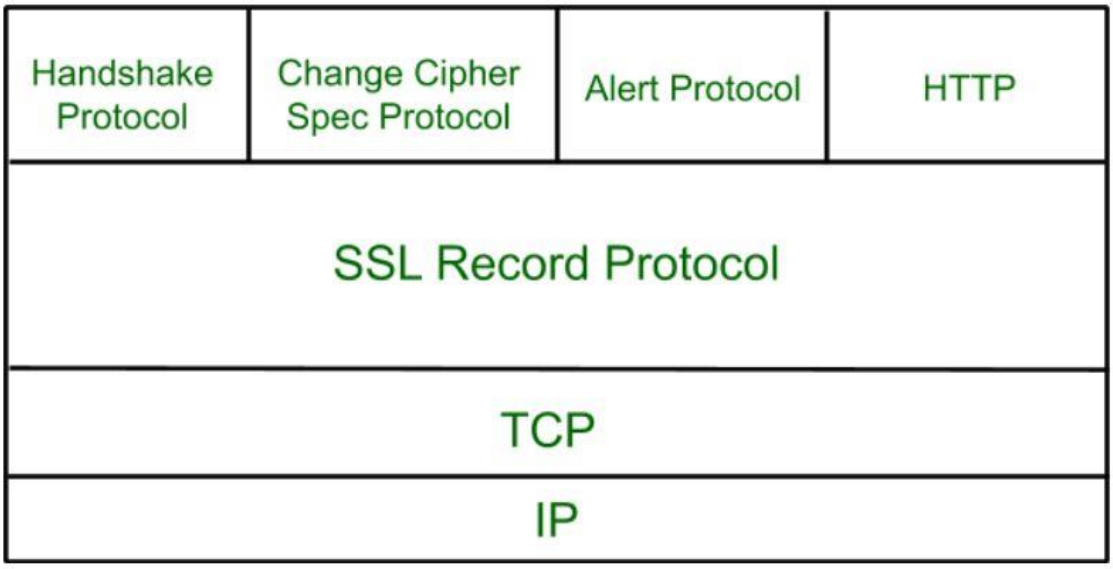
Secure Socket Layer (SSL)

Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

SSL Protocol Stack:



Network Devices & Layers:

Devices	**Layers**
Repeater	Physical Layer
Hub	Physical Layer
Bridge	Data Link Layer
Switch	Data Link Layer
Router	Network Layer
Gateway	Logical Gateway- N/W Layer Physical Gateway- Data Link Layer (MAC)

Network Threat

A network threat is when an attacker targets a computer network or the computers and devices connected to it. Network threats can cause significant damage to data, systems, and networks and lead to downtime or even complete system failure.

There are many different types of network threats, but some of the most common include:

- **Denial-of-Service (DoS) Attacks:** A DoS attack is an attempt to make a computer or network resource unavailable to users. They can be carried out using various methods, including flooding the target with requests or traffic or exploiting vulnerabilities in the network or system.
- **Distributed Denial-of-Service (DDoS) Attacks:** A DDoS attack is similar to a DoS attack, but multiple computers or devices, known as zombies, are used to carry out the attack. A large number of requests or traffic from the zombies can overwhelm the target, thus denying access to legitimate users.
- **Malware:** Malware or malicious software refers to any type of software that is designed to damage or disrupt a computer system. Viruses, worms, and Trojans are some examples of malware.
- **Phishing:** Phishing is a type of social engineering attack that attempts to trick users into revealing sensitive information, like passwords or credit card numbers. Such attacks are often carried out by email and may include links to fake websites that look identical to the real website.

Types of active attacks are as follows:

- Masquerade
- Modification of messages
- Repudiation
- Replay
- Denial of Service

Masquerade –
Masquerade is a type of cybersecurity attack in which an attacker pretends to be someone else in order to gain access to systems or data. This can involve impersonating a legitimate user or system to trick other users or systems into providing sensitive information or granting access to restricted areas.

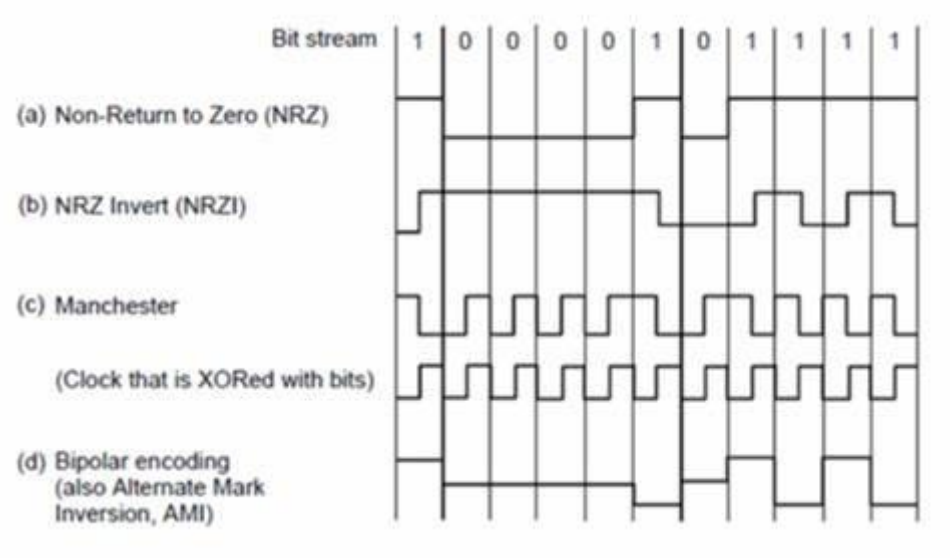
Modification of messages –
It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect.

