Fundamentals of Computer Network

Network Fundamentals

A computer network is a group of computers connected to each other for easy sharing of information and resources. The computers share information using a data path. A commonly known computer network is the Internet.

Network is a cluster of computer hardware connected together physically or logically

Networking describes the processes involved in designing, implementing, upgrading, and managing networks

A computer network is a group of computers connected to each other for easy sharing of information and resources

Features of computer networks include:

- Allows sharing of resources from one computer to another.
- Allows storing files and other information in one computer and other computers accessing those files and information.

Advantages

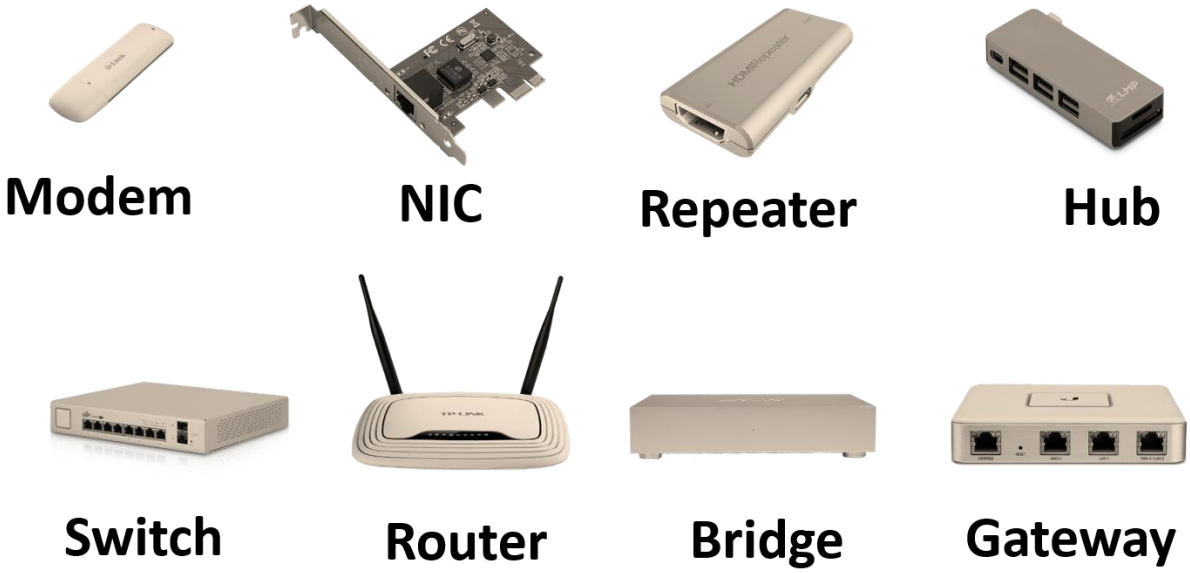
- Sharing of resources
- Data sharing
- Internet access
- Data security and management

Disadvantages

- Initial cost of setting network - hardware and software
- Maintenance costs
- Data security concerns
- Vulnerability to attacks

Network Components

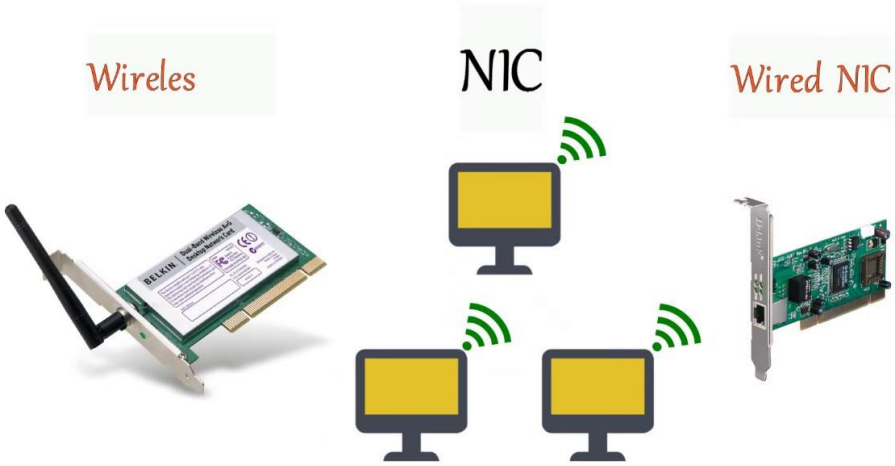
Computer network components are the *major parts* which are needed to *install the software*. Some important network components are NIC**,** switch**,** cable**,** hub**,** router, and modem. Depending on the type of network that we need to install, some network components can also be removed. For example, the wireless network does not require a cable.



