CYBERSECURITY ESSENTIALS

ABHILASH KARAMPURI

CYBERSECURITY ESSENTIALS

ALL IN ONE

Published by

Abhilash Karampuri

Table of Contents…

Sno.	Chapter	Topic	Page
1	Introduction to Networking	1. Definition	
		2. Networking devices	
		3. Network topologies	
		4. Types of Networks	
		5. Components of Network	
		6. IP Address	
		7. Subnet mask	
2	Network Models and protocols	**1. Introduction to Network Models**	
		2. OSI Model	
		3. TCP/IP Model	
		4. Comparison between OSI and TCP/IP	
		5. Important Network Protocols	
3	Introduction to Network Security	**1. Definition**	
		2. Types of Hackers	
		3. CIA Triad	
		4. OSI Security architecture	
		5. Network Security model	
4	Introduction to Cryptography	**1. Definition**	
		2. Features	
		3. Types of Cryptography	
		4. Block Cipher Algorithms	
5	Cyber Attacks and social engineering	**Introduction**	
		Phishing	
		Malware	
		Man in the Middle	
		Brute force	
		Ransomware	
		DOS and DDOS	

1 INTRODUCTION TO NETWORKING

What is a Network?

A network refers to a collection of interconnected devices and systems that communicate with each other to share resources and information.

A Network consists of N number of interconnected devices. These devices are called as nodes.

All these devices are connected through a Networking device.

Lets discuss about Networking devices.

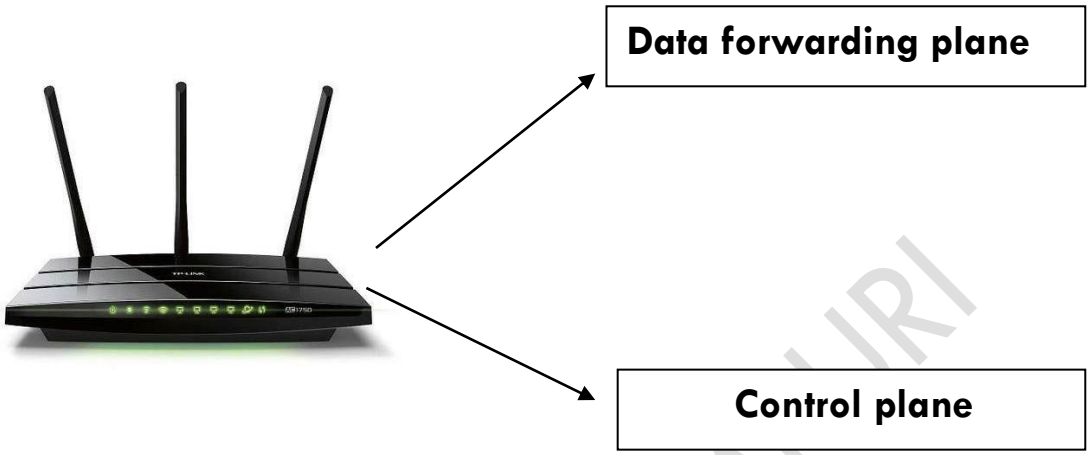
Networking devices

Network devices, also known as networking hardware, are the physical components that facilitate the communication and interaction of devices within a network.

Networking devices are of many types such as Routers, Physical Cables, Switches, Hubs etc.

Lets discuss about each of them in detail.

1. **Routers**
   - Routers are the networking devices which are used to connect the computers to ISP(Internet Service Providers) by unique IP addresses.
   - IP addresses are the unique identifiers for each networks.
   - Similar IP addresses indicates similar network whereas Distinct IP addresses indicates distinct networks.
   - Routers are used to connect the computers to share resources through internet among distinct IP addresses.
   - Routers consists of two planes: Data forwarding plane and control plane.
   - Control plane determines how data packets are transferred among the network by using a routing table which consists of IP addresses.
   - Data forwarding plane actually forwards the data packets to the destination.



Lets understand about routers with an example

You all may heard about Hathway which is a popular Internet Service provider allowing the users to facilitate the access to internet, Can you imagine how they usually do this in reality.

All the devices or computers at your home or at office may have distinct IP addresses. All these devices are connected through a router to connect to the main router of Hathway ISP allowing you to access the internet on daily basis.

Since they are having distinct IP addresses they cannot be connected to internet through any other networking devices like HUB or switch etc. Routers are specifically designed to connect the devices of various IP addresses to the same network.

Have you ever heard about modems? Modems are the inbuilt component of routers that convert analog signals into digital signals.

The computers are incapable of converting the transmitted analog signals into digital signals hence we place modems in the middle for converting the analog signals travelled through cables into digital signals.

2. HUB

- HUBs are networking devices that are used to connect multiple computers to facilitate communication and the exchange of resources.
- Hubs broadcast incoming data packets to all ports, regardless of the destination. This means every device connected to the hub receives the data, even if it is not the intended recipient. This can lead to network congestion and inefficiency, as all devices must process the irrelevant data, increasing the likelihood of collisions and slowing down the network.
- Hubs do not have the capability to filter data or manage network traffic. They do not inspect or make decisions based on the MAC addresses of devices. This lack of data management means that hubs cannot optimize the flow of traffic or enhance network performance.
- Hence Hubs are often referred to as "dumb" devices because they lack the intelligence to manage data traffic efficiently within a network.

- Since Hubs broadcasts the data to all available nodes of a network it is not considered as intelligent device because there is lack of security and availability.
- Hence we do not use Hubs in general we use switches which can overcome the limitations of Hubs.

3. Switch

- A switch is an intelligent networking device used to facilitate communication across multiple devices or computers by connecting them to a common device called switch.
- When a switch receives a data packet, it examines the source MAC address and the port it arrived on. It records this information in its MAC address table (or CAM table).

- This process allows the switch to learn which devices are connected to which ports, building a map of the network.
- When a switch receives a data frame destined for a specific MAC address, it looks up the destination MAC address in its MAC address table.
- If the destination MAC address is found in the table, the switch forwards the frame only to the port associated with that address.
- If the destination MAC address is not found (or the frame is a broadcast frame), the switch floods the frame to all ports except the one it arrived on.
- Switches can filter and control the flow of data based on the MAC addresses. They only send data to the intended recipient, reducing unnecessary traffic on the network.
- This reduces network collisions and improves overall network performance and efficiency.

Advantages:

Switches offer several advantages over other networking devices like hubs. Here are some key advantages of switches:

1. Efficient Data Transmission

- Switches operate at the data link layer (Layer 2) of the OSI model and use MAC addresses to forward data frames. Unlike hubs, which broadcast data to all connected devices, switches send data only to the intended recipient, reducing unnecessary network traffic and improving overall network efficiency.

2. Increased Bandwidth

- Switches provide dedicated bandwidth to each port, allowing devices to communicate simultaneously without contention. This improves network performance and ensures that devices can transmit data at their maximum capacity.

3. Reduced Collisions

- By creating separate collision domains for each port, switches prevent collisions that can occur in shared media environments (e.g., with hubs). This enhances network reliability and minimizes the chances of data loss or corruption.

4. Enhanced Security

- Switches can filter and control the flow of data based on MAC addresses. They only forward data to the intended recipient, reducing the risk of eavesdropping and unauthorized access to sensitive information.

Additionally, switches support features like VLANs, which isolate traffic between different segments of the network, enhancing security.

5. Flexibility and Scalability

- Switches support flexible network configurations and can accommodate various types of devices, including computers, printers, servers, and VoIP phones. They also support features like link aggregation, VLANs, and Quality of Service (QoS), allowing for the creation of complex and scalable network architectures.

6. Easy Troubleshooting

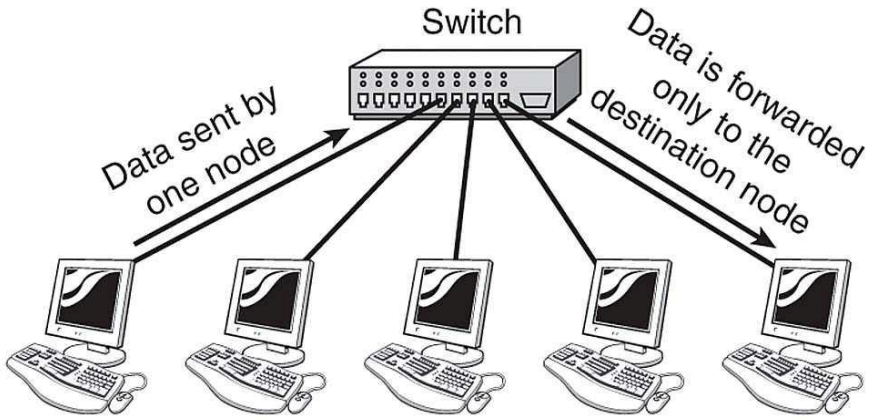
- Switches provide advanced diagnostic tools and management capabilities, making it easier to troubleshoot network issues and monitor network performance. Features like port mirroring allow administrators to analyze network traffic for troubleshooting and security purposes.

7. Support for Advanced Features

- Switches support advanced networking features such as Spanning Tree Protocol (STP) for loop prevention, Quality of Service (QoS) for prioritizing traffic, and Link Aggregation for increased bandwidth and redundancy. These features enhance network functionality and reliability.

8. High Performance

- Switches offer high-speed connectivity and low latency, making them ideal for demanding applications such as video streaming, VoIP, and online gaming. They provide consistent and reliable network performance, even under heavy loads.



why Hubs or Switches are often connected to Routers?

Switches or Hubs themselves cannot provide communication among WANs like the internet. Switches or Hubs are just responsible for connecting multiple devices to facilitate communication over LANs. To enable communication over the internet or to connect multiple networks through switches over different IP addresses or locations we must use Routers.

I guess you had some basic idea about routers and the differences between switches and hubs.

Lets move on to network topologies.

Till now we have discussed about networking devices which are used to provide communication in a network.

Can you imagine how the network looks like?

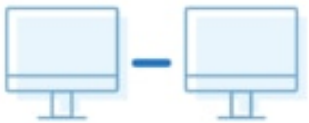
Networking Topologies

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as **Network Topology**.
The various network topologies are:

- Point to Point Topology
- Mesh Topology
- Star Topology
- Bus Topology
- Ring Topology
- Tree Topology
- Hybrid Topology

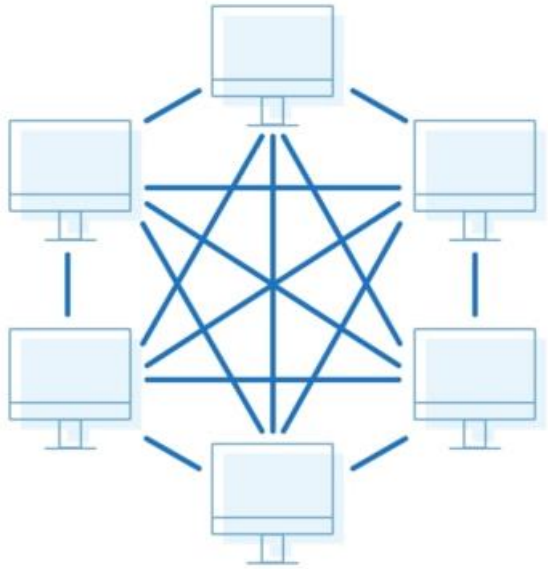
1. Point to Point Topology

Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.



2. Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.



Every device is connected to another via dedicated channels. These channels are known as links.

- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required = N * (N-1).
- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is ${}^{N}C_2$ i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 5*4/2 = 10.

Advantages of Mesh Topology

- Communication is very fast between the nodes.
- Mesh Topology is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

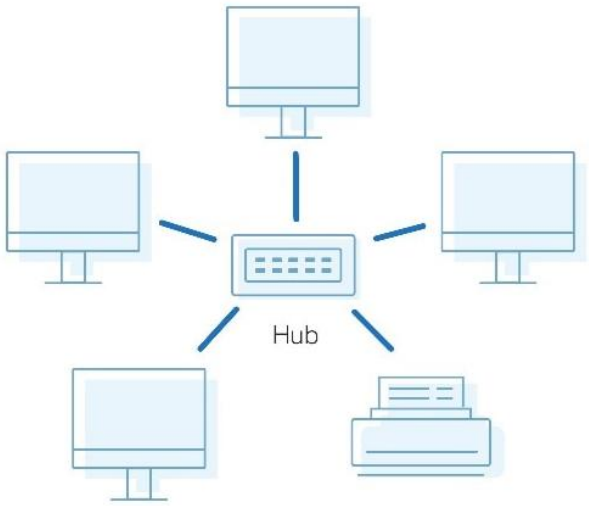
Drawbacks of Mesh Topology

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

A common example of mesh topology is the internet backbone, where various internet service providers are connected to each other via dedicated channels. This topology is also used in military communication systems and aircraft navigation systems.

3. **Star Topology**

   In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.



A star topology having four systems connected to a single point of connection i.e. hub.

Advantages of Star Topology

- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

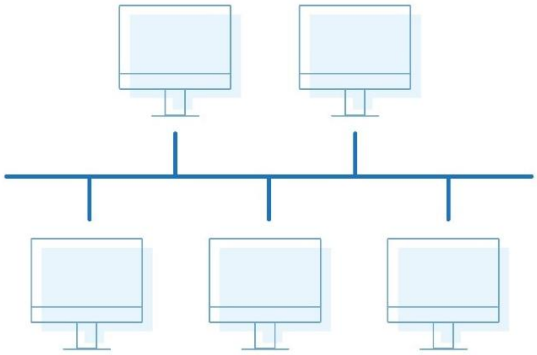
Drawbacks of Star Topology

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

A common example of star topology is a local area network (LAN) in an office where all computers are connected to a central hub. This topology is also used in wireless networks where all devices are connected to a wireless access point.

4. Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.



A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

Advantages of Bus Topology

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
  - Bus topology is familiar technology as installation and troubleshooting techniques are well known.
  - CSMA is the most common method for this type of topology.

Drawbacks of Bus Topology

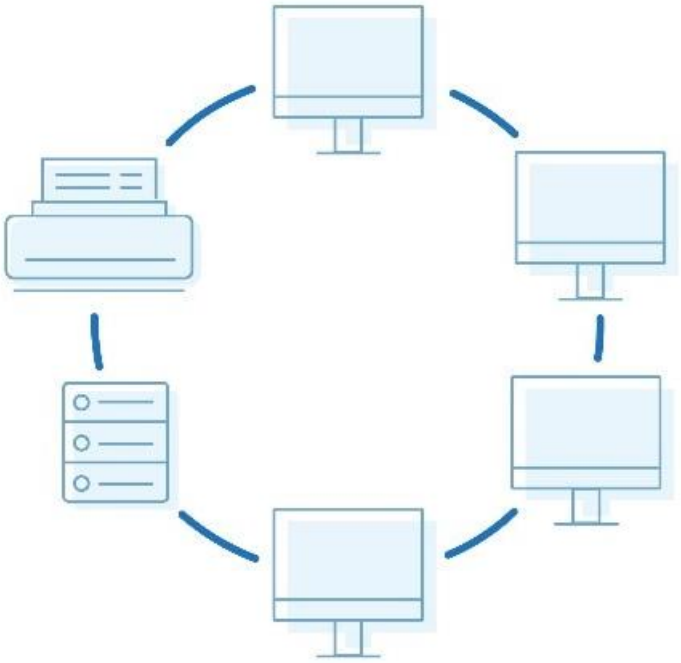
- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks.

5. Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighbouring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.



A ring topology comprises 4 stations connected with each forming a ring.

The most common access method of ring topology is token passing.

- **Token passing:** It is a network access method in which a token is passed from one node to another node.
- **Token:** It is a frame that circulates around the network.

Advantages of Ring Topology

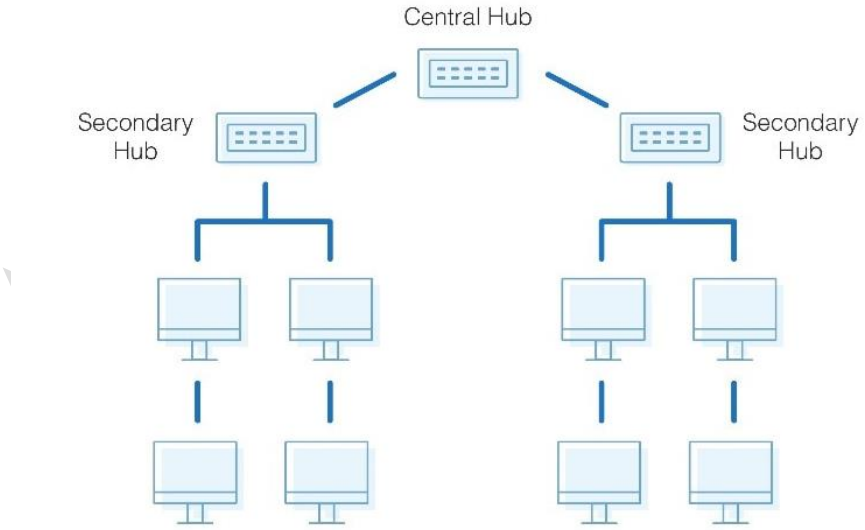
- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

Drawbacks of Ring Topology

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.
- Less secure.

Tree Topology

This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and SAC (Standard Automatic Configuration) are used.



In this, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of Tree Topology

- It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.
- It allows the network to get isolated and also prioritize from different computers.
- We can add new devices to the existing network.
- Error detection and error correction are very easy in a tree topology.

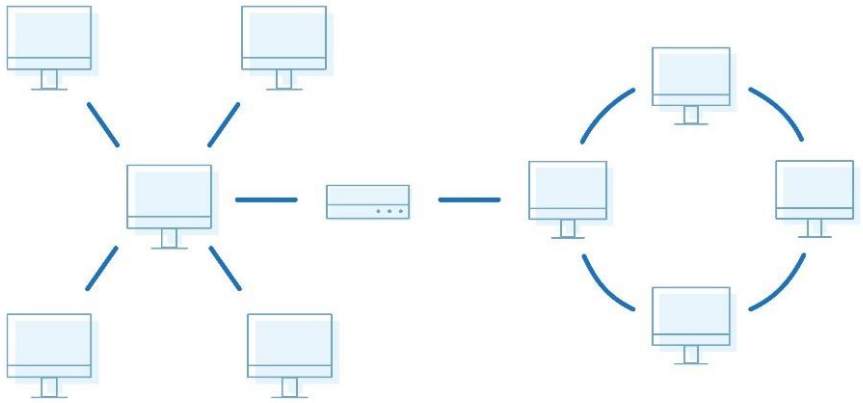
Drawbacks of Tree Topology

- If the central hub gets fails the entire system fails.
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

A common example of a tree topology is the hierarchy in a large organization. At the top of the tree is the CEO, who is connected to the different departments or divisions (child nodes) of the company. Each department has its own hierarchy, with managers overseeing different teams (grandchild nodes). The team members (leaf nodes) are at the bottom of the hierarchy, connected to their respective managers and departments.

Hybrid Topology

This topological technology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.



The above figure shows the structure of the Hybrid topology. As seen it contains a combination of all different types of networks.

Advantages of Hybrid Topology

- This topology is very flexible.
- The size of the network can be easily expanded by adding new devices.

Drawbacks of Hybrid Topology

- It is challenging to design the architecture of the Hybrid Network.
- Hubs used in this topology are very expensive.
- The infrastructure cost is very high as a hybrid network requires a lot of cabling and network devices.

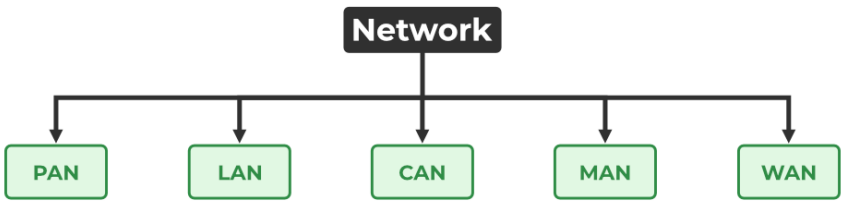
A common example of a hybrid topology is a university campus network. The network may have a backbone of a star topology, with each building connected to the backbone through a switch or router. Within each building, there may be a bus or ring topology connecting the different rooms and offices. The wireless access points also create a mesh topology for wireless devices. This hybrid topology allows for efficient communication between different buildings while providing flexibility and redundancy within each building.

Hope you have understood Network topologies. Next we move on to next topic.

Do you know How many types of networks are there? You may have confused between network topologies and types of networks. Both are different. Network topologies are the layout or arrangement of computer devices in a network where as types of the network determines the range of networks in terms of kilometers.

Lets discuss in detail about Types or classifications of Networks.

Networks are broadly classified into 5 types:



Parameters	PAN	LAN	CAN	MAN	WAN
Full Name	Personal Area Network	Local Area Network	Campus Area Network	Metropolitan Area Network	Wide Area Network
Technology	Bluetooth, IrDA,Zigbee	Ethernet & Wifi	Ethernet	FDDI, CDDi. ATM	Leased Line, Dial-Up
Range	1-100 m	Upto 2km	1 – 5 km	5-50 km	Above 50 km
Transmission Speed	Very High	Very High	High	Average	Low
Ownership	Private	Private	Private	Private or Public	Private or Public
Maintenance	Very Easy	Easy	Moderate	Difficult	Very Difficult
Cost	Very Low	Low	Moderate	High	Very High

The above table shows differences between types of networks.

By observing the table based on parameters we can easily understand the types of networks.

In addition to above types of networks we have other networks of different sizes or purposes (eg., SAN- Storage Area Network, EPN- Enterprise Private Network, VPN- Virtual Private Network)

Now u may have understood what is network and its devices, topologies and their types. Lets move on to the components of the Network.

Components of a Network

Components are the necessary things that need to built a network.

The main components of network may include the following:

- **End Device:**

  End devices are the systems or devices like PC, Laptops, smart phones or servers etc., at user interaction level.

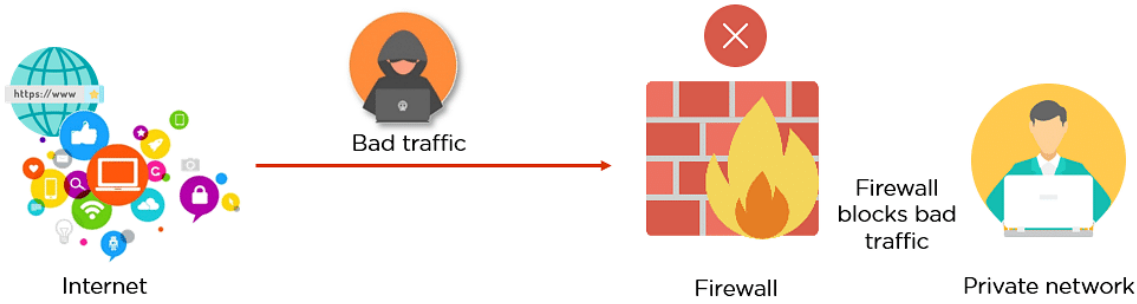
- **Switch:**

  As we discussed earlier, Switches are the network devices that are used to connect multiple end devices within a network.

- **Router:**

As we have discussed about Routers, which are the fundamental pillars of the networks used to connect multiple networks of distinct IP addresses. (For an example IP addresses 168.265.1 and 168.265.2,..... can be connected together using routers but 168.265.1 and 168.266.2 cannot be interconnected through routers because their ISP are different. Remember that routers are used to connect multiple networks of similar ISP networks only)

- **Firewall:**



A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Its primary function is to establish a barrier between a trusted internal network and untrusted external networks, such as the internet.

- **Transmission medium:**

The way information is transmitted is called as transmission medium.

(e.g., through cable or wireless)

Till now we have discussed all the fundamental concepts of networking. Do you know how end devices have access to internet so easily? This is due to IP address.

Lets discuss in detail about IP address.

IP Address:

To enable communication among end devices or to access Facebook, google etc through internet, each device must have a unique identifier.

This unique identifier is called IP address. There cant be two or more same IP address in a same network (or on the internet) because there will be conflict and internet connection will not work properly.

Here we are going to discuss about general version of IP Adress that is used everywhere which is called as IPv4 IP address.

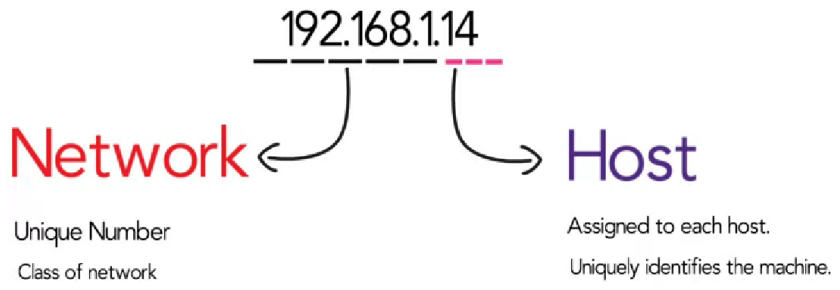
IP address of IPv4 consists of 32 bits of 4 parts separated by '.'

Each part can be a number from 0 to 255 which indicates total number of 256 bytes or 32 bits.

IP Adress consists of two classes i.e., Network class and host class.

Network class is similar for all devices of a network but host class is unique for each machine.

This host class particularly determines the location of a machine in a network.



Do you know how to know your device IP address?