Repudiation –
Repudiation attacks are a type of cybersecurity attack in which an attacker attempts to deny or repudiate actions that they have taken, such as making a transaction or sending a message. These attacks can be a serious problem because they can make it difficult to track down the source of the attack or determine who is responsible for a particular action.

Replay –
It involves the passive capture of a message and its subsequent transmission to produce an authorized effect. In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network and later on use this data for personal uses.

Physical Layer

Bit Stream Encoding



Multiplexing in Data Communications

Multiplexing is the sharing of a medium or bandwidth. It is the process in which multiple signals coming from multiple sources are combined and transmitted over a single communication/physical line.

Types of Multiplexing

There are Five types of Multiplexing :

1. Frequency Division Multiplexing (FDM)
2. Time-Division Multiplexing (TDM)
3. Wavelength Division Multiplexing (WDM)
4. Code-division multiplexing (CDM)
5. Space-division multiplexing (SDM)

Gray Code Table

Decimal	Hex	Binary	Gray Code
0	0	0000	0000
1	1	0001	0001
2	2	0010	0011
3	3	0011	0010
4	4	0100	0110
5	5	0101	0111
6	6	0110	0101
7	7	0111	0100
8	8	1000	1100
9	9	1001	1101
10	a	1010	1111
11	b	1011	1110
12	c	1100	1010
13	d	1101	1011
14	e	1110	1001
15	f	1111	1000

16-QAM and 64-QAM

16-QAM and 64-QAM are types of **Quadrature Amplitude Modulation (QAM)**, which is a technique that modulates both the phase and amplitude of a carrier signal to transmit data. The number indicates how many different symbols or states the QAM system can generate. For example, 16-QAM can generate 16 different symbols, each carrying 4 bits of information. 64-QAM can generate 64 different symbols, each carrying 6 bits of information. Higher QAM schemes can achieve higher data rates, but they also require higher signal-to-noise ratios to avoid errors. QAM is widely used for digital television, cable and wireless communications.

Interrupt request (or **IRQ**)

In a computer, an **interrupt request** (or **IRQ**) is a hardware signal sent to the processor that temporarily stops a running program and allows a special program, an interrupt handler, to run instead. Hardware interrupts are used to handle events

such as receiving data from a modem or network card, key presses, or mouse movements.

IRQs

Master PIC

- IRQ 0 – system timer (cannot be changed)
- IRQ 1 – keyboard on PS/2 port (cannot be changed)
- IRQ 2 – cascaded signals from IRQs 8–15 (any devices configured to use IRQ 2 will actually be using IRQ 9)
- IRQ 3 – serial port controller for serial port 2 (shared with serial port 4, if present)
- IRQ 4 – serial port controller for serial port 1 (shared with serial port 3, if present)
- IRQ 5 – parallel port 3 or sound card
- IRQ 6 – floppy disk controller
- IRQ 7 – parallel port 1 (shared with parallel port 2, if present). It is used for printers or for any parallel port if a printer is not present. It can also be potentially be shared with a secondary sound card with careful management of the port.

Slave PIC

- IRQ 8 – real-time clock (RTC)
- IRQ 9 – Advanced Configuration and Power Interface (ACPI) system control interrupt on Intel chipsets.[3] Other chipset manufacturers might use another interrupt for this purpose, or make it available for the use of peripherals (any devices configured to use IRQ 2 will actually be using IRQ 9)
- IRQ 10 – The Interrupt is left open for the use of peripherals (open interrupt/available, SCSI or NIC)
- IRQ 11 – The Interrupt is left open for the use of peripherals (open interrupt/available, SCSI or NIC)
- IRQ 12 – mouse on PS/2 port
- IRQ 13 – CPU co-processor or integrated floating point unit or inter-processor interrupt (use depends on OS)
- IRQ 14 – primary ATA channel (ATA interface usually serves hard disk drives and CD drives)
- IRQ 15 – secondary ATA channel

The public switched telephone network (PSTN)

The public switched telephone network (PSTN) is the aggregate of the world's telephone networks that are operated by national, regional, or local telephony operators. It provides infrastructure and services for

public telecommunication. The network consists of telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables interconnected by switching centers, such as central offices, network tandems, and international gateways, which allow telephone users to communicate with each other.

Digital subscriber line

Digital subscriber line (**DSL**; originally **digital subscriber loop**) is a family of technologies that are used to transmit digital data over telephone lines. In telecommunications marketing, the term DSL is widely understood to mean asymmetric digital subscriber line (ADSL), the most commonly installed DSL technology, for Internet access.