NIC

- NIC stands for network interface card.
- NIC is a hardware component used to connect a computer with another computer onto a network
- It can support a transfer rate of 10,100 to 1000 Mb/s.
- The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).

There are two types of NIC:

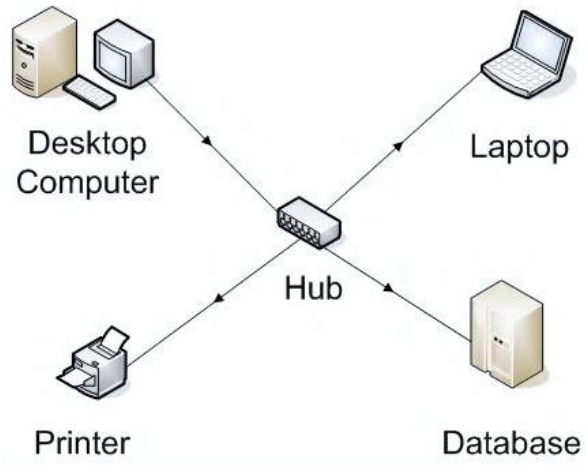


1. Wired NIC
2. Wireless NIC

Wired NIC: The Wired NIC is present inside the motherboard. Cables and connectors are used with wired NIC to transfer data.

Wireless NIC: The wireless NIC contains the antenna to obtain the connection over the wireless network. For example, laptop computer contains the wireless NIC.

Hub

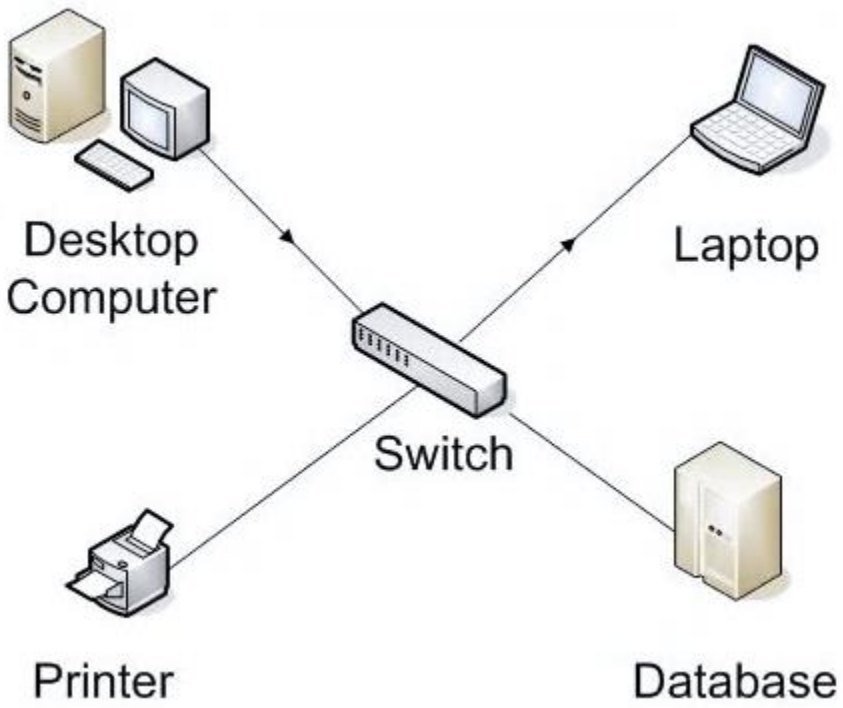


A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the

devices will check whether the request belongs to them or not. If not, the request will be dropped.