If you want to know the IP address of your PC or Laptop you need to open the command prompt and enter "ipconfig" Then you will be able to see the IP address of your device.

```
C:\Users\abhil>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : bbrouter
   Link-local IPv6 Address . . . . . : fe80::a695:6310:dd68:cc2c%8
   IPv4 Address. . . . . . . . . . . : 192.168.1.8
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

As you can observe the IP Address of my Laptop is 192.168.1.8

Here 192.168.1.0 is the IP address of my network and 0.0.0.8 is the IP address of host device. But how can you identify this?

To identify which portion of IP Address is network class and which portion belongs to host class subnet mask comes into action.

Subnet mask

Subnet mask describes which portion of your IP address belongs to network class and which portion of IP address belongs to host class.

For example subnet mask is shown as 255.255.255.0 for IP Address 192.168.1.8 which means 192.168.1 belongs to network class and 8 represents host class.

But how computers in a network analyze this? They are incapable of understanding numeric computation, they only know binary numbers.

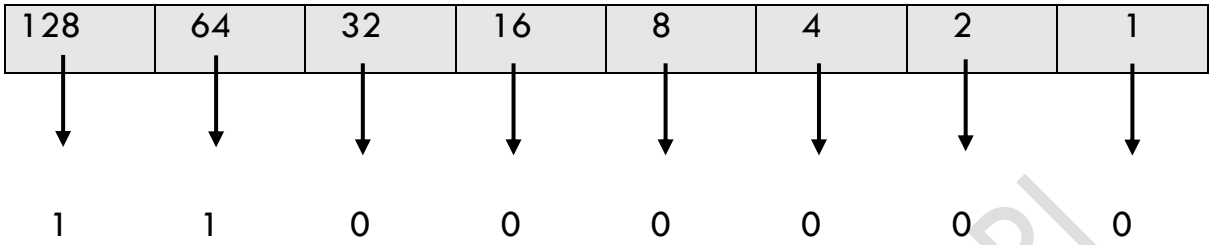
Hence they convert the IP address into binary form to identify the network class and host class. Lets understand this with octet chart.

128	64	32	16	8	4	2	1

The above octet chart helps to convert the digits into binary form.

Now lets convert the IP address into binary format.

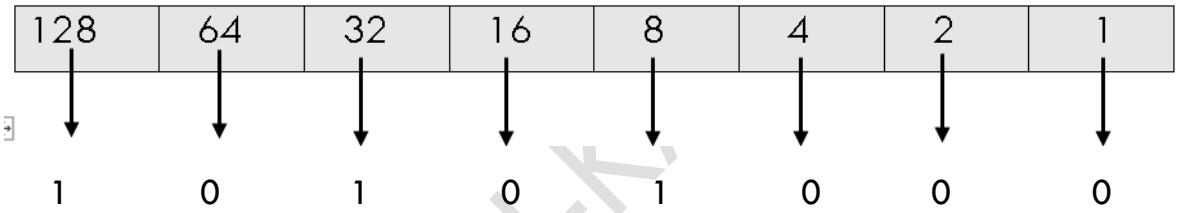
First lets convert 192 into binary



The sum of 128+64+32=192

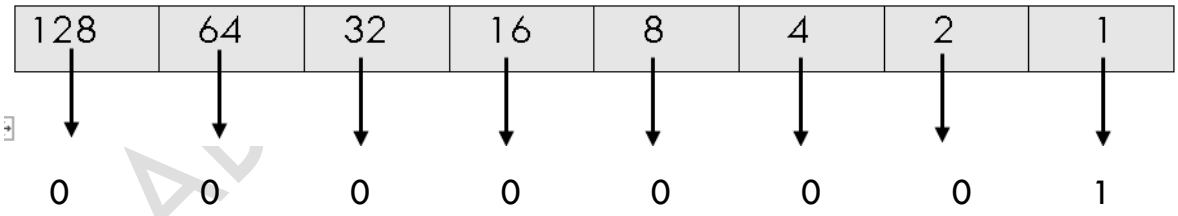
Hence the binary form of 192 is 11000000.

Similarly the binary form of 168 is



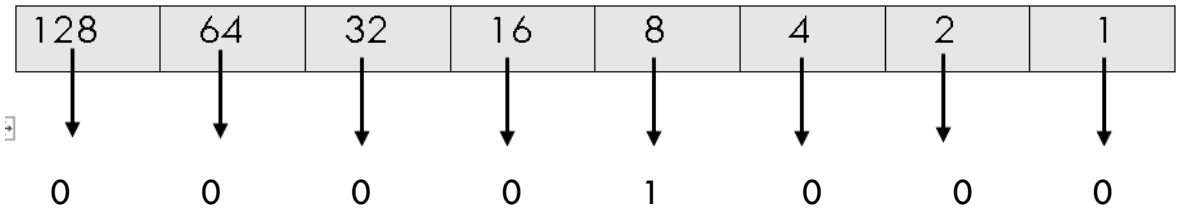
The binary form of 168 is 10101000

Now lets find the binary form of 1



The binary form of 1 is 00000001

Lets find the binary form of remaining one i.e., 8



The binary form of 8 is 00001000

Therefore the binary format of the IP address for the above example is **11000000.10101000.00000001.00001000**

In the above console, the subnet mask is given as 255.255.255.0

Now we need to convert this into binary form to understand which is the network class and which is the host class.

The binary form of 255 is 11111111

Therefore the binary form of subnet mask is

11111111.11111111.11111111.00000000

Now lets map the IP address with subnet mask

1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 0 . 0 0 0 0 0 0 0 1 . 0 0 0 0 1 0 0 0

1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 0 0 0 0 0 0 0 0

The bits of IP address mapping to 1s in subnet mask indicates the network class and the bits of IP address mapping to 0s in subnet mask indicates the host class.

Therefore,

1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 0 0 0 1 0 0 0

1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 0 0 0 0 0 0 0 0

Therefore, 11000000.101010000.00000001 indicates the network class and 00001000 indiactes host class.

Lets convert into numerical digits.

192.168.1.0 → IP address of network class

0.0.0.8 → IP address of host class

Now you have clear idea about how the end devices have their unique IP address now lets see advantages of IP address.

Unique Identification

One key advantage of IP addresses is unique identification. Each device on a network is assigned a unique IP address, ensuring that data sent over the network reaches the correct destination. This uniqueness is maintained globally for public IP addresses and within local networks for private IP addresses.

Addressing and routing

Addressing and routing are another important benefit. IP addresses are crucial for routing data packets between networks. Routers use IP addresses to determine the best path to forward packets to their destination. The hierarchical structure of IP addressing, which includes network and host portions, helps efficiently manage and route traffic both within and between networks.

Scalability

Scalability is another significant advantage of IP addressing. IP addressing schemes, particularly IPv6, support a vast number of unique addresses, enabling the growth of the internet and the addition of new devices without running out of addresses. Network subnetting allows administrators to divide a larger network into smaller, more manageable sub-networks, optimizing performance and security.

Flexibility

IP addresses offer flexibility in network management. They can be assigned dynamically using DHCP or statically through manual configuration. Private IP addresses can be reused in different local networks, conserving the global pool of public IP addresses.

Security

In terms of security, IP addresses facilitate various network security measures. Firewalls and access control lists (ACLs) can use IP addresses to define security rules. Additionally, IP addresses can help determine the geographic location of a device, enabling location-based security policies.

Communication

IP addresses are essential for communication and connectivity. They enable devices to access the internet and communicate with web servers, email servers, and other internet services. Their support for interoperability allows seamless communication between different types of devices and networks.

Management and monitoring

For management and monitoring, IP addresses allow administrators to effectively manage and monitor network devices, identifying and troubleshooting issues. They are also used in network logs and audit trails to track and investigate network activity for security and compliance purposes.

Service provisioning

Service provisioning is another advantage of IP addresses. They are crucial for hosting websites, email services, and other online services, allowing clients to reach servers by resolving domain names to IP addresses. IP addresses also facilitate load balancing, which distributes network or application traffic across multiple servers to ensure reliability and performance.

Quality of service

Quality of Service (QoS) mechanisms rely on IP addresses to prioritize certain types of traffic, ensuring that critical services receive the necessary bandwidth and low latency.

Can you ever imagine a world without IP address?

Imagining a world without IP addresses reveals how crucial they are for the functioning of modern technology and communication systems. The absence of IP addresses would fundamentally disrupt how devices communicate on local networks and the internet. Here are some scenarios and consequences in such a world:

1. Lack of Device Identification
2. Internet Collapse
3. Failure of Online services
4. No future technology advancement
5. Impact on IoT and Smart devices
6. Loss of Digital Innovation
7. Security and surveillance issues.

Hope you have a clear idea about IP address and its importance. Lets move on to next topic.

Components required to communicate over internet

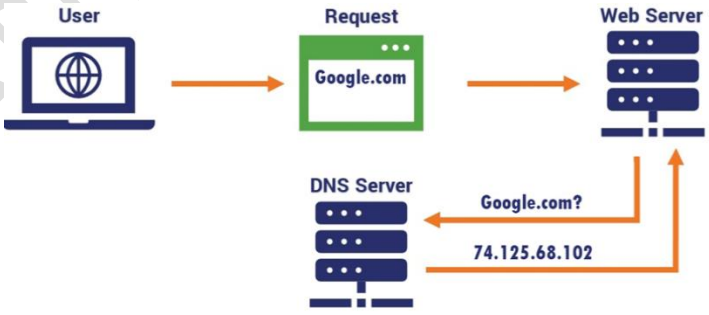
1. **IP address:**
   As we have discussed about IP address which are the unique identifiers for each device. It is the pillar for communication and identification over network communication over internet.
2. **Subnet mask**
   It indicates the size of the network. Subnet mask is usually used to determine the classes of network and host to identify the network and host IP address.
3. **Default gateway**
   The default gateway is router which specifies the way out of network and helps to access to internet. It maintains connectivity over internet with the device.
4. **DNS**

   Have you ever imagined how the computer searches our query on google or Chrome etc. If we want to open YouTube we enter YouTube in the google or we can type https://youtube.com to access to YouTube services. But the computer cannot identify the exact word or query to get access to the webpage. It directly extends the link as https:// and then it converts it into its unique IP address. But how it can be done> By using DNS (Domain Name Server) which is a domain generating engine which converts the domains into its unique IP addresses.

   For example

   https://google .com → 216.58.192.142

   These IP address can be updated and changes can be made by the ISP. Hence they are not fixed, but the changes are incurred into DNS server too to facilitate easy search and access to web services.



Very short answer questions

- Define a Network.
- Define Networking devices.

- Define Router
- Define Switches and Hubs
- Why Hubs or Switches are often connected to Routers?
- List out Network Topologies
- List out range and applications of Local Area Network.
- Write a short note on VPN.
- What do you mean by end devices?
- Define firewall.
- Write a short note on IP Address.
- Define subnet mask.
- Write a short note on DNS.

Short answer questions

- Differentiate Switches and Hubs
- Explain in brief about features of Router.
- We use Switches in a network instead of Hubs. Justify?
- List out Advantages and Disadvantages of Switch.
- Write a short note on Mesh topology and star topology.
- List out Advantages and disadvantages of Ring topology.
- Compare LAN and MAN Networks.
- List out consequences of not having IP Address in this world.
- Write a short note on Components required to communicate over internet.

Long answer questions

- Explain Networking devices (Routers, Switches, Hubs, Cables)
- Explain in brief about Networking topologies with neat diagram.
- Discuss Types of Networks (PAN, LAN, CAN, MAN, WAN).
- Explain about IP Address and subnet mask in detail.

***

2 NETWORK MODELS & PROTOCOLS

What is a Network Model?

A Network model is a conceptual framework that describes how end devices communicate with each other.

It describes how the data is transferred from sender to receiver.

There are two common computer network models

1. OSI (Open System Interconnection) Model
2. TCP/IP (Transmission Control Protocol) Model

To send a data from sender to receiver the data come across many layers like application, presentation, session, Transport, Network, Data link layer and Physical layer in order to reach data to the destination.

These layers involve various techniques such as encryption, decryption, compression, and decompression to provide security for the data for data integrity and confidentiality.

Lets discuss about OSI Model in detail.

OSI Model stands for Open System Interconnection which was developed by ISO (International Standardized Organization)

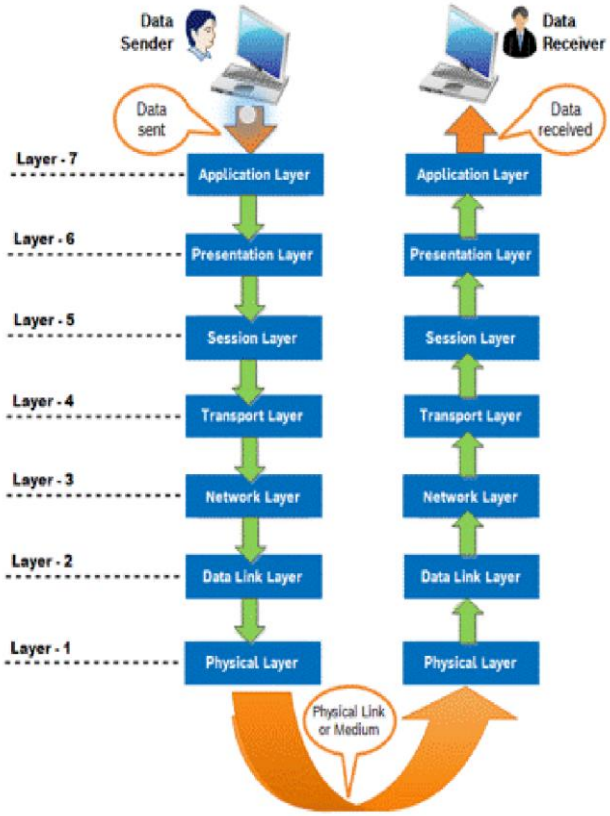
OSI Model is a conceptual framework that describes how data communication is established among two devices (sender and receiver).

It is a 7 layer architecture with each layer having its own functionality.

All layers work together and are independent of each other.

OSI Model is a base model for all advanced latest network models.

This model helps us in understanding the network communication between computers easily.



Imagine the data is transferred from sender to receiver. Both sender and receiver have 7 layers(i.e., Application, Presentation,……,Physical Layers).

First, the data is sent by the sender through the application interface, and the data is passed through 7 layers from top to bottom the data reaches the physical layer of the receiver side and the data is transferred from bottom to up and reaches the application interface of the receiver side and the data can be accessed by the receiver.

In this way, data communication is established between the sender and receiver.

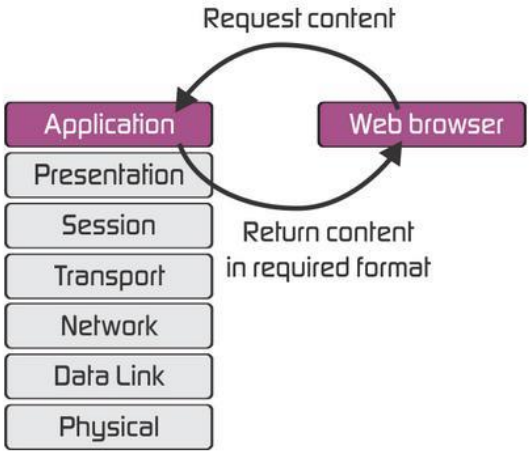
Now you may have a clear idea about how data is transferred externally from sender to receiver.