Synchronous optical networking

Synchronous Optical Networking (**SONET**) and **Synchronous Digital Hierarchy** (**SDH**) are standardized protocols that transfer multiple digital bit streams synchronously over optical fiber using lasers or highly coherent light from light-emitting diodes (LEDs). At low transmission rates data can also be transferred via an electrical interface. The method was developed to replace the plesiochronous digital hierarchy (PDH) system for transporting large amounts of telephone calls and data traffic over the same fiber without the problems of synchronization.

Wavelength-division multiplexing

In fiber-optic communications, **wavelength-division multiplexing** (**WDM**) is a technology which multiplexes a number of optical carrier signals onto a single optical fiber by using different wavelengths (i.e., colors) of laser light.[1] This technique enables bidirectional communications over a single strand of fiber, also called **wavelength-division duplexing**, as well as multiplication of capacity.

Cell phone generation refers to the different stages of wireless cellular technology[1].The main cell phone generations are:

- 1G: The first generation of analog voice communication.
- 2G/2.5G: The second generation of digital voice and data transmission, such as GSM, CDMA, GPRS, EDGE, and IS95-B.
- 3G: The third generation of high-speed data and multimedia services, such as WCDMA, HSDPA, and CDMA2000.

- 4G: The fourth generation of broadband mobile internet, such as LTE, WiMAX, and HSPA+.
- 5G: The latest generation of ultra-fast and low-latency wireless connectivity, using various frequency bands.

Data Link Layer

Error Correcting Code:

1. Hamming codes
2. Binary convolutional codes
3. Reed Solomon code
4. Low Density Parity check codes

Error Detection code:

1. Parity
2. Checksum
3. Cyclic Redundancy Check (CRCs)

**Some of the Data-Link layer process run on dedicated H/W called a NIC (Network Interface Card)

Protocol:

1. **Simplex Stop & Wait**
2. **Sliding window protocols**

The primitives of stop and wait protocol are:

Sender side

Rule 1: Sender sends one data packet at a time.

Rule 2: Sender sends the next packet only when it receives the acknowledgment of the previous packet.

Therefore, the idea of stop and wait protocol in the sender's side is very simple, i.e., send one packet at a time, and do not send another packet before receiving the acknowledgment.

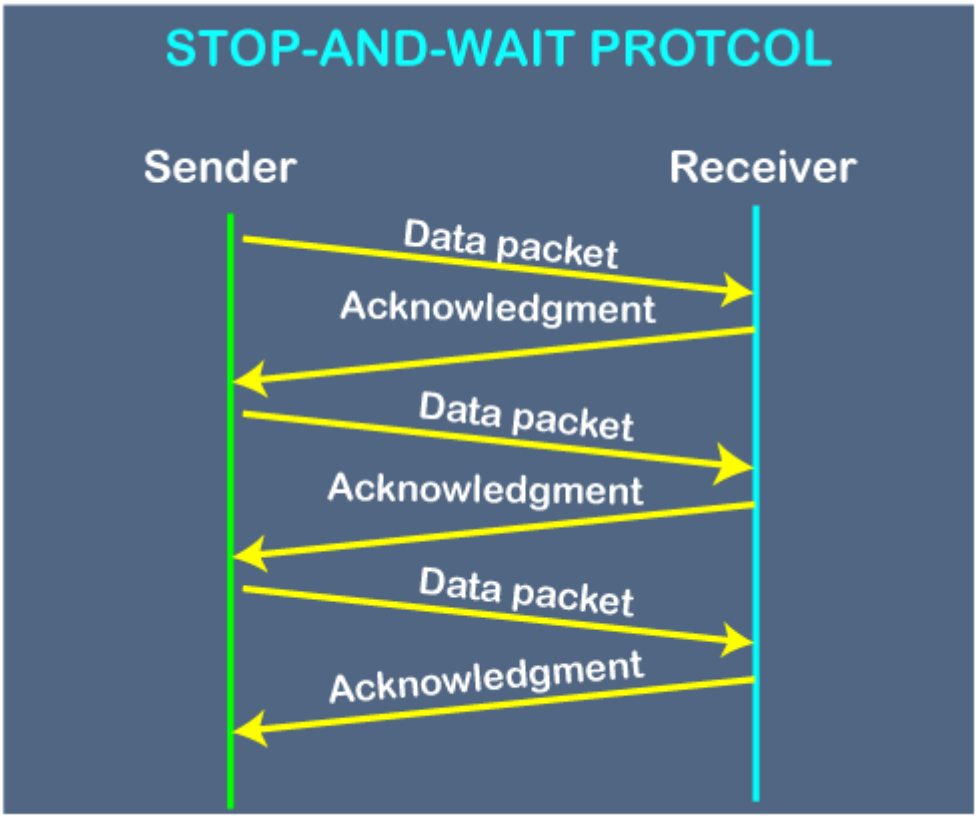
Receiver side

Rule 1: Receive and then consume the data packet.

Rule 2: When the data packet is consumed, receiver sends the acknowledgment to the sender.

Therefore, the idea of stop and wait protocol in the receiver's side is also very simple, i.e., consume the packet, and once the packet is consumed, the acknowledgment is sent. This is known as a flow control mechanism.