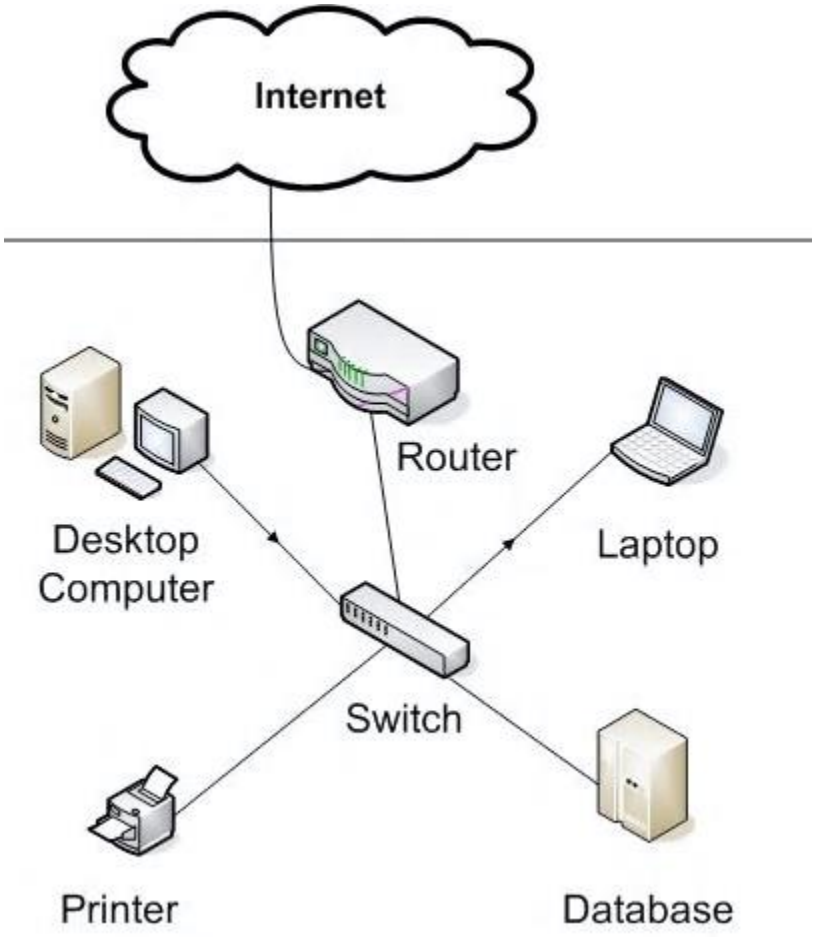
The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

Switch



A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.