But what is happening inside these layers? What are the internal functionalities that are applied on the data.

Lets discuss about each layers in detail:

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

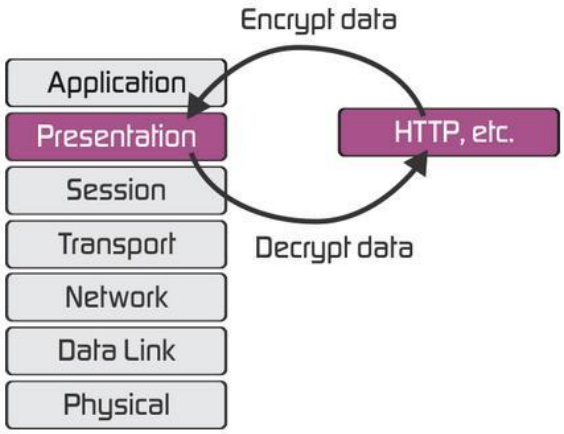
1. Application Layer



At the topmost, we can find application layer which is responsible for application services.
It generates the data to be transferred over the network.
It also serves as a window for the receiver side to display the data transferred.
Examples: Skype, Chrome, Gmail services.

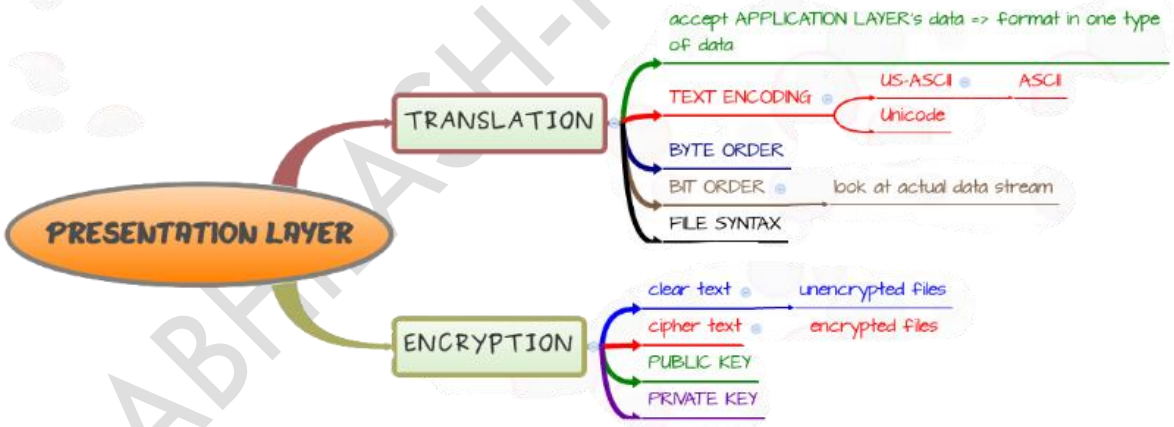
2. Presentation Layer

The Presentation Layer is the sixth layer of the OSI model. Its primary function is to ensure that the data sent from the application layer of one system can be read by the application layer of another.

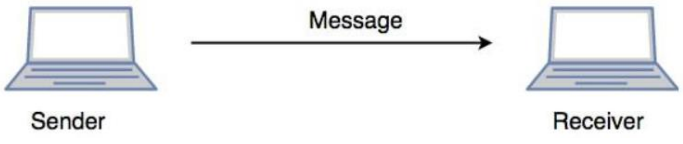


It acts as a translator, handling data format translation, encryption/decryption, and data compression. Key tasks include:

1. **Data Translation**: Converts data formats between systems, ensuring compatibility.
2. **Data Encryption/Decryption**: Secures data by encoding it for transmission and decoding it upon receipt.
3. **Data Compression/Decompression**: Reduces the size of data to optimize transmission speed and bandwidth usage.

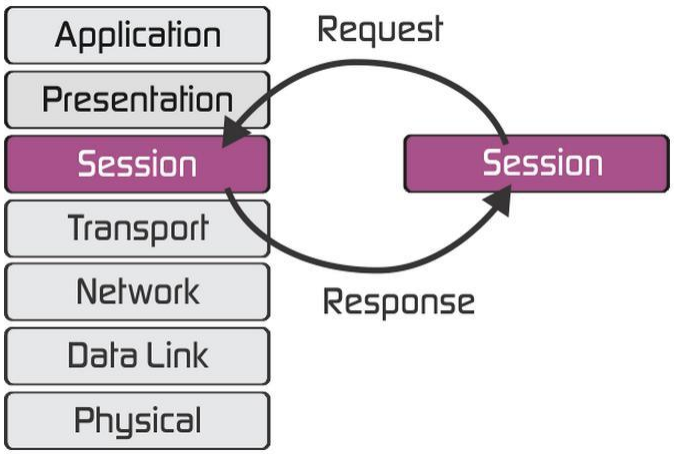


The two major techniques used in presentation layer are Translation and encryption/Decryption to maintain data confidentiality.
We will discuss about encryption and decryption techniques in detail in upcoming units.
Lets understand presentation layer with an example:



Let us consider a scenario where a user wants to send a message through some Messenger application running in their browser. The "**Messenger**" here acts as the application layer which provides the user with an interface to create the data. This message or so-called **Data** is compressed, optionally encrypted (if the data is sensitive), and converted into bits (0's and 1's) so that it can be transmitted.

3. Session Layer

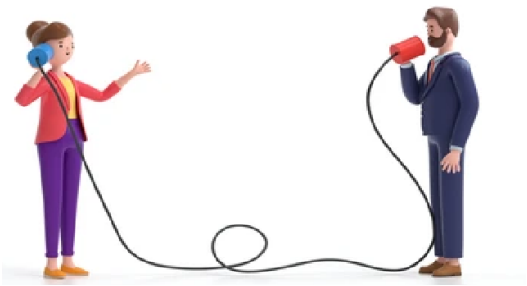


This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.

Functions of the Session Layer

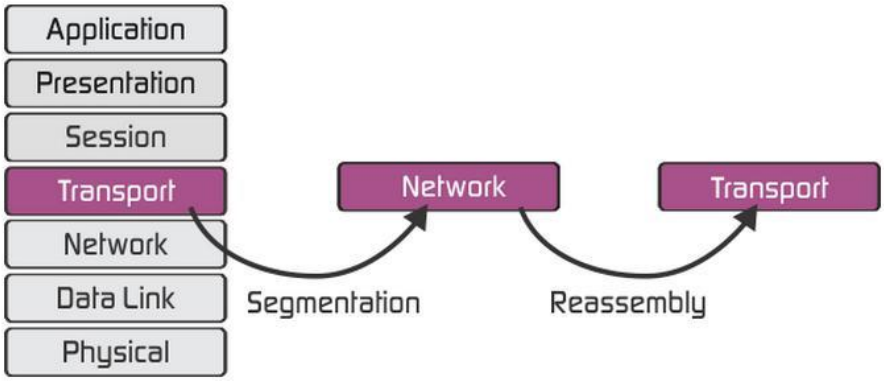
- **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use, and terminate a connection.
- **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
- **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

Lets understand Session with an example



To help understand the session layer, imagine two people at a party. They would typically say hello to each other at the start of the party, initiating a long session between the two of them. The length of the conversation between when they say hello and goodbye would be one session. When they say goodbye, it would end the session. Maybe much later they bump into each other and then say hello again, starting a new session.

4. Transport Layer



- The transport layer provides services to the application layer and takes services from the network layer.
- The data in the transport layer is referred to as *Segments*.
- It is responsible for the end-to-end delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.
- **At the sender's side:** The transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow and error control** to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.
- Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.
- The transport layer is called as **Heart of the OSI** model.

Functions of the Transport Layer

- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:** To deliver the message to the correct process, the transport layer header includes a type of address called service point

address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

Services Provided by Transport Layer

1. Connection-Oriented Service
2. Connectionless Service

1. Connection-Oriented Service: It is a three-phase process that includes

- Connection Establishment
- Data Transfer
- Termination/disconnection

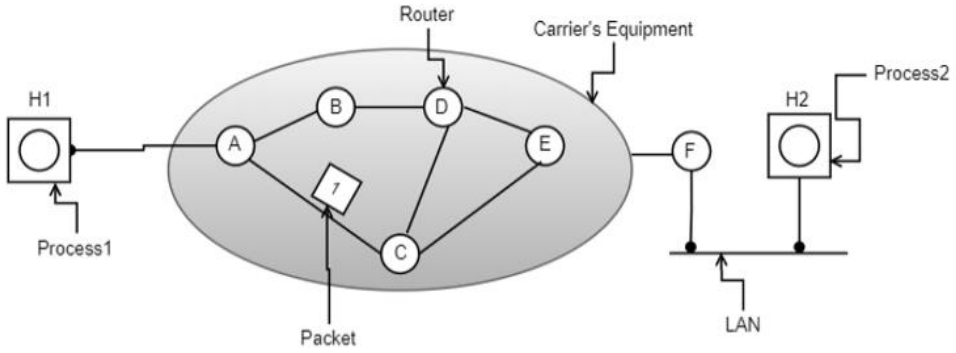
In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

3. **Connectionless service:** It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

5. Network Layer

In Network Layer the data is referred as packets.
Network Layer provides services to Transport layer and access services from data link layer.
The services provided by network layer are Routing and Logical Addressing.

- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
- **Logical Addressing:** To identify each device inter-network uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.



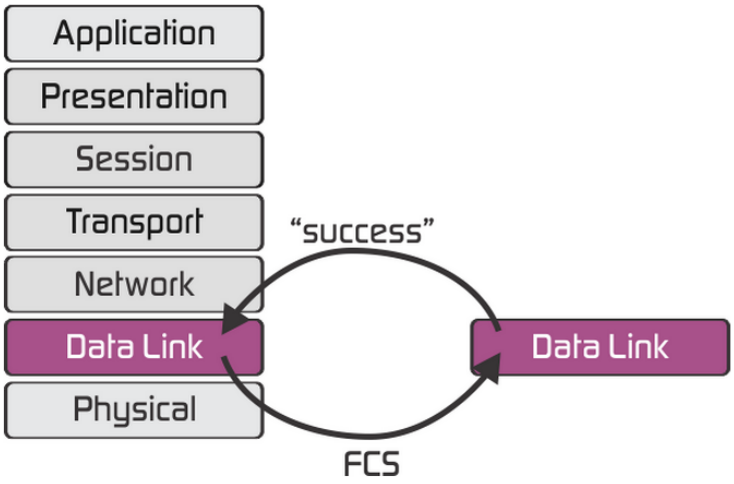
Observe the above fig which represents the data packets forwarding from one router to another by choosing the best path from source (H1) to destination (H2).

The data packet is forwarded from the A node (Router) to the C node instead of the B node. Why did the packet move to the C node instead of the B node? Is there any reason behind the packet moments?

The best path chosen depends on the routing table. Based on the information provided by the routing table the data packets are transferred from one router to another.

The Routing table is a service provided by the network layer which consists of information on the moments of data packets.

6. Data link Layer



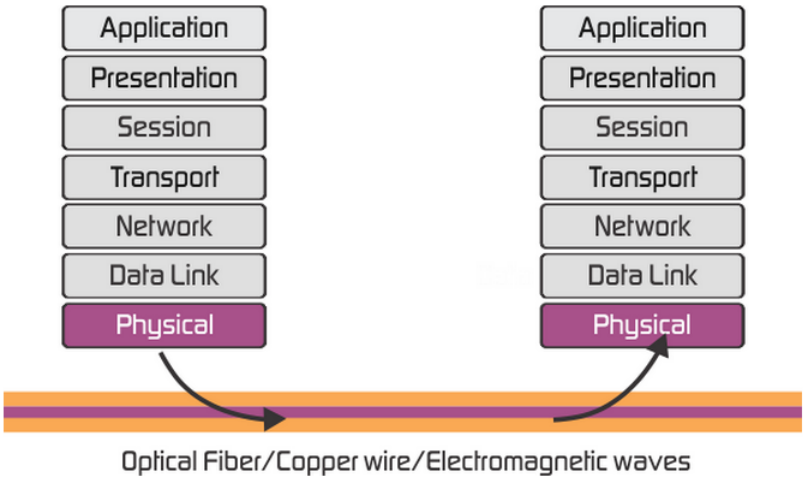
The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.

Functions of the Data Link Layer

- **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
- **Physical addressing:** After creating frames, the Data link layer adds physical addresses (**MAC addresses**) of the sender and/or receiver in the header of each frame.
- **Error control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.

- **Access control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

7. Physical Layer

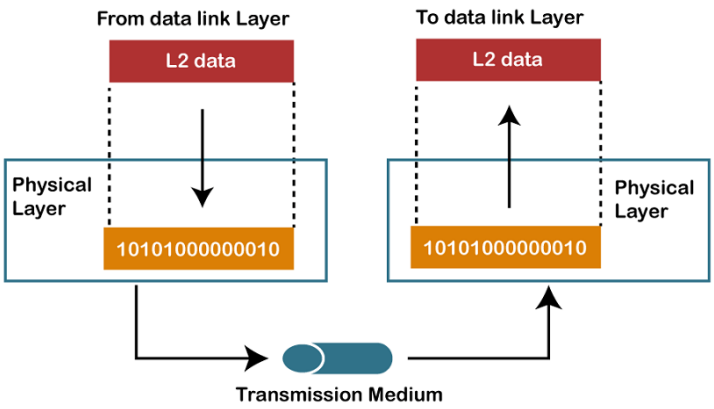


The data can be transferred from sender to receiver through LAN cables or through air(connection-less) i.e., wi-fi or Bluetooth.

The data from the data link layer is moved to the physical layer which consists of a transmission medium like cable wires or Open air (wi-fi or Bluetooth).

In the physical layer before transmission, the data received from the data link layer is converted into binary form or in bits.

These bits or binary forms of data from physical layer of sender side is moved to physical layer of receiver side and then they are grouped into frames in the data link layer on the receiver side.



Layer No	Layer Name	Functionality	Data unit	Protocols
7	Application Layer	Helps in identifying the client and synchronizing communication.	Message	SMTP
6	Presentation Layer	Data from the application layer is extracted and manipulated in the required format for transmission.	Message	JPEG, MPEG, GIF
5	Session Layer	Establishes Connection and maintenance, Ensures Authentication, and Ensures security.	Message (or encrypted message)	Gateway
4	Transport Layer	Take Service from Network Layer and provide it to the Application Layer.	Segment	Firewall
3	Network Layer	Transmission of data from one host to another, located in different networks.	Packet	Router
2	Data Link Layer	Node to Node Delivery of Message.	Frame	Switch, Bridge
1	Physical Layer	Establishing Physical connections	Bits	Hub, Repeater, Modem, Cables

What is the Flow of Data in OSI Model?

When we transfer information from one device to another, it travels through 7 layers of OSI model. First data travels down through 7 layers from the sender's end and then climbs back 7 layers on the receiver's end.

Let's look at it with an Example:

Luffy sends an e-mail to his friend Zoro.

Step 1: Luffy interacts with e-mail application like **Gmail, outlook**, etc. Writes his email to send. (This happens in **Layer 7: Application layer**)

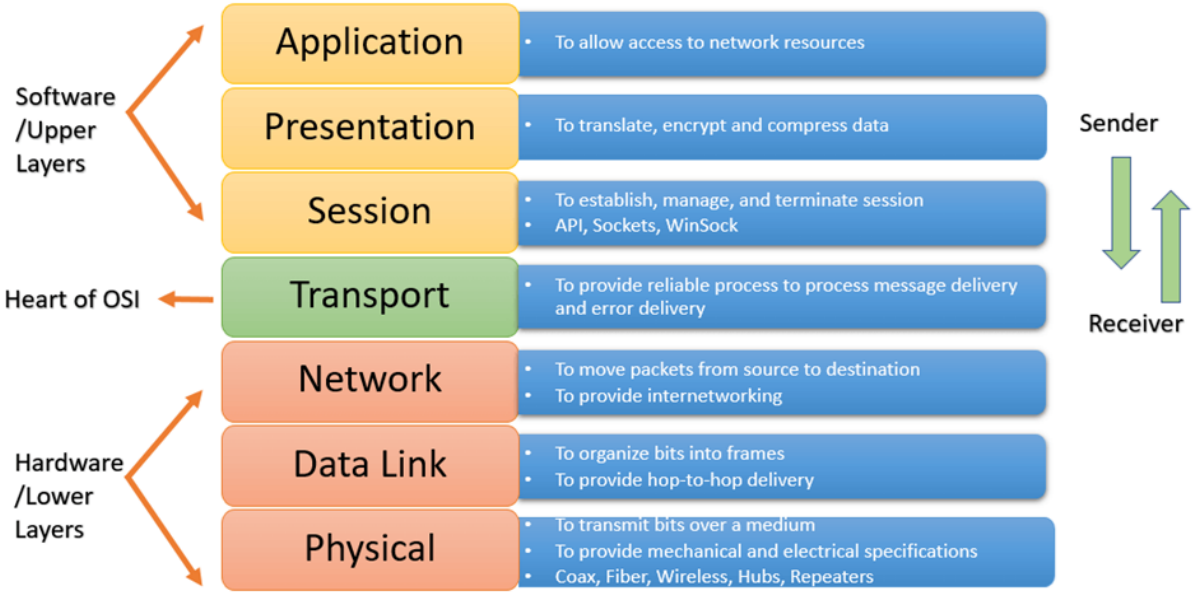
Step 2: Mail application prepares for data transmission like encrypting data and formatting it for transmission. (This happens in **Layer 6: Presentation Layer**)

Step 3: There is a connection established between the sender and receiver on the internet. (This happens in **Layer 5: Session Layer**)

Step 4: Email data is broken into smaller segments. It adds sequence number and error-checking information to maintain the reliability of the information. (This happens in **Layer 4: Transport Layer**)

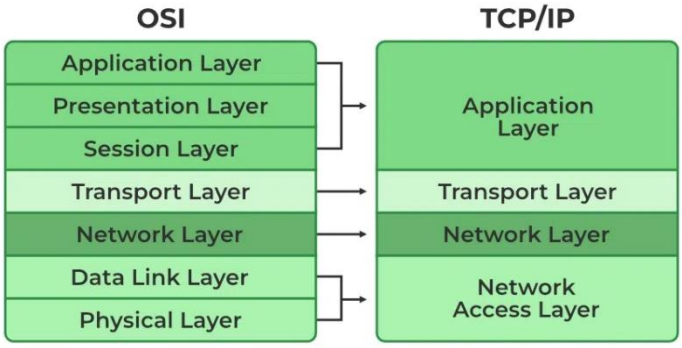
Step 5: Addressing of packets is done in order to find the best route for transfer. (This happens in **Layer 3: Network Layer**)
Step 6: Data packets are encapsulated into frames, then MAC address is added for local devices and then it checks for error using error detection. (This happens in **Layer 2: Data Link Layer**)
Step 7: Lastly Frames are transmitted in the form of electrical/ optical signals over a physical network medium like ethernet cable or WiFi.
After the email reaches the receiver i.e. Zoro, the process will reverse and decrypt the e-mail content. At last, the email will be shown on Zoro's email client.

Overview of OSI model:

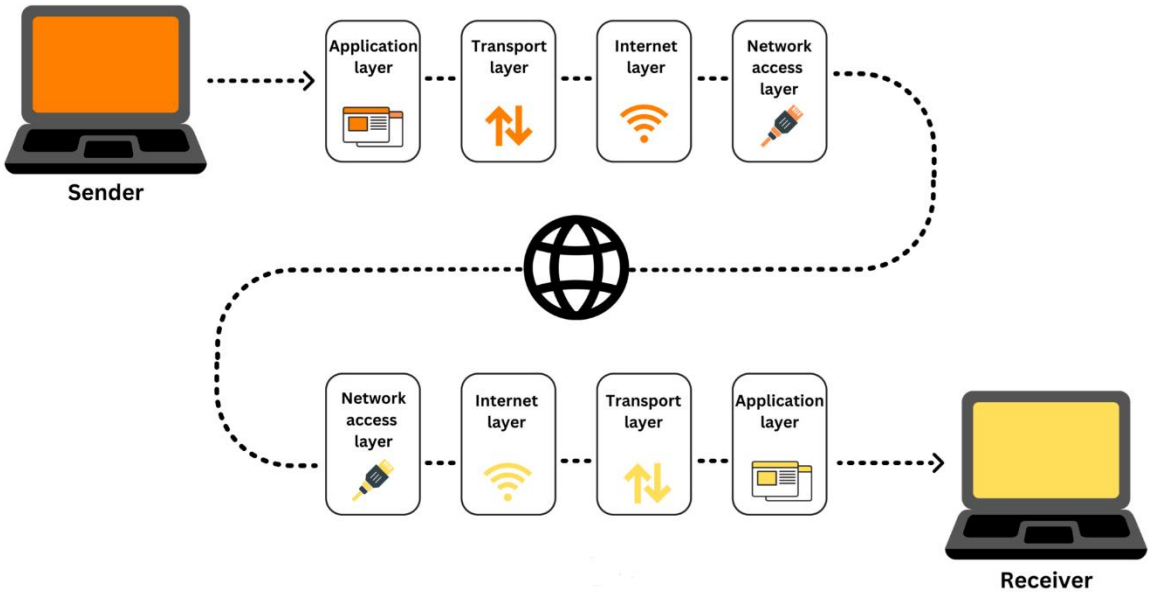


Till now you have seen OSI model and its layers, their services and functionalities in detail. Now lets discuss about new version of Network model that is used now a days i.e., TCP/IP model.

TCP / IP Model



- The OSI Model we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.
- **TCP/IP** was designed and developed by the Department of Defence (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.
- Whenever we want to send something over the internet using the TCP/IP Model, the TCP/IP Model divides the data into packets at the sender's end and the same packets have to be recombined at the receiver's end to form the same data, and this thing happens to maintain the accuracy of the data.
- TCP/IP model divides the data into a 4-layer procedure, where the data first go into this layer in one order and again in reverse order to get organized in the same way at the receiver's end as shown below.



Lets discuss about each layer in detail.

1. Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.

- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

2. Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Example:

Imagine that you are using a computer to send an email to a friend. When you click "send," the email is broken down into smaller packets of data, which are then sent to the Internet Layer for routing. The Internet Layer assigns an IP address to each packet and uses routing tables to determine the best route for the packet to take to reach its destination. The packet is then forwarded to the next hop on its route until it reaches its destination. When all of the packets have been delivered, your friend's computer can reassemble them into the original email message.

In this example, the Internet Layer plays a crucial role in delivering the email from your computer to your friend's computer. It uses IP addresses and routing tables to determine the best route for the packets to take, and it ensures that the packets are delivered to the correct destination. Without the Internet Layer, it would not be possible to send data across the Internet.

3. Transport Layer

The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error. End-to-end communication is referred to as such.

4. Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.

- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.

What is difference between TCP and IP?