Working of Stop and Wait protocol



Sliding Window Protocol

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

Types of Sliding Window Protocol

Sliding window protocol has two types:

1. Go-Back-N ARQ
2. Selective Repeat ARQ

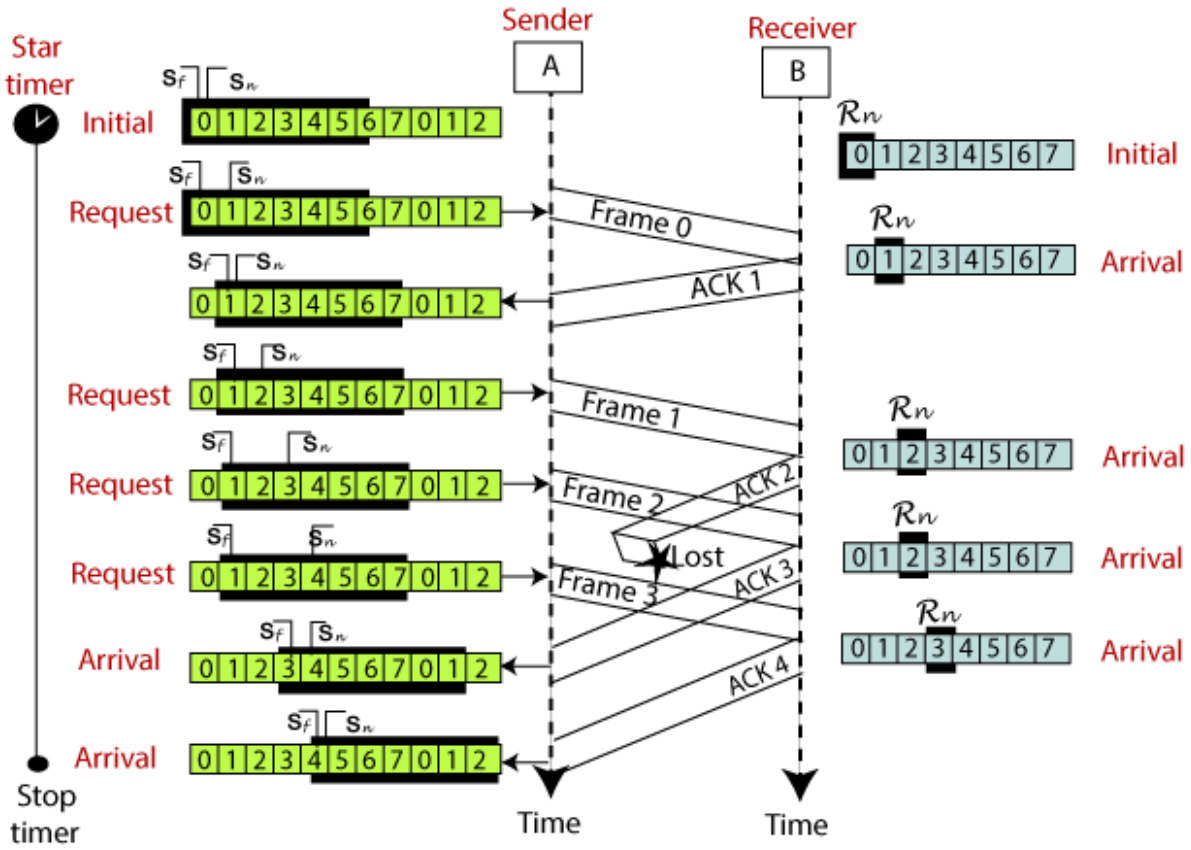
Go-Back-N ARQ
Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method.

Go-Back-N ARQ

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

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

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



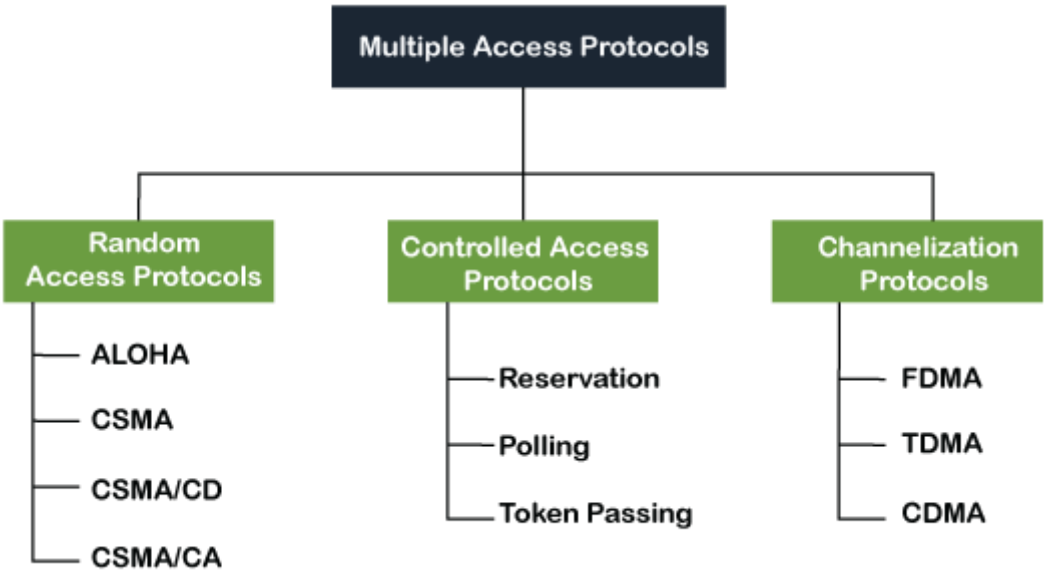
Multi access protocols (MACs)

Multi access protocols are a set of protocols that allow multiple nodes or users to access a shared network channel without interference. There are different types of multi access protocols, such as random access, controlled access, and channelization. Some examples of multi access protocols are ALOHA, CSMA, CSMA/CA, CSMA/CD, FDMA, TDMA, and CDMA.