Router



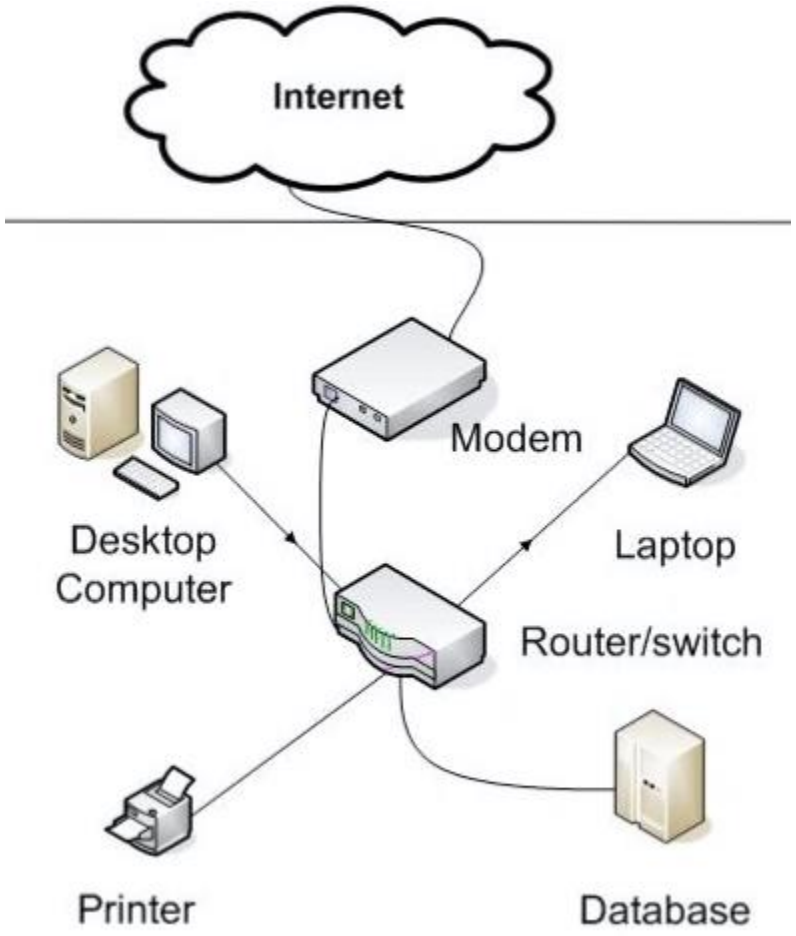
- A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.
- A router works in a **Layer 3 (Network layer)** of the OSI Reference model.
- A router forwards the packet based on the information available in the routing table.
- It determines the best path from the available paths for the transmission of the packet.

Advantages of Router:

- **Security:** The information which is transmitted to the network will traverse the entire cable, but the only specified device which has been addressed can read the data.

- **Reliability:** If the server has stopped functioning, the network goes down, but no other networks are affected that are served by the router.
- **Performance:** Router enhances the overall performance of the network. Suppose there are 24 workstations in a network generates a same amount of traffic. This increases the traffic load on the network. Router splits the single network into two networks of 12 workstations each, reduces the traffic load by half.
- **Network range**

Modem



- A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
- A modem is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard.

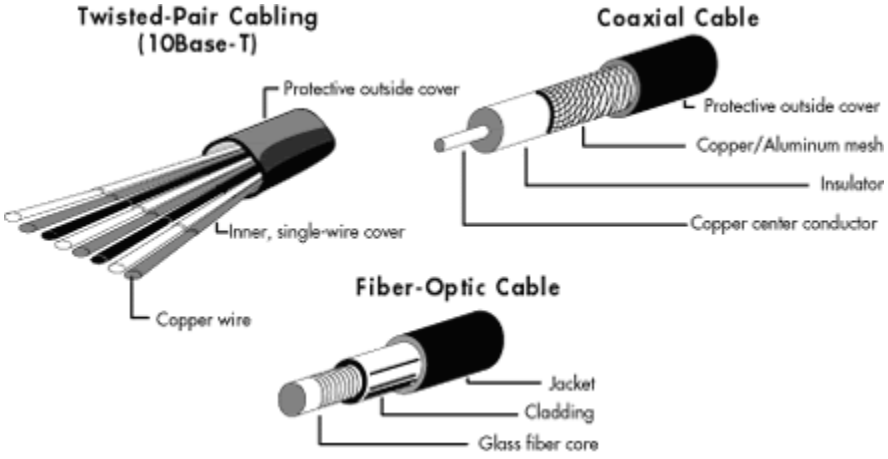
- It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

Based on the differences in speed and transmission rate, a modem can be classified in the following categories:

- Standard PC modem or Dial-up modem
- Cellular Modem
- Cable modem

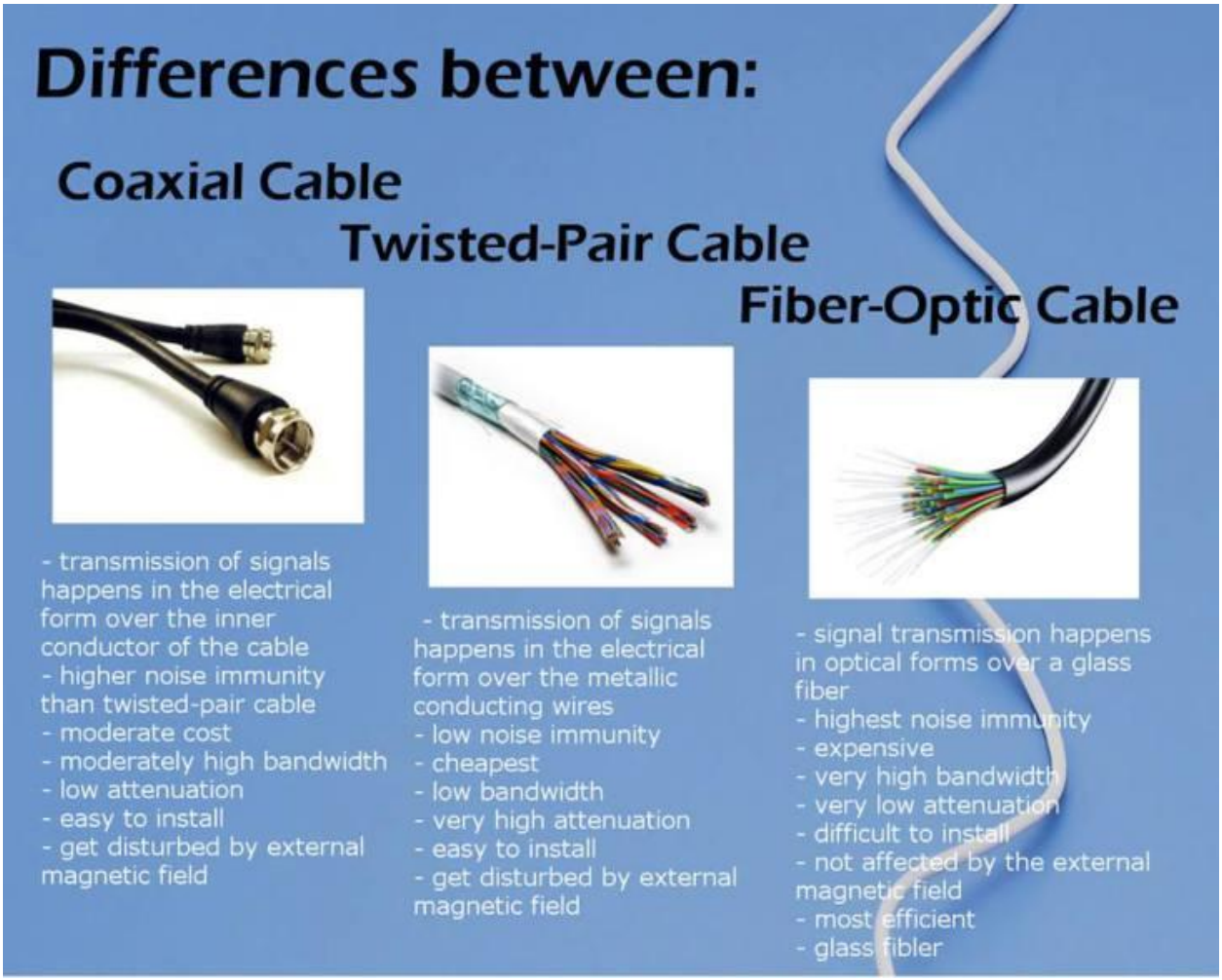
Cables and Connectors

Cable is a transmission media used for transmitting a signal.



There are three types of cables used in transmission:

- Twisted pair cable
- Coaxial cable
- Fibre-optic cable



LAN cable: A wire that is used to connect more than one computers or other devices such as printers and scanner to each other.