- TCP and IP are two different computer network protocols. Each function in the data transmission process distinguishes TCP (Transmission Control Protocol) from IP (Internet Protocol). Using IP, you may find out where data is sent (your device has an IP address). Once that IP address has been discovered, TCP guarantees accurate data delivery. The pair make up the TCP/IP protocol suite.

Comparison between OSI and TCP/IP Models

Parameters	OSI Model	TCP/IP Model
Full Form	OSI stands for Open Systems Interconnection.	TCP/IP stands for Transmission Control Protocol/Internet Protocol.
Layers	It has 7 layers.	It has 4 layers.
Usage	It is low in usage.	It is mostly used.
Approach	It is vertically approached.	It is horizontally approached.
Delivery	Delivery of the package is guaranteed in OSI Model.	Delivery of the package is not guaranteed in TCP/IP Model.
Replacement	Replacement of tools and changes can easily be done in this model.	Replacing the tools is not easy as it is in OSI Model.
Reliability	It is less reliable than TCP/IP Model.	It is more reliable than OSI Model.

Lets know about the most important topic of this chapter i.e., protocols.

Protocols

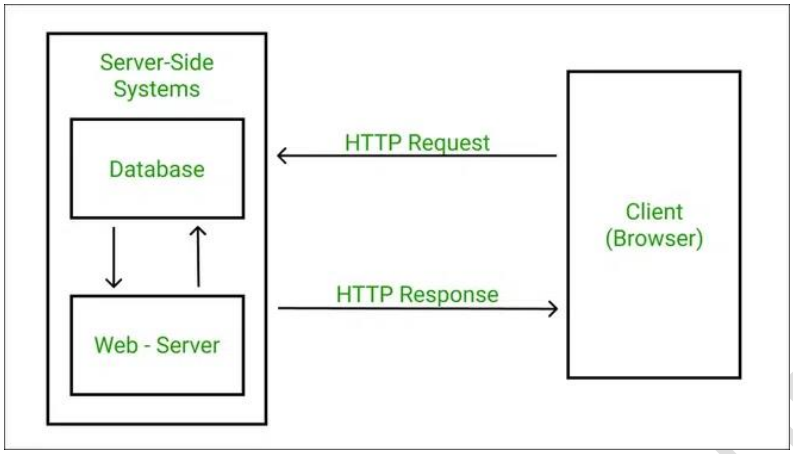
TCP/IP	OSI Model	Protocols
Application Layer	Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP,POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
	Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
	Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	Transport Layer	TCP, UDP
Internet Layer	Network Layer	ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP
Link Layer	Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
	Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi

Lets discuss about important protocols of TCP/IP model in detail.

1.HTTP

- HTTP stands for **HyperText Transfer Protocol.**
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

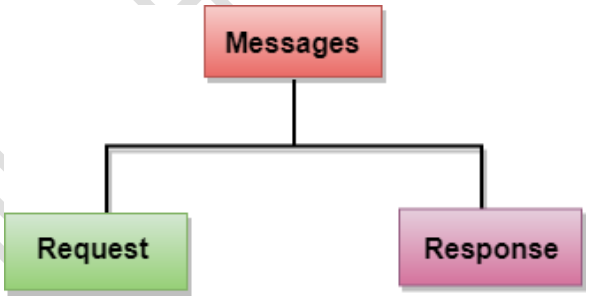
HTTP Transactions



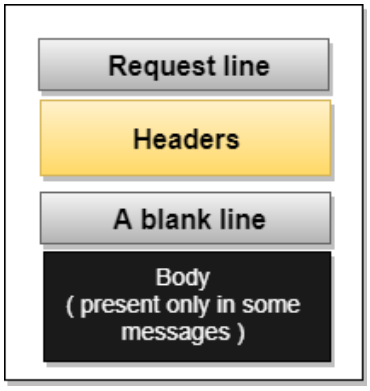
The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

Messages

HTTP messages are of two types: request and response. Both the message types follow the same message format.



Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.



Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.

2.HTTPS

HTTPS (Hypertext Transfer Protocol Secure) is an extension of HTTP (Hypertext Transfer Protocol) that provides secure communication over a computer network, typically the Internet. It is widely used to protect sensitive transactions like online banking and shopping order forms.

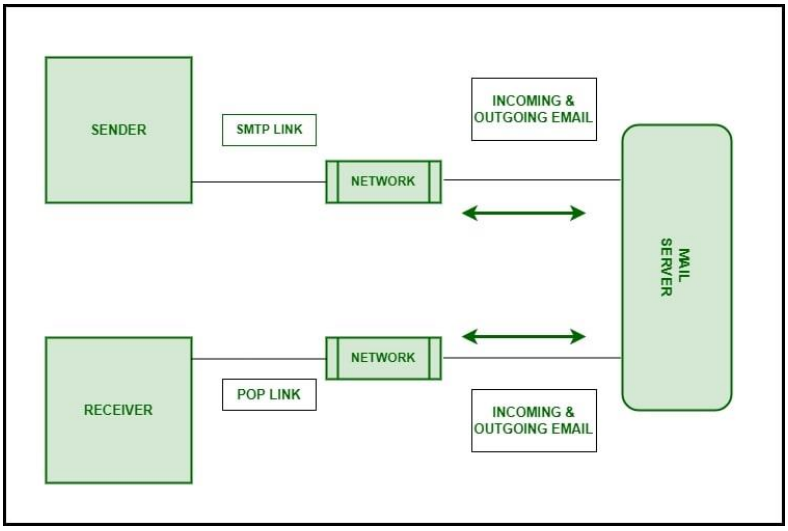
3.SMTP

The Simple Mail Transfer Protocol (SMTP) is a technical standard for transmitting electronic mail (email) over a network. Like other networking protocols, SMTP allows computers and servers to exchange data regardless of their underlying hardware or software.

Working of SMTP

Below mentioned are the steps of the working of SMTP [Simple Mail Transfer Protocol].

- **Communication between the sender and the receiver:** The sender's user agent prepares the message and sends it to the MTA. The MTA's responsibility is to transfer the mail across the network to the receiver's MTA. To send mail, a system must have a client MTA, and to receive mail, a system must have a server MTA.
- **Sending Emails:** Mail is sent by a series of request and response messages between the client and the server. The message which is sent across consists of a header and a body. A null line is used to terminate the mail header and everything after the null line is considered the body of the message, which is a sequence of ASCII characters. The message body contains the actual information read by the receipt.
- **Receiving Emails:** The user agent on the server-side checks the mailboxes at a particular time of intervals. If any information is received, it informs the user about the mail. When the user tries to read the mail it displays a list of emails with a short description of each mail in the mailbox. By selecting any of the mail users can view its contents on the terminal.

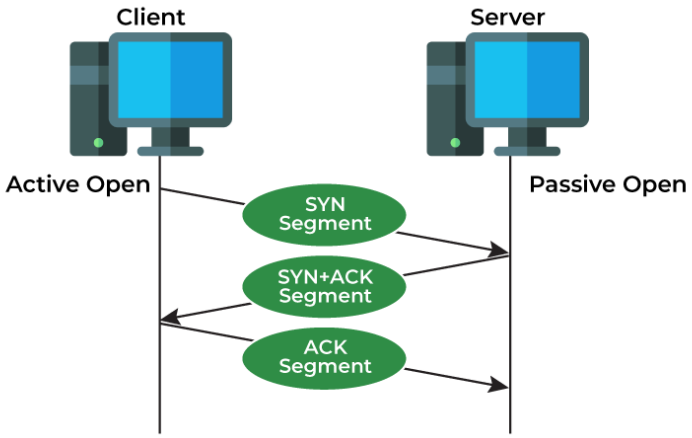


Some SMTP Commands

- **HELO:** Identifies the client to the server, fully qualified domain name, only sent once per session
- **MAIL:** Initiate a message transfer, the fully qualified domain of the originator
- **RCPT:** Follows MAIL, identifies an addressee, typically the fully qualified name of the addressee, and for multiple addressees use one RCPT for each addressee
- **DATA:** Send data line by line.

4.TCP Protocol

TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.



Features of TCP

- TCP keeps track of the segments being transmitted or received by assigning numbers to every single one of them.
- Flow control limits the rate at which a sender transfers data. This is done to ensure reliable delivery.
- TCP implements an error control mechanism for reliable data transfer.
- TCP takes into account the level of congestion in the network.

Advantages of TCP

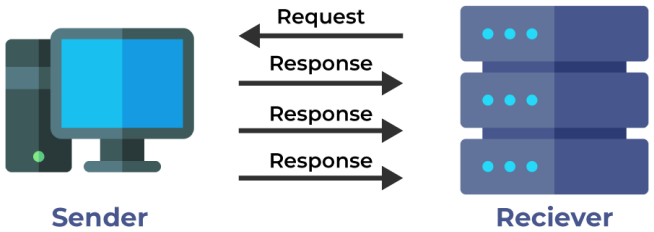
- It is reliable for maintaining a connection between Sender and Receiver.
- It is responsible for sending data in a particular sequence.
- Its operations are not dependent on OS.
- It allows and supports many routing protocols.
- It can reduce the speed of data based on the speed of the receiver.

Disadvantages of TCP

- It is slower than UDP and it takes more bandwidth.
- Slower upon starting of transfer of a file.
- Not suitable for LAN and PAN Networks.
- It does not have a multicast or broadcast category.
- It does not load the whole page if a single data of the page is missing.

5.User Datagram Protocol (UDP)

User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as the UDP/IP suite. Unlike TCP, it is an unreliable and connectionless protocol. So, there is no need to establish a connection before data transfer. The UDP helps to establish low-latency and loss-tolerating connections establish over the network. The UDP enables process-to-process communication.



Features of UDP

- Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control.
- It is a suitable protocol for multicasting as UDP supports packet switching.
- UDP is used for some routing update protocols like RIP(Routing Information Protocol).
- Normally used for real-time applications which can not tolerate uneven delays between sections of a received message.

Advantages of UDP

- It does not require any connection for sending or receiving data.
- Broadcast and Multicast are available in UDP.
- UDP can operate on a large range of networks.
- UDP has live and real-time data.
- UDP can deliver data if all the components of the data are not complete.

Disadvantages of UDP

- We can not have any way to acknowledge the successful transfer of data.
- UDP cannot have the mechanism to track the sequence of data.
- UDP is connectionless, and due to this, it is unreliable to transfer data.
- In case of a Collision, UDP packets are dropped by Routers in comparison to TCP.
- UDP can drop packets in case of detection of errors.

3 INTRODUCTION TO NETWORK SECURITY

What is Network Security?

Network Security is the process of taking measures to protect the systems and confidential data from unauthorized access.

The unauthorized access are those people who try to steal , tamper the data for their benefits.

These people are often referred to as hackers.

Hackers can be of two types:

White hat hackers:

White hat hackers are authorized people who work under the organization. They try to protect the systems and confidential data of organizations to prevent from security attacks. They also use some measures to protect the systems and data which is confidential hence they are termed as hackers. But they are good people and strive for good works and they don't harm individuals or a group.

Black hat hackers:

Black hat hackers are unauthorized people who do illegal works by hacking the systems and data by using various security attacks and try to steal confidential information. They are intelligent people and well trained professionals in illegal hacking.

CIA Triad

CIA Triad stands for three elements: Confidentiality, Integrity, Availability.

For any organization or individual the main goal is protecting the systems or data in terms of ensuring Confidentiality, Integrity, and Availability.

The objective of Cybersecurity is to protect information from being stolen, compromised or attacked. Cybersecurity can be measured by at least one of three goals-

1. Protect the confidentiality of data.
2. Preserve the integrity of data.
3. Promote the availability of data for authorized users.

Lets discuss about each term in detail.

Confidentiality:

Confidentiality refers to protecting the data from unauthorized access. It means the data can be only accessed by its owner and it shouldn't be accessed by anu other people.

Methods to ensure Confidentiality are:

- **Encryption**

  Encryption is a method of transforming information to make it unreadable for unauthorized users by using an algorithm. The transformation of data uses a secret key (an encryption key) so that the transformed data can only be read by using another secret key (decryption key). It protects sensitive data such as credit card numbers by encoding and transforming data into unreadable cipher text. This encrypted data can only be read by decrypting it. Asymmetric-key and symmetric-key are the two primary types of encryption.

- **Access Control**

  Access control defines rules and policies for limiting access to a system or to physical or virtual resources. It is a process by which users are granted access and certain privileges to systems, resources or information. In access control systems, users need to present credentials before they can be granted access such as a person's name or a computer's serial number. In physical systems, these credentials may come in many forms, but credentials that can't be transferred provide the most security.

- **Authentication**

  It is a method of providing security to the systems and sensitive data by providing an extra layer of security to ensure user credentials like username and password providing the limited access control to the users from unauthorized access.

- **Authorization**

  Authorization is a security mechanism which gives permission to do or have something. It is used to determine a person or system is allowed access to resources, based on an access control policy, including computer programs, files, services, data and application features. It is normally preceded by authentication for user identity verification. System administrators are typically assigned permission levels covering all system and user resources. During authorization, a system verifies an authenticated user's access rules and either grants or refuses resource access.

- **Physical Security**

  Physical security describes measures designed to deny the unauthorized access of IT assets like facilities, equipment, personnel, resources and other

properties from damage. It protects these assets from physical threats including theft, vandalism, fire and natural disasters.

Integrity:

Integrity refers to the methods for ensuring that data is real, accurate, and safeguarded from unauthorized user modification. It is the property that the information has not been altered in an unauthorized way, and that the source of the information is genuine.

Availability:

Availability is the property in which information is accessible and modifiable in a timely fashion by those authorized to do so. It is the guarantee of reliable and constant access to our sensitive data by authorized people.