The data link layer is used in a computer network to transmit the data between two devices or nodes. It divides the layer into parts such as **data link control** and the **multiple access resolution/protocol**. The upper layer has the responsibility to flow control and the error

control in the data link layer, and hence it is termed as **logical of data link control**.
Whereas the lower sub-layer is used to handle and reduce the collision or multiple access on a channel. Hence it is termed as **media access control** or the multiple access resolutions.

Following are the types of multiple access protocol that is subdivided into the different process as:



CSMA (Carrier Sense Multiple Access)

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

CSMA/ CD

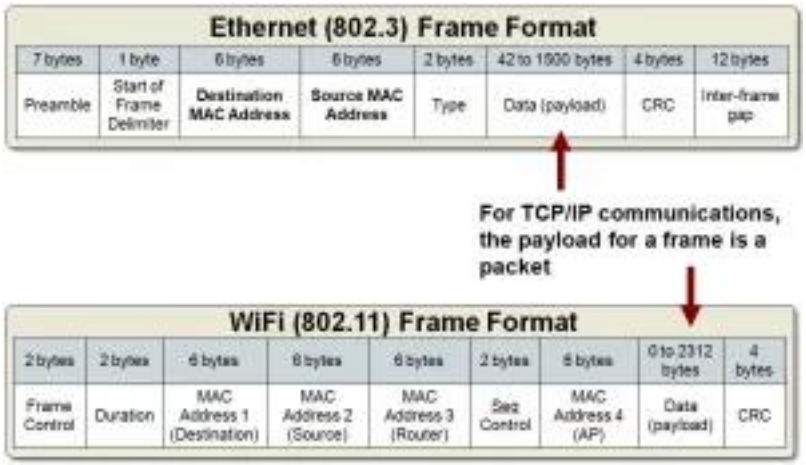
It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check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

CSMA/ CA

It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own)

acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

Ethernet



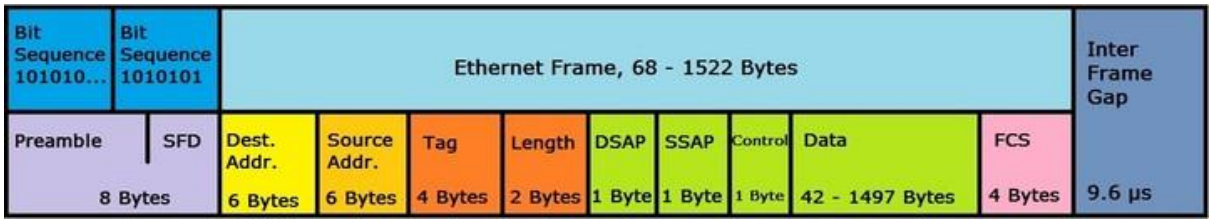
Ethernet (IEEE 802.3) Frame Format:

PREAMBLE	SFD	DESTINATION ADDRESS	SOURCE ADDRESS	LENGTH	DATA	CRC
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 - 1500 Bytes	4 Bytes

IEEE 802.3 ETHERNET Frame Format

1. **PREAMBLE –** Ethernet frame starts with a 7-Bytes Preamble. This is a pattern of alternative 0's and 1's which indicates starting of the frame and allow sender and receiver to establish bit synchronization. Initially, PRE (Preamble) was introduced to allow
2. for the loss of a few bits due to signal delays. But today's high-speed Ethernet doesn't need Preamble to protect the frame bits. PRE (Preamble) indicates the receiver that frame is coming and allow the receiver to lock onto the data stream before the actual frame begins.
3. **Start of frame delimiter (SFD) –** This is a 1-Byte field that is always set to 10101011. SFD indicates that upcoming bits are starting the frame, which is the destination address. Sometimes SFD is considered part of PRE, this is the reason Preamble is described as 8 Bytes in many places. The SFD warns station or stations that this is the last chance for synchronization.