Server: Servers are computers that runs operating system and hold data that can be shared over a computer network.

Client: A client is a computer that is connected to other computers in the network and can receive data sent by other computers.

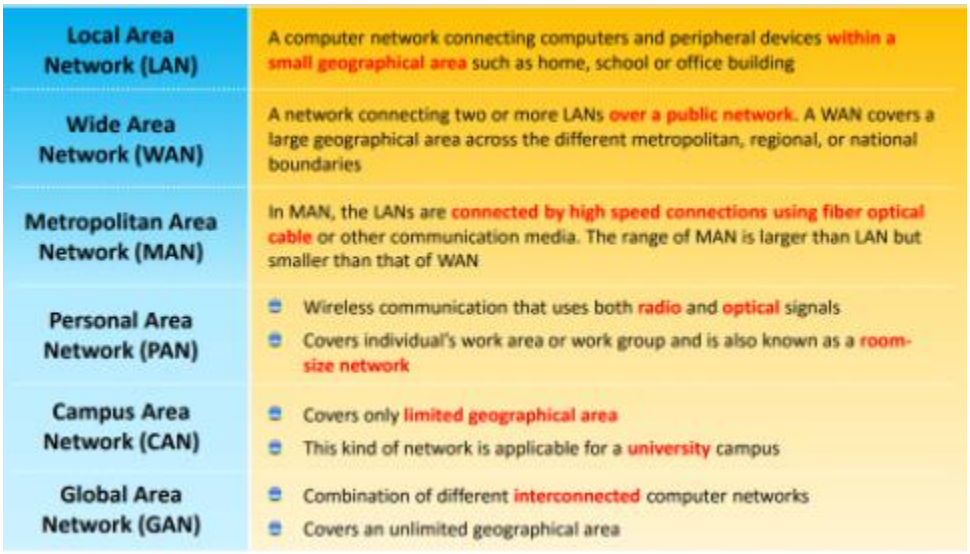
Transmission Media: All computers in a computer network are connected with each other through a transmission media such as wires, optical fibre cables, coaxial cables etc.

Gateways
A gateway acts as the meeting point or go between point between 2 different networks, using different protocols. e.g. Network A uses one protocol, Network B uses another.

Access points

Access points allow devices to connect to the wireless network without cables. A wireless network allows you to bring new devices and provides flexible support to mobile users.