Till now we have discussed types of hackers and CIA triad. Now lets see about OSI security Architecture.

OSI Security Architecture

The OSI (Open Systems Interconnection) Security Architecture defines a systematic approach to providing security at each layer. It defines security services and security mechanisms that can be used at each of the seven layers of the OSI model to provide security for data transmitted over a network. These security services and mechanisms help to ensure the confidentiality, integrity, and availability of the data.

OSI layer focus on three concepts:

1. Security Attacks
2. Security mechanisms
3. Security Services

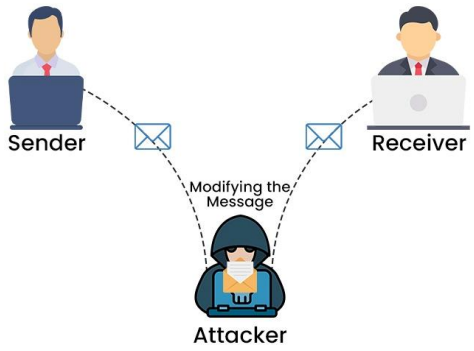
Security Attacks:

Security Attack refers to an attempt by a person or an entity to gain unauthorized access to compromise the security of a system , network or data.

These are defined as the actions that put at risk an organization safety.

They are further classified into 2 types:

a) Active Attack



Active attacks refers to type of attacks in which the attacker actively alter system, network or data and make modifications in the data.

Active attackers are typically focussed on causing damage.

Here the sender and receiver have no clue that message is modified by some third party intruder. So the receiver is not aware that the data / message which was received was sent by sender or not.

Active attacks are classified into 2 types:

1. Masquerade

Masquerade is a type of attack in which the attacker pretends to be an authentic sender or legitimate source to gain access to confidential information such as credit card details and many more.

Common Security attack under masquerade is Phishing which is the most dangerous attack and common now a days. The attackers send the links by online advertisements in authorized third party apps or web applications or by sending message to the people by pretending himself as a legitimate source.

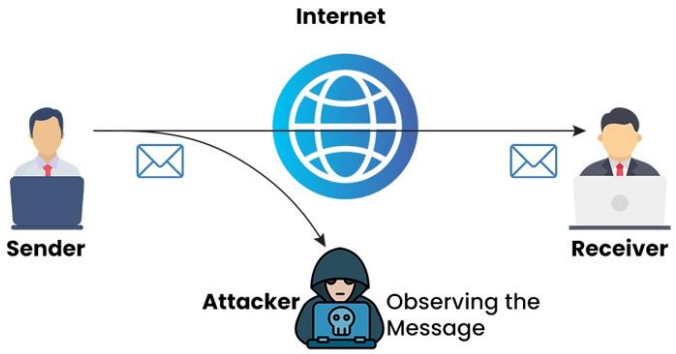
People think it as trusted one and they open it and enter their details and they their credit details are compromised and they can be accessed by attackers any time they want.

2. Replay

The attacker in the middle of the sender and receiver tries to send the messages continuously to the receiver to hang or reduce the performance of the system.

DDoS attack fall under Replay security attacks which involve attacker sending a large volumes of traffic to a system or devices or a network in an attempt to make the server unavailable to legitimate users.

b) Passive attack



Attacks in which a third-party intruder tries to access the message/ content/ data being shared by the sender and receiver by keeping a close watch on the transmission or eave-dropping the transmission is called Passive Attacks. These types of attacks involve the attacker observing or monitoring system, network, or device activity without actively disrupting or altering it. Passive attacks are typically focused on gathering information or intelligence, rather than causing damage or disruption.

Here, both the sender and receiver have no clue that their message/ data is accessible to some third-party intruder. The message/ data transmitted remains in its usual form without any deviation from its usual behaviour. This makes passive attacks very risky as there is no information provided about the attack happening in the communication process. One way to prevent passive attacks is to encrypt the message/data that needs to be transmitted, this will prevent third-party intruders from using the information though it would be accessible to them.

Passive attacks are further divided into two parts based on their behavior:

Eavesdropping: This involves the attacker intercepting and listening to communications between two or more parties without their knowledge or consent. Eavesdropping can be performed using a variety of techniques, such as packet sniffing, or man-in-the-middle attacks.

Traffic analysis: This involves the attacker analyzing network traffic patterns and metadata to gather information about the system, network, or device. Here the intruder can't read the message but only understand the pattern and length of encryption. Traffic analysis can be performed using a variety of techniques, such as network flow analysis, or protocol analysis.

Security Services

It is a processing or communication service that is provided by as system to give a specific kind of protection to system resources, security services implement security policies and are implemented by security mechanisms.

There are various services of network security which are as follows –

Message Confidentiality

Message confidentiality or privacy means that the sender and the receiver expect confidentiality. The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage. When a customer communicates with her bank, she expects that the communication is totally confidential.

Message Integrity

Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally nor maliciously. As more and more monetary exchanges occur over the Internet, integrity is crucial.

For example, it would be disastrous if a request for transferring 100changedtoarequestfor

10,000 or $100,000. The integrity of the message must be preserved in secure communication.

Message Authentication

Message authentication is a service beyond message integrity. In message authentication, the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.

Message Nonrepudiation

Message nonrepudiation means that a sender must not be able to deny sending a message that he or she, in fact, did send. The burden of proof falls on the receiver.

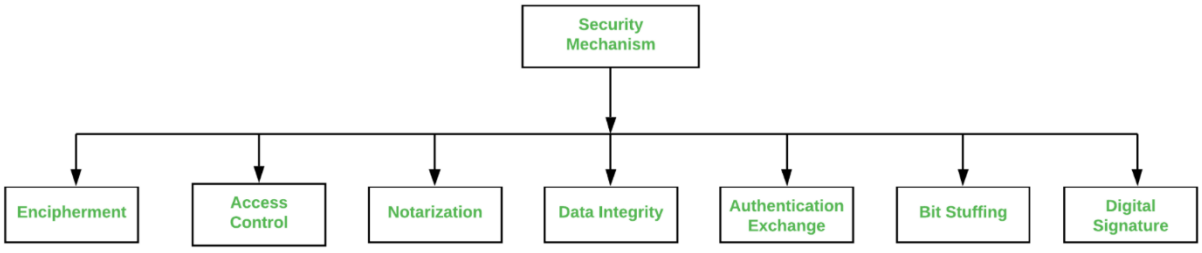
For example, when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction.

Entity Authentication
In entity authentication (or user identification), the entity or user is verified prior to access to the system resources (files, for example).

For example, a student who needs to access her university resources needs to be authenticated during the logging process. This is to protect the interests of the university and the student.

Security Mechanisms

Network Security is field in computer technology that deals with ensuring security of computer network infrastructure. As the network is very necessary for sharing of information whether it is at hardware level such as printer, scanner, or at software level. Therefore security mechanism can also be termed as is set of processes that deal with recovery from security attack. Various mechanisms are designed to recover from these specific attacks at various protocol layers.



Types of Security Mechanism are :

1. **Encipherment :**
   This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved by two famous techniques named Cryptography and Encipherment. Level of data encryption is dependent on the algorithm used for encipherment.

2. **Access Control :**
   This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.

3. **Notarization :**
   This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.

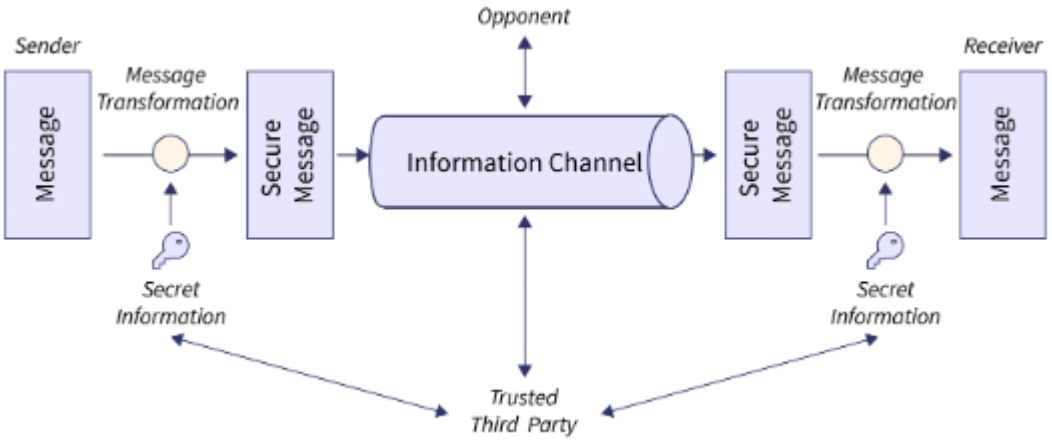
4. **Data Integrity :**
   This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.

5. **Authentication exchange :**
   This security mechanism deals with identity to be known in communication. This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not.

6. **Bit stuffing :**
   This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.

7. **Digital Signature :**
   This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential but sender's identity is to be notified.

Network Security Model



Network security refers to the defensive measures and controls set in place to protect a computer network's integrity and confidential data from unauthorised access, misuse, malware and external threats. It focuses on securing the network infrastructure, including all connected devices, applications, servers, data storage systems, and the entire network's traffic flow.

It includes firewalls that filter incoming and outgoing traffic, antivirus software to detect and block malware, encryption to scramble and unscramble data as required, and access control mechanisms such as credential requirements, permissions levels, and device and user policies.

Robust network security measures safeguard network availability and provide layered defences against a range of cyber threats that can exploit vulnerabilities to breach networks and steal critical data.

A network security model in computer networks refers to the structured defensive mechanisms and protocols implemented to protect the integrity, confidentiality and availability of data transmitted between devices over an interconnected system of networks.

Its core purpose in computer network security (CNS) is to transform plain text data into encrypted ciphertext before sending it over the vulnerable network channel so that potential attackers cannot decipher or make sense of the information.

This is achieved by applying a cryptographic algorithm powered by a secret key known only to the communicating parties in the network security model in CNS. The

encrypted data gets transmitted and later decrypted at the receiving end with the same secret key.

An effective network security model in computer networks has the following key aspects:

1. An encryption algorithm encodes plaintext into ciphertext and decodes cypher text back into plain text. The strength of the algorithm relies on its ability to withstand cracking attempts by adversaries.
2. Secure generation, distribution and usage of a secret key exclusively shared between the communicating parties over the computer network. A trusted third party facilitates the secret key exchange in the network security model in CNS.
3. Communication protocols enable the application of the chosen encryption powered by the secretly shared key to deliver security services like confidentiality, integrity and authentication of the sender.

Additionally, a network access security model in CNS focuses on protecting computer systems and network resources from unauthorised access and cyber threats that can damage software, steal data and disable services.

Intrusion detection systems, firewalls and antivirus programs are some common controls that can be found in network security models in computer networks.

What are the Components of a Network Security Model?

A strong network security model consists of layered components working together to safeguard the confidentiality, integrity and availability of systems and data. The key components that comprise an effective network security model include:

- **Firewalls:** Firewalls monitor all incoming and outgoing network traffic and stop viruses, hackers and DDoS assaults depending on security standards. Firewalls provide perimeter security through traffic filtering and block unauthorised access attempts.
- **Intrusion Prevention Systems (IPS):** IPS monitors traffic patterns to detect malicious activity, policy violations, vulnerability exploits or threats that firewalls can miss. It can analyse packet payloads and block attacks in real-time before the damage is done.

- **VPN:** Virtual Private Networks (VPNs) enable secure remote connections for teleworkers and road warriors and connect distributed sites. VPNs create encrypted tunnels across public networks to ensure data confidentiality and integrity.
- **Access Controls:** Access controls regulate access to networks and systems by implementing strict authentication, authorisation and accounting. Methods like multi-factor authentication, role-based access and device compliance enforcement ensure appropriate resource access.