802.3 Frame Format



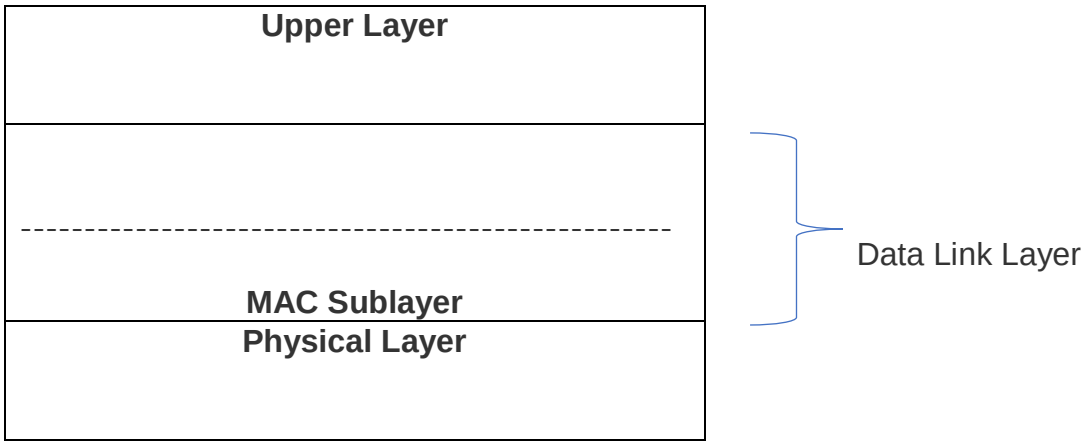
Wireless LAN (802.11):

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

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

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

802.11 standard uses the Ethernet protocol and CSMA/CA.



Components in Wireless LAN architecture as per IEEE standards are as follows:

1. Stations: Stations consist of all the equipment that is used to connect all wireless LANs. Each station has a wireless network controller.
2. Base Service Set (BSS): It is a group of stations communicating at the physical layer.
3. Extended Service Set (ESS): It is a group of connected Base Service Set (BSS).
4. Distribution Service (DS): It connects all Extended Service Set (ESS).

Network Layer

(Host to Host)

Connectionless Service --→ Packet (Datagram) ---→ N/W (Datagram N/W)

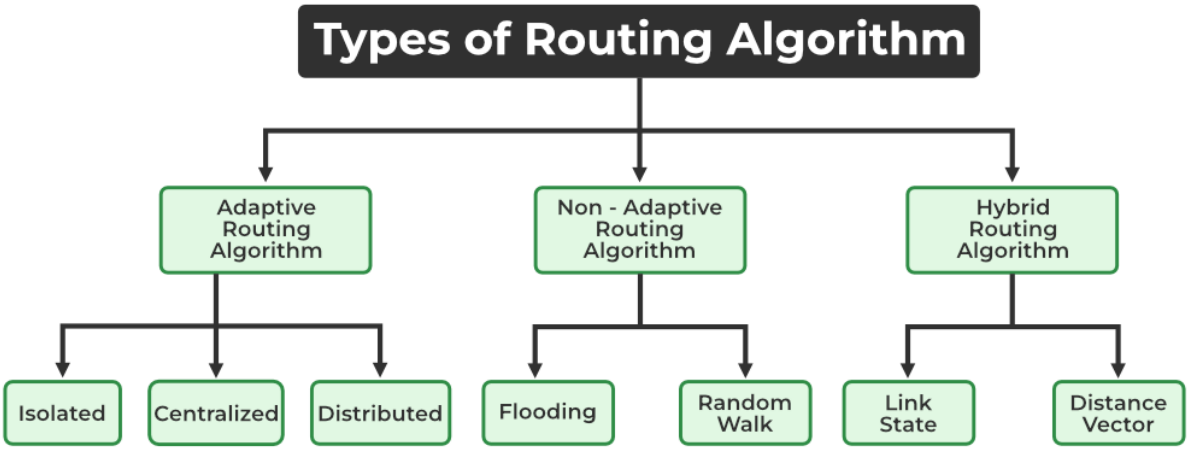
Connection Oriented service--→ Virtual Circuit --→ V/C N/W

Routing Algorithm:

Routing algorithms are methods for finding the best path to send packets from a source to a destination in a network. There are different types of routing algorithms, such as **adaptive**, **non-adaptive** and **hybrid**.

Classification of Routing Algorithms
The routing algorithms can be classified as follows:

1. Adaptive Algorithms
2. Non-Adaptive Algorithms
3. Hybrid Algorithms



Types of Routing Algorithm

Routing Algorithm:

- Optimality Principle ---------sink tree ---------- Bellman Ford Algorithm
- Shortest path Algorithm -----Dijkstra
- Flooding
- Distance vector Routing ------ Bellman Ford
- Link State Routing ------- OSPF (Open Shortest Path First)
- Hierarchical Routing
- Broadcast Routing (All destination) --------- Sink Tree (Spanning Tree)
- Multicast Routing (Group destination) ---------- MOSPF
- Anycast Routing ---------- packet is delivered to nearest member of group ---- part of DNS.
- Routing for Mobile Host
- Routing for Ad Hoc N/W

*** Routing Table : Hierarchy ---→ Cluster x Region x Routers = No of Routers

Congestion Control Algorithms:

- Traffic Aware Routing
- Admission control
- Traffic Throttling
- Load shedding

Integrated Services Digital Network (ISDN)

These are a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. Before Integrated Services Digital Network (ISDN), the telephone system was seen as a way to transmit voice, with some special services available for data.

Resource Reservation Protocol (RSVP)

Resource Reservation Protocol (RSVP) is used in real-time systems for an efficient quality band transmission to a particular receiver. It is generally used by the receiver side for the fast delivery of the transmission packets from the sender to the receiver.

Tunnelling:

--------→ IPV6 ----------→ IPV4 ----------→ IPV6

Internet Control Protocols:

1. **IMCP (Internet Control Protocol)**
2. **ARP (Address Resolution Protocol)**
3. **DHCP (Dynamic Host Congestion Protocol)**
4. **MPLS (Multi Protocol Label Switching)**
5. **OSPF (Open Source Path First)**
6. **BGP (Border Gateway Protocol)**

7. **IGMP (Internet Group Management Protocol)**

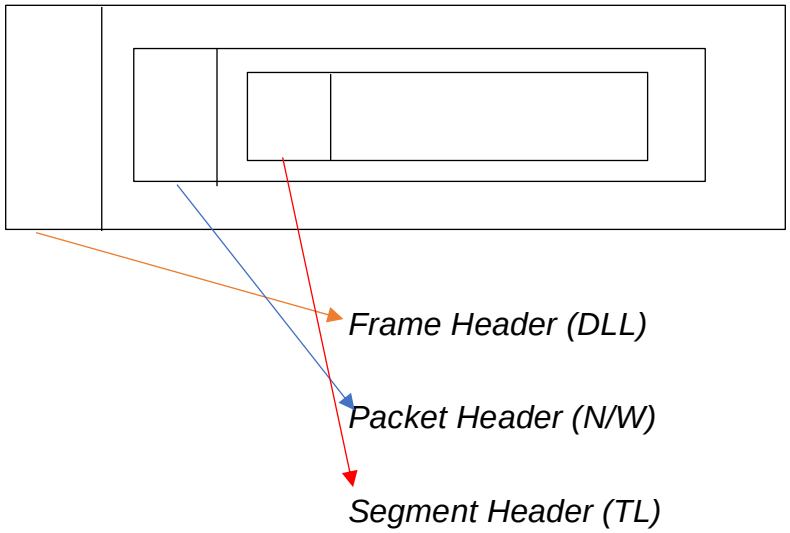
8. **PIM (Protocol Independence Multicast)**

Transport Layer

(End to End Layer)

Transport Service Primitives:

- **Listen**
- **Connect**
- **Send**
- **Receive**
- **Disconnect**



***Four Primitives are executed in that order by server**

- Socket
- Bind
- Listen
- Accept

Other primitives: Connect, Send, Received, Close

Port : 1024 – 65535

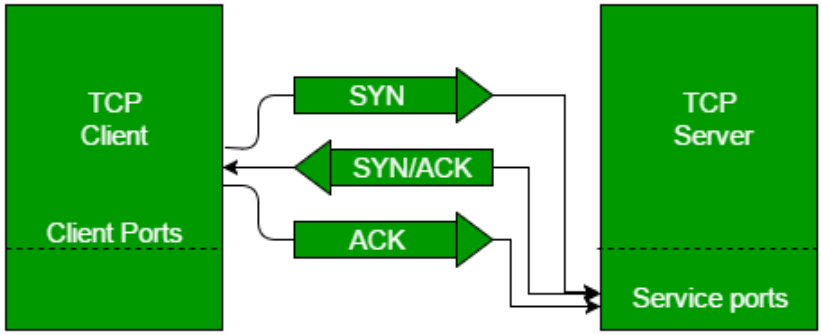
Port : Below 1023 are reserved for privileged users

TSAP ---→ Service Name ---→ Bit Torrent ----→ Port Mapper--→Rec Inf (Data set)

(Transport service access protocol)

TCP Connection Establishment:

3 way Handshake



Connection Release:

Asymmetric & Symmetric release

Error control & Flow control:

1. CRC
2. ARQ (Automatic Repeat Request)
3. Stop & Wait
4. Sliding window (Bidirectional)

Multiplexing:

Multiplexing (sometimes contracted to **muxing**) is a method by which multiple analog or digital signals are combined into one signal over a shared medium.

SCTP (Stream Control Transmission Protocol): inverse multiplication

Protocol & Signal

Sl NO.	Protocol	Signal
01	XCP	Rate to use

02	TCP with ECN	Congestion warning
03	Fast TCP	End to End delay
04	Compound TCP	Packet Loss & End to End delay
05	Cubic TCP	Packet loss
06	TCP	Packet loss

Internet Transport Protocol:

- Transmission Control Protocol (TCP)
  - Connection oriented
  - Reliable layer
- User Datagram Protocol (UDP)
  - Connectionless
  - DNS
  - Remote procedural Call
  - Real Time Transport Protocol

Important Port- protocol – Use

Port	Protocol	Use
20,21	FTP	File Transfer
23	Telnet	Remote Login
25	SMTP	Email
80	HTTP	World Wide Web
110	POP-3	Remote email access
143	IMAP	Remote email access
443	HTTPS	Secure Web HTTP over SSL
543	RTSP	Medium Player Control
631	IPP	Printer Sharing

1024 – Reserved for standard services

Email:

To :- Primary Receipt (whom it intended); who will reply the email

CC (Carbon Copy) :- Includes people who might be interested, not mean to respond, sometime when primary not respond. Every one can see who was include in the To & CC.

BCC (Blind Carbon Copy):- Sender doesn't want that other people know who else email chain. BCC can monitor others. BCC invisible to both people in To & CC

What is jitter?

Jitter is any deviation in, or displacement of, the signal pulses in a high-frequency digital signal. The deviation can be in terms of amplitude, phase timing or the width of the signal pulse.