- **Data Encryption:** Encrypting data secures sensitive information from unauthorised access or modification attempts. It scrambles data using encryption algorithms and keys, ensuring only parties with decryption keys can read it.
- **Endpoint Security:** Hardening endpoints via antivirus software, strict access controls, and patching helps prevent malware, unauthorised access and attacks targeting end users. It blocks threats from entering networks through endpoints.
- **Network Monitoring:** Continuous monitoring using SIEM systems collects and analyses network activity logs to rapidly detect potential attacks and anomalous behaviour indicative of a breach. It enables threat visibility.
- **Incident Response Plans:** Despite defences, breaches can happen, so incident response plans prepare organisations to respond appropriately to security events. Playbooks detailing roles, responsibilities and actions are essential for effective breach containment.

A layered model covering people, processes and technology focused on prevention, timely threat detection, and minimising breach impacts provides in-depth defence against cyber attacks that leverage network access.

4 CRYPTOGRAPHY

Definition

Cryptography is a technique of securing communication by converting plain text to cipher text. It involves various algorithms and protocols to ensure data

Plain text(Readable format):

Plain text is the original message or data that is not modified and can be read easily for understanding the purpose of sending message.

Cipher text(Non-Readable format):

Cipher text is the modified text that can be converted using various cipher algorithms which cannot be understand by anyone even hackers too.

Why do we use cipher text:

To protect the confidentiality of the message or data that is sent must be protected from the intruder in the middle. Hence we modify the data using secret keys.

What are secret keys?

Secret keys are the keys that can be used to convert plain text to cipher text and can be converted from cipher text to plain text again at receiver side.

Features Of Cryptography

1. **Confidentiality:**
   Information can only be accessed by the person for whom it is intended and no other person except him can access it.

2. **Integrity:**
   Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

3. **Non-repudiation:**
   The creator/sender of information cannot deny his intention to send information at a later stage.

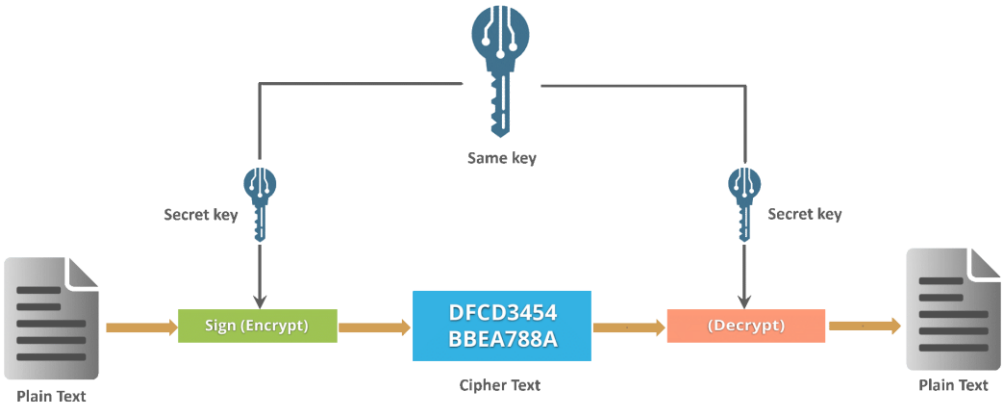
4. **Authentication:**
   The identities of the sender and receiver are confirmed. As well destination/origin of the information is confirmed.

5. **Interoperability:**
   Cryptography allows for secure communication between different systems and platforms.

6. **Adaptability:**
   Cryptography continuously evolves to stay ahead of security threats and technological advancements.

Types of Cryptography

1. Symmetric key Cryptography
   Symmetric key cryptography is a type of cryptography where same key is used for both encrypt and decrypt messages.



Symmetric key cryptography is faster and simpler but the problem is that sender and receiver have to somehow exchange the keys securely. The most popular symmetric key cryptography are Data Encryption Systems(DES) and Advanced Encryption systems(AES).

2. Asymmetric Key Cryptography

In Asymmetric key both sender and receiver use distinct keys for encryption and decryption. The asymmetric keys are public keys and private keys. A receiver's public key is used for encryption and a receiver's private key is used for decryption. Public keys and Private keys are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows his private key. The most popular asymmetric key cryptography algorithm is the RSA algorithm.

Block Cipher

Block ciphers are built in the Feistel cipher structure. Block cipher has a specific number of rounds and keys for generating ciphertext.Block cipher is a type of encryption algorithm that processes fixed-size blocks of data, usually 64 or 128 bits, to produce ciphertext. The design of a block cipher involves several important principles to ensure the security and efficiency of the algorithm. Some of these principles are:

1. **Number of Rounds –** The number of Rounds is regularly considered in design criteria, it just reflects the number of rounds to be suitable for an algorithm to make it more complex, in DES we have 16 rounds ensuring it to be more secure while in AES we have 10 rounds which makes it more secure.
2. **Design of function F –** The core part of the Feistel Block cipher structure is the Round Function. The complexity of cryptanalysis can be derived from the Round function i.e. the increasing level of complexity for the round function would be greatly contributing to an increase in complexity. To increase the complexity of the round function, the avalanche effect is also included in the round function, as the change of a single bit in plain text would produce a mischievous output due to the presence of avalanche effect.
3. **Confusion and Diffusion:** The cipher should provide confusion and diffusion to make it difficult for an attacker to determine the relationship between the plaintext and ciphertext. Confusion means that the ciphertext should be a complex function of the key and plaintext, making it difficult to guess the key. Diffusion means that a small change in the plaintext should cause a significant change in the ciphertext, which makes it difficult to analyze the encryption pattern.
4. **Key Size:** The key size should be large enough to prevent brute-force attacks. A larger key size means that there are more possible keys, making it harder for an attacker to guess the correct one. A key size of 128 bits is considered to be secure for most applications.
5. **Key Schedule:** The key schedule should be designed carefully to ensure that the keys used for encryption are independent and unpredictable. The key schedule should also resist attacks that exploit weak keys or key-dependent properties of the cipher.
6. **Block Size:** The block size should be large enough to prevent attacks that exploit statistical patterns in the plaintext. A block size of 128 bits is generally considered to be secure for most applications.
7. **Non-linearity:** The S-box used in the cipher should be non-linear to provide confusion. A linear S-box is vulnerable to attacks that exploit the linear properties of the cipher.
8. **Avalanche Effect:** The cipher should exhibit the avalanche effect, which means that a small change in the plaintext or key should cause a significant change in the ciphertext. This ensures that any change in the input results in a complete change in the output.
9. **Security Analysis:** The cipher should be analyzed for its security against various attacks such as differential cryptanalysis, linear cryptanalysis, and

brute-force attacks. The cipher should also be tested for its resistance to implementation attacks, such as side-channel attacks.

Overall, a good block cipher design should be resistant to various attacks, efficient, and easy to implement.

Block Cipher Algorithms

1)Data Encryption Standard

Data Encryption Standard (DES) is a block cipher with a 56-bit key length that has played a significant role in data security. Data encryption standard (DES) has been found vulnerable to very powerful attacks therefore, the popularity of DES has been found slightly on the decline. DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.

The basic idea is shown below:

We have mentioned that DES uses a 56-bit key. Actually, The initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

Figure - discording of every 8th bit of original key

Thus, the discarding of every 8th bit of the key produces a 56-bit key from the original 64-bit key.

DES is based on the two fundamental attributes of cryptography: substitution (also called confusion) and transposition (also called diffusion). DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition. Let us now discuss the broad-level steps in DES.

In the first step, the 64-bit plain text block is handed over to an initial Permutation (IP) function.

The initial permutation is performed on plain text.

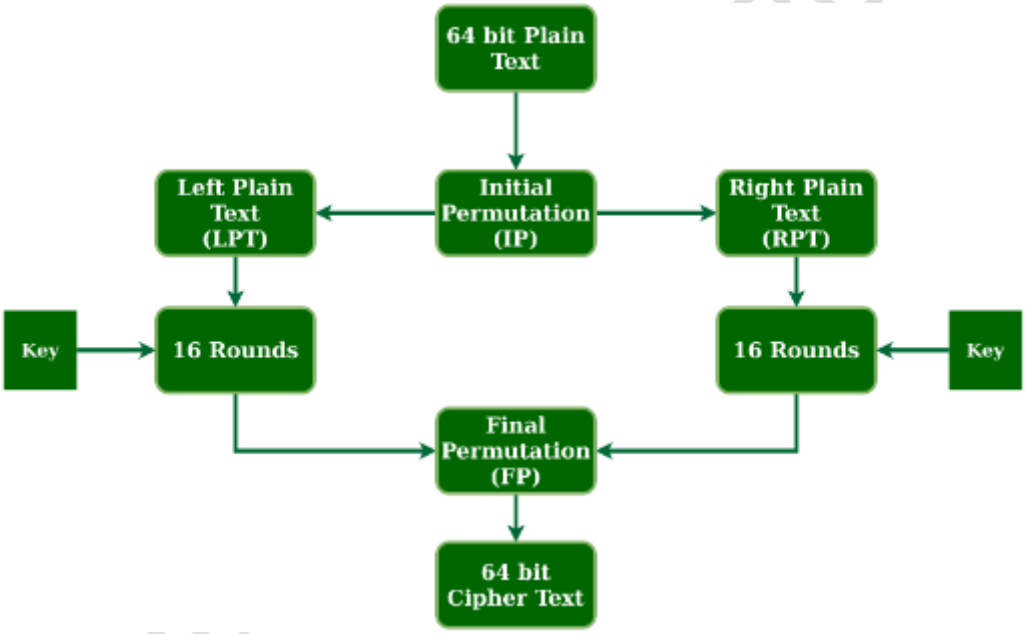
Next, the initial permutation (IP) produces two halves of the permuted block; saying Left Plain Text (LPT) and Right Plain Text (RPT).

Now each LPT and RPT go through 16 rounds of the encryption process.

In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block

The result of this process produces 64-bit ciphertext.

Steps in DES



Initial Permutation (IP)

As we have noted, the initial permutation (IP) happens only once and it happens before the first round. It suggests how the transposition in IP should proceed, as shown in the figure. For example, it says that the IP replaces the first bit of the original plain text block with the 58th bit of the original plain text, the second bit with the 50th bit of the original plain text block, and so on.

This is nothing but jugglery of bit positions of the original plain text block. the same rule applies to all the other bit positions shown in the figure.

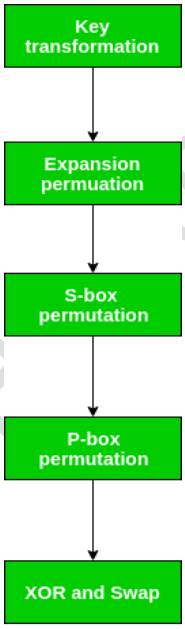
Initial Permutation table

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	33	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Figure - Initial permutation table

As we have noted after IP is done, the resulting 64-bit permuted text block is divided into two half blocks. Each half-block consists of 32 bits, and each of the 16 rounds, in turn, consists of the broad-level steps outlined in the figure.

Rounds in DES



Step 1: Key transformation

We have noted initial 64-bit key is transformed into a 56-bit key by discarding every 8th bit of the initial key. Thus, for each a 56-bit key is available. From this 56-bit key, a different 48-bit Sub Key is generated during each round using a process called key transformation. For this, the 56-bit key is divided into two halves, each of 28 bits. These halves are circularly shifted left by one or two positions, depending on the round.

For example: if the round numbers 1, 2, 9, or 16 the shift is done by only one position for other rounds, the circular shift is done by two positions. The number of key bits shifted per round is shown in the figure.

Number of key bits shifted per round

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
#key bits shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Figure - number of key bits shifted per round

After an appropriate shift, 48 of the 56 bits are selected. From the 48 we might obtain 64 or 56 bits based on requirement which helps us to recognize that this model is very versatile and can handle any range of requirements needed or provided. for selecting 48 of the 56 bits the table is shown in the figure given below. For instance, after the shift, bit number 14 moves to the first position, bit number 17 moves to the second position, and so on. If we observe the table , we will realize that it contains only 48-bit positions. Bit number 18 is discarded (we will not find it in the table), like 7 others, to reduce a 56-bit key to a 48-bit key. Since the key transformation process involves permutation as well as a selection of a 48-bit subset of the original 56-bit key it is called Compression Permutation.

Compression permutation

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Figure - compression permutation