Jitter in Internet Protocol (IP) networks is the variation in the latency on a packet flow between two systems when some packets take longer to travel from one system to the other. Jitter results from network congestion, timing drift and route changes.

Jitter can cause a display monitor to flicker, affect the ability of the processor in a desktop or server to perform as intended.

Application Layers

DNS (Domain Name System):

Naming hierarchy is managed by an organization called ICANN (International Corporation for Assigned Name & Numbers).

Protocols:

- MIME (Multipurpose Internet Mail Extensions)
- SMTP (Simple Mail Transfer Protocol)

Caching:

Squirrelling away pages that are ffetched for subsequent use is called caching.

Web search: Engine- Google, Yahoo, Bing

Digital Audio: Human ear runs from 20 Hz to 20,000 Hz

Digital Video: Sequence 50 image/ sec

Color- 29.97 frame/ sec

Video compression: JPEG (Joint Photograph Expert Group)

MPEG (Motion Picture Expert Group)

SIP (session initiation protocol): describe how set up internet telephone calls, video conferences and other multimedia connection.

Web Proxies: Browser can cache response & reuse then to answer future requests.

Content Delivery Network (CDNs): Provider who places a copy of page in a set of nodes at different locations & directs the client to use a near by node as the server.

Peer to Peer N/W: File sharing N/W is that many computers come together and pool their resources to form a content distribution system.

Bit Torrent-→ Distributed Hash Tables → Function of an index is to map key to a value.

Network Security

Decryption and Encryption

RSA Algorithm:

RSA is an encryption algorithm that uses two large prime numbers to generate public and private keys. The public key can be used to encrypt messages, and the private key can be used to decrypt them. Here is a simple example

- Choose two prime numbers p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and φ(n) are coprime. Let e = 7
- Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- The public key is (e, n) = (7, 33)
- The private key is (d, n) = (3, 33)
- To encrypt a message m, compute c = m^e % n. For example, if m = 9, then c = 9^7 % 33 = 27
- To decrypt a message c, compute m = c^d % n. For example, if c = 27, then m = 27^3 % 33 = 9

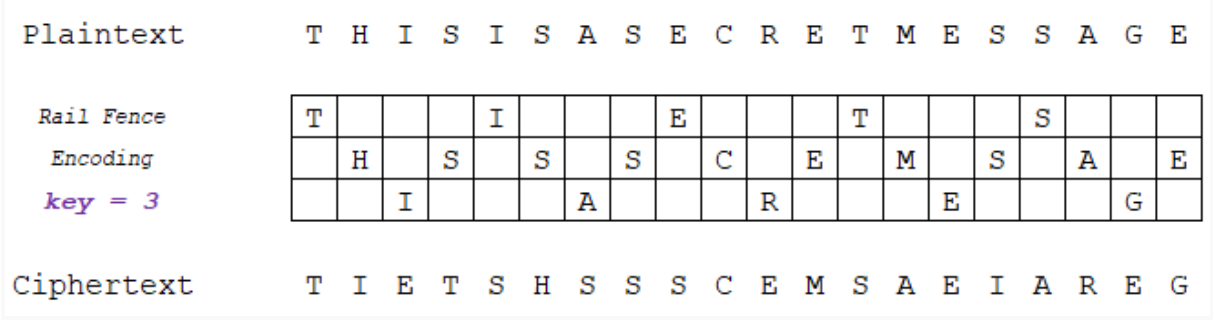
Transposition cipher:

A transposition cipher is a type of encryption that rearranges the letters of the plaintext according to a certain pattern. For example, the rail fence cipherwrites the plaintext in zigzag lines and reads it off by rows. Another example is the columnar transposition cipher that writes the plaintext in columns and reads it off by a certain order.

Rail Fence Cipher:

More complex Rail Fence Ciphers have more “rails”. For instance instead of writing the code over two lines (“rails”) you can write over three or four or more lines. The number of lines used in a Rail Fence Cipher is called the **key**.

Key = 3



A Rail Fence Cipher with 3 “rails” (Key = 3)

Route Cipher:

As an example, lets encrypt the plaintext "abort the mission, you have been spotted". First we need to decide on the number of columns we are going to use, lets say 5.

A	B	O	R	T
T	H	E	M	I
S	S	I	O	N
Y	O	U	H	A
V	E	B	E	E
N	S	P	O	T
T	E	D	X	X

Notice how we have used nulls

We then choose which route w

The plaintext written in a grid with 5 columns.

With a route of reading down the columns we get the ciphertext: "ATSYV NTBHS OESEO EIUBP DRMOH EOXTI NAETX".

With a route of spiralling inwards counter-clockwise from the bottom right we get: "XTEAN ITROB ATSYV NTEDX OEHOM EHSOE SPBUI".

Column Transposition:

The message WE ARE DISCOVERED SAVE YOURSELF

using the key word AUTHOR and ordering the columns by the lexicographic order of the letters in the key word

```
A U T H O R
1 6 5 2 3 4
-----------
W E A R E D
I S C O V E
R E D S A V
E Y O U R S
E L F A B C
```

yields the cipher

W I R E E R O S U A E V A R B D E V S C A C D O F E S E Y L .