Because of this compression permutation technique, a different subset of key bits is used in each round. That makes DES not easy to crack.

Step 2: Expansion Permutation

Recall that after the initial permutation, we had two 32-bit plain text areas called Left Plain Text(LPT) and Right Plain Text(RPT). During the expansion permutation, the RPT is expanded from 32 bits to 48 bits. Bits are permuted as well hence called expansion permutation. This happens as the 32-bit RPT is divided into 8 blocks, with each block consisting of 4 bits. Then, each 4-bit block of the previous step is then expanded to a corresponding 6-bit block, i.e., per 4-bit block, 2 more bits are added.

Division of 32 bit RPT into 8 bit blocks

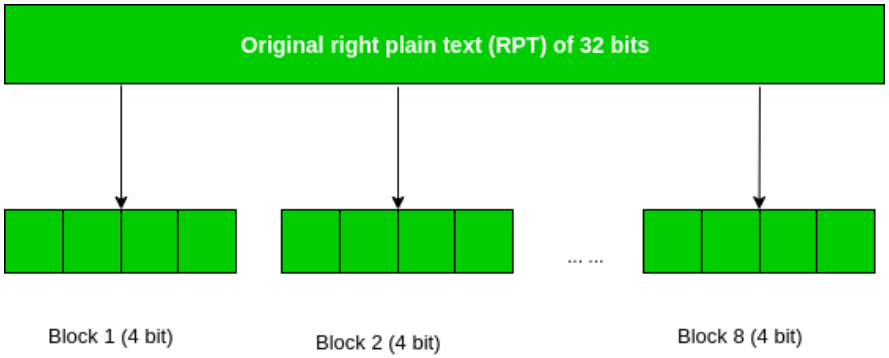


Figure - division of 32 bit RPT into 8 bit blocks

This process results in expansion as well as a permutation of the input bit while creating output. The key transformation process compresses the 56-bit key to 48 bits. Then the expansion permutation process expands the 32-bit RPT to 48-bits. Now the 48-bit key is XOR with 48-bit RPT and the resulting output is given to the next step, which is the S-Box substitution.

2) Advanced Encryption Standard

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.
Points to remember

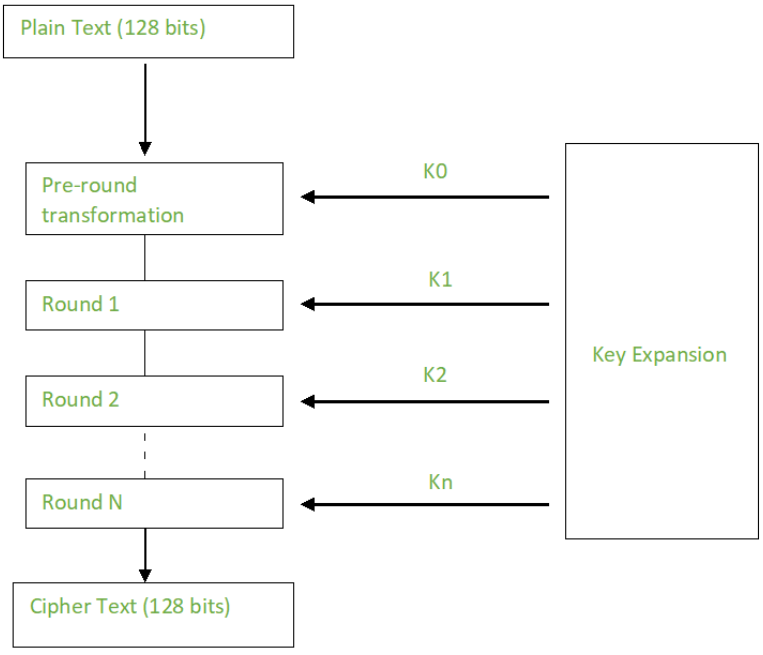
- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

Working of the cipher :
AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time. The number of rounds depends on the key length as follows :

- 128 bit key – 10 rounds
- 192 bit key – 12 rounds
- 256 bit key – 14 rounds

Creation of Round keys :
A Key Schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.



Encryption :
AES considers each block as a 16 byte (4 byte x 4 byte = 128) grid in a column major arrangement.
[b0 | b4 | b8 | b12 |
| b1 | b5 | b9 | b13 |
| b2 | b6 | b10| b14 |
| b3 | b7 | b11| b15]
Each round comprises of 4 steps :

- SubBytes
- ShiftRows
- MixColumns
- Add Round Key

The last round doesn't have the MixColumns round.

The SubBytes does the substitution and ShiftRows and MixColumns performs the permutation in the algorithm.

SubBytes :
This step implements the substitution.
In this step each byte is substituted by another byte. Its performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16 byte (4 x 4) matrix like before.

The next two steps implement the permutation.

ShiftRows :
This step is just as it sounds. Each row is shifted a particular number of times.

- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.

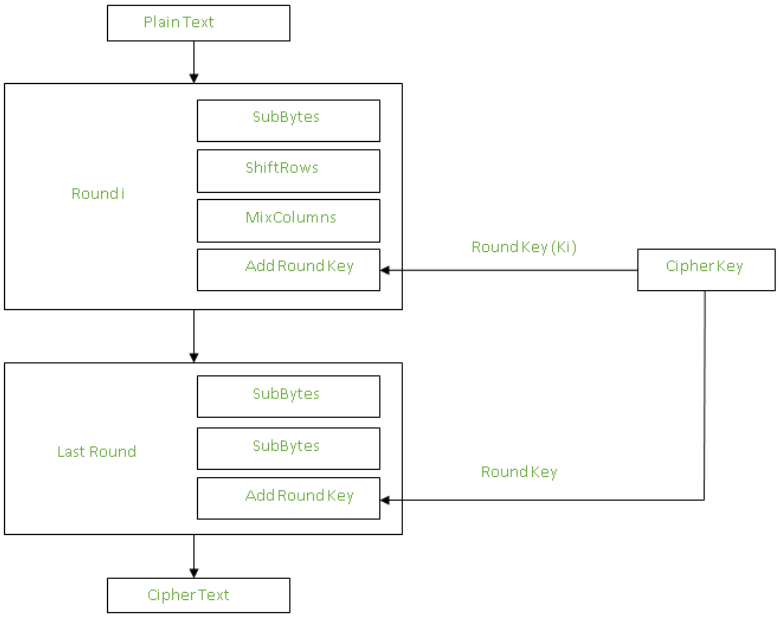
(A left circular shift is performed.)

[b0 | b1 | b2 | b3] [b0 | b1 | b2 | b3]
| b4 | b5 | b6 | b7 | -> | b5 | b6 | b7 | b4 |
| b8 | b9 | b10 | b11 | | b10 | b11 | b8 | b9 |
[b12 | b13 | b14 | b15] [b15 | b12 | b13 | b14]

MixColumns :
This step is basically a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.
This step is skipped in the last round.
[c0] [2 3 1 1] [b0]
| c1 | = | 1 2 3 1 | | b1 |
| c2 | | 1 1 2 3 | | b2 |
[c3] [3 1 1 2] [b3]

Add Round Keys :
Now the resultant output of the previous stage is XOR-ed with the corresponding

round key. Here, the 16 bytes is not considered as a grid but just as 128 bits of data.



After all these rounds 128 bits of encrypted data is given back as output. This process is repeated until all the data to be encrypted undergoes this process.

Decryption :
The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes.Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.
The stages of each round in decryption is as follows :

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

The decryption process is the encryption process done in reverse so i will explain the steps with notable differences.

Inverse MixColumns :
This step is similar to the MixColumns step in encryption, but differs in the matrix used to carry out the operation.

$$\begin{bmatrix} b0 \\ b1 \\ b2 \\ b3 \end{bmatrix} = \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix} \begin{bmatrix} c0 \\ c1 \\ c2 \\ c3 \end{bmatrix}$$

Inverse SubBytes :
Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.

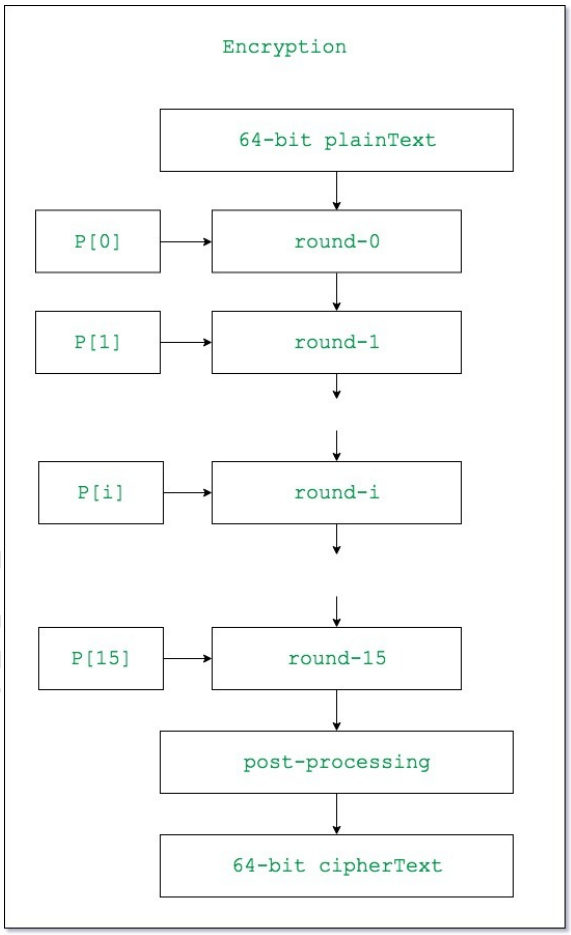
3)Blow fish Algorithm

Blowfish is an encryption technique designed by **Bruce Schneier** in 1993 as an alternative to DES Encryption Technique. It is significantly faster than DES and provides a good encryption rate with no effective cryptanalysis technique found to date. It is one of the first, secure block cyphers not subject to any patents and hence freely available for anyone to use. It is symmetric block cipher algorithm.

1. **blockSize**: 64-bits
2. **keySize**: 32-bits to 448-bits variable size
3. **number of subkeys**: 18 [P-array]
4. **number of rounds**: 16
5. **number of substitution boxes**: 4 [each having 512 entries of 32-bits each]

Blowfish Encryption Algorithm

The entire encryption process can be elaborated as:



Lets see each step one by one:

Step1: Generation of subkeys:

- 18 subkeys{P[0]…P[17]} are needed in both encryption as well as decryption process and the same subkeys are used for both the processes.

- These 18 subkeys are stored in a P-array with each array element being a 32-bit entry.
- It is initialized with the digits of pi(?).
- The hexadecimal representation of each of the subkeys is given by:

P[0] = "243f6a88"
P[1] = "85a308d3"
.
.
.
P[17] = "8979fb1b"

32-bit hexadecimal representation of initial values of sub-keys

P[0]	: 243f6a88	P[9]	: 38d01377
P[1]	: 85a308d3	P[10]	: be5466cf
P[2]	: 13198a2e	P[11]	: 34e90c6c
P[3]	: 03707344	P[12]	: c0ac29b7
P[4]	: a4093822	P[13]	: c97c50dd
P[5]	: 299f31d0	P[14]	: 3f84d5b5
P[6]	: 082efa98	P[15]	: b5470917
P[7]	: ec4e6c89	P[16]	: 9216d5d9
P[8]	: 452821e6	P[17]	: 8979fb1b

- Now each of the subkey is changed with respect to the input key as:

P[0] = P[0] xor 1st 32-bits of input key
P[1] = P[1] xor 2nd 32-bits of input key
.
.
.
P[i] = P[i] xor (i+1)th 32-bits of input key
(roll over to 1st 32-bits depending on the key length)
.
.
.
P[17] = P[17] xor 18th 32-bits of input key
(roll over to 1st 32-bits depending on key length)
The resultant P-array holds 18 subkeys that is used during the entire encryption process.

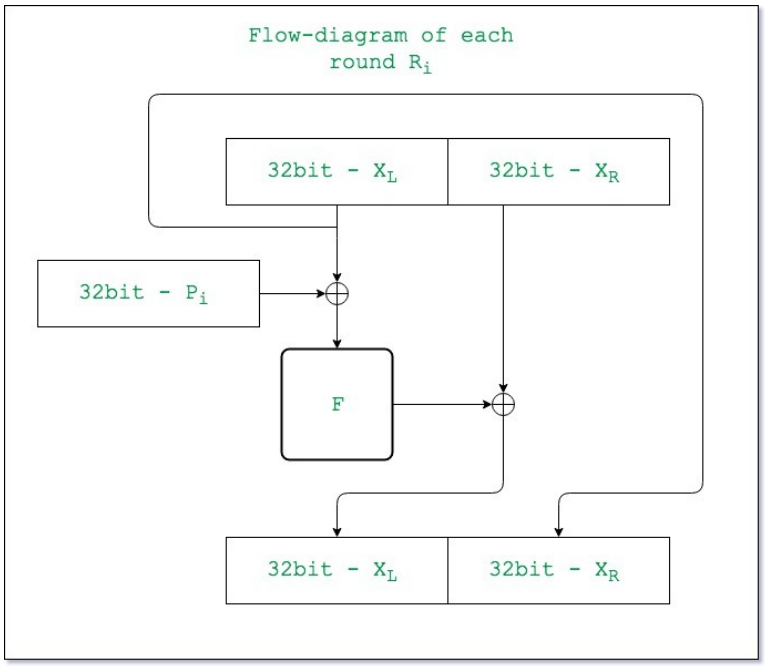
Step2: initialise Substitution Boxes:

- 4 Substitution boxes(S-boxes) are needed{S[0]…S[4]} in both encryption aswell as decryption process with each S-box having 256 entries{S[i][0]…S[i][255], 0&lei&le4} where each entry is 32-bit.

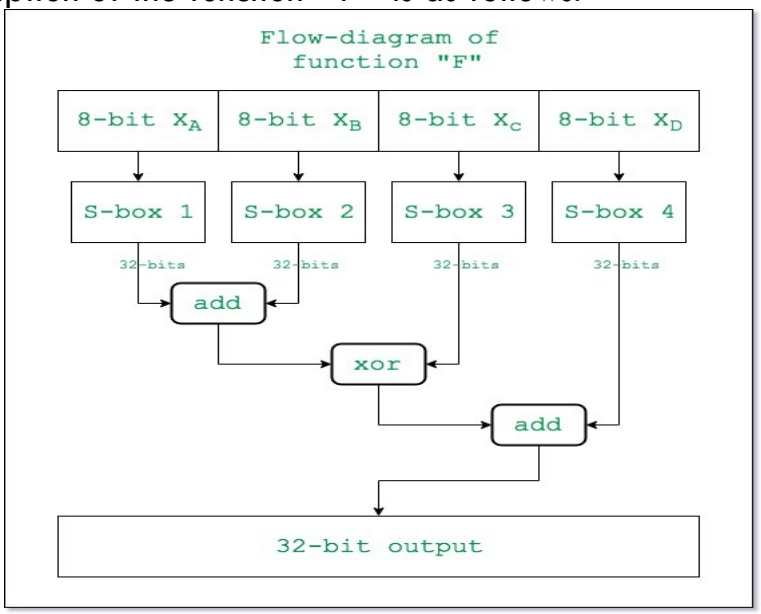
- It is initialized with the digits of pi(?) after initializing the P-array. You may find the **s-boxes** in here!

Step3: Encryption:

- The encryption function consists of two parts:
  a. Rounds: The encryption consists of 16 rounds with each round(Ri) taking inputs the plainText(P.T.) from previous round and corresponding subkey(Pi). The description of each round is as follows:

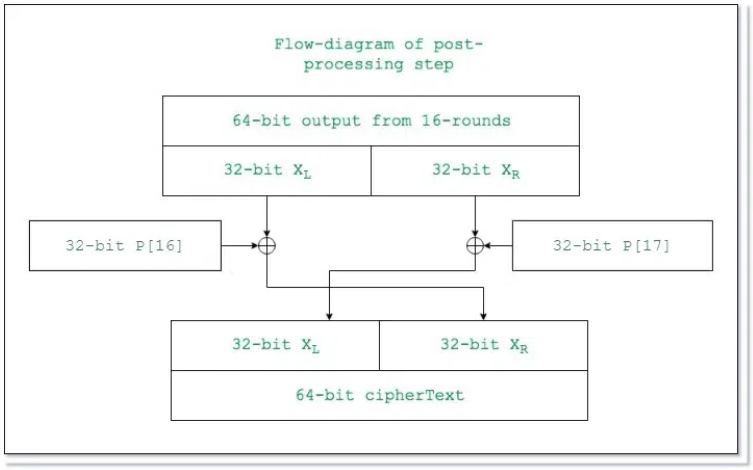


The description of the function ” F ” is as follows:



Here the function “add” is addition modulo 2^32.

b. Post-processing: The output after the 16 rounds is processed as follows:



5 CRYBERATTACKS AND SOCIAL ENGINEERING

What is a Cyberattack

A Cyberattack is a malicious attempt by an undividual or group to infiltrate , damage, disrupt, or gain unauthorized access to computer systems, networks or digital devices.

These attacks can target various components of digital infrastructure including hardware, software, data, and internet itself.

These motivations behind cyberattacks can vary widely, ranging from financial gain to political activism.

There are many types of Cyberattacks such as malware infections, phishing scams, denial of service(DoS) attacks, ransomware, or exploitation of software vulnerabilities.

Types:

Cyber attacks refer to deliberate attempts to breach the security of computer systems or networks to steal, alter, or destroy data, or to disrupt normal operations. These attacks can take various forms, including:

1. **Malware**: Malicious software designed to damage or disrupt systems. Examples include viruses, worms, ransomware, and spyware.
2. **Phishing**: A method of tricking individuals into providing sensitive information by masquerading as a trustworthy entity, usually through email.
3. **Denial of Service (DoS) Attacks**: Overloading a system or network with excessive traffic to render it inoperable.
4. **Man-in-the-Middle (MitM) Attacks**: Intercepting and altering communication between two parties without their knowledge.
5. **SQL Injection**: Exploiting vulnerabilities in a web application's database query system to gain unauthorized access to data.
6. **Zero-Day Exploits**: Attacks that exploit previously unknown vulnerabilities in software or hardware before developers have had a chance to fix them.

These attacks can have severe consequences, including financial loss, data breaches, and damage to an organization's reputation.

Social Engineering

Social engineering is a technique used to manipulate people into divulging confidential information or performing actions that compromise security. Unlike traditional cyber attacks that exploit technical vulnerabilities, social engineering relies on psychological manipulation. Common tactics include:

1. **Phishing**: As previously mentioned, this involves deceiving people into revealing personal information via fraudulent emails or websites. It's a blend of cyber attack and social engineering.
2. **Pretexting**: Creating a fabricated scenario or pretext to obtain sensitive information. For example, an attacker might pose as a company employee or IT support personnel to gain access to private data.
3. **Baiting**: Enticing victims with a lure, such as a free download or a prize, to persuade them to provide personal information or install malware.
4. **Tailgating**: Gaining physical access to a restricted area by following authorized personnel through secure entry points.
5. **Impersonation**: Pretending to be someone else, such as a trusted figure or authority, to deceive individuals into sharing confidential information.

Social engineering attacks exploit human psychology and trust, making them particularly challenging to defend against. They often rely on the attacker's ability to manipulate emotions and exploit the natural tendencies of individuals to trust and cooperate.

Defense Strategies

Combating cyber attacks and **social engineering** requires a multi-layered approach:

- **Education and Training**: Regularly educate employees and individuals about the latest threats and best practices for security. This includes recognizing phishing attempts and understanding the importance of strong, unique passwords.
- **Robust Security Measures**: Implement comprehensive cybersecurity measures such as firewalls, intrusion detection systems, and encryption to protect against various types of cyber attacks.
- **Regular Updates and Patching**: Ensure that all software and systems are up-to-date with the latest security patches to minimize vulnerabilities.
- **Incident Response Plan**: Develop and regularly test an incident response plan to quickly address and mitigate the effects of a cyber attack.
- **Access Controls**: Use strong access control measures to limit who can access sensitive information and systems. This includes multi-factor authentication and role-based access controls.

In summary, while cyber attacks and social engineering involve different methods of compromising security, both are potent threats in the digital landscape. A combination of technical defenses and awareness training is essential to protect against these evolving threats.