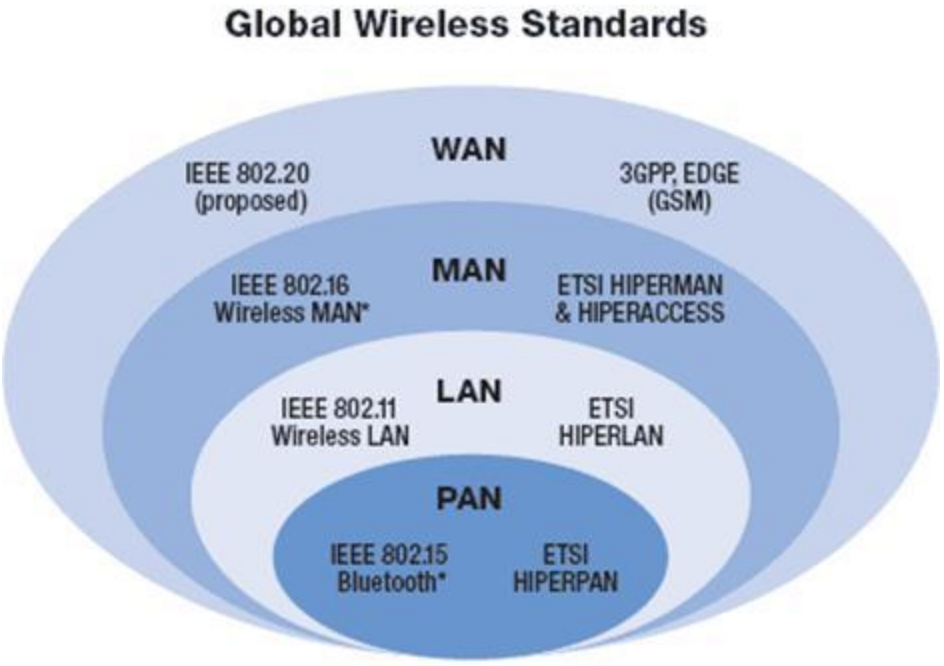
Types of Networks



These networks may differ in many ways. For example: by size, by functions, by the geographical distance. The services provided by the networks differ according to the layout of the networks.

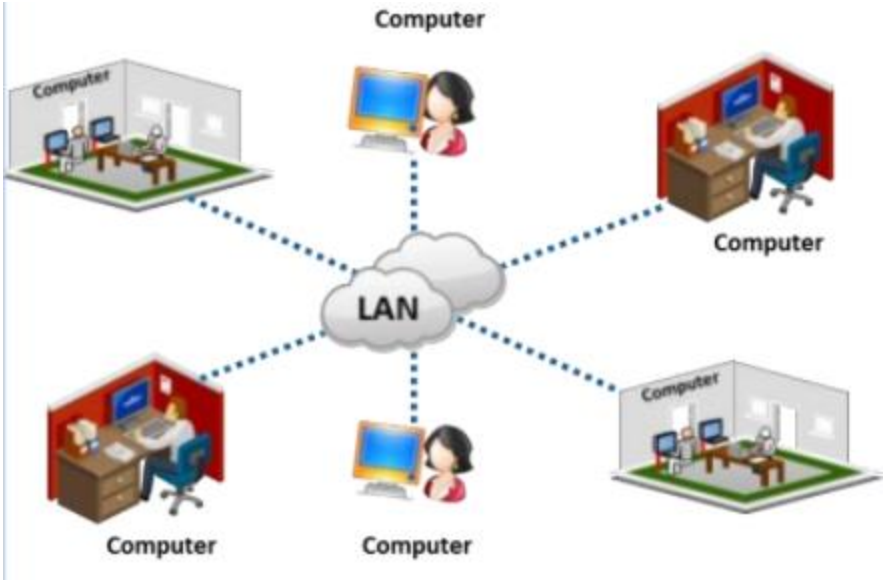
The networks that differ by size depend on the area occupied by the network and the number of computers present in the network. The computers in a network can vary from one single computer to millions of computers. The different networks are based on the size of the area they cover:

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)
- Personal Area Network (PAN)
- Campus Area Network (CAN)
- Global Area Network (GAN)



Local Area Network (LAN)

The LAN consists of computers and its related devices that share information over the same communication line. The LAN may extend only within an office building or home. The LAN can handle hundreds of users. The two commonly used LAN technologies are Ethernet and Wi-Fi. There are virtual LANs that enable the network administrators to provide a network connection to a group of nodes. LAN enables the use of many application programs and the users can achieve those applications by simply downloading it from the LAN. Wireless LANs are becoming much more popular. This is due to more flexibility and a cost which is less when compared to wired-LANs.



Advantages:

- Allows sharing of printers between the computers at home or office.
- LAN provides the users the privilege to work from any system in the LAN.
- Allows storage of files in a single folder and sharing between users on the network.

Disadvantages:

- As it provides file-sharing facility, it requires separate security measures to restrict access to certain files and folders.
- Any small issue in the file server can affect all the users on the server machine

Wide Area Network (WAN)

The WAN is spread over a larger geographical area and is more far-reaching than a LAN. WANs usually connect the nodes in the network using leased telecommunication lines. These lines assist in carrying the information efficiently across the various computers in the network. WANs can connect different LANs in a network. Most often, public networks are connected to the wide-area network. The LANs connect to WANs for quick and secure transfer of data. However, WANs requires a group of authorities to manage.

Features of WAN:

- WAN networks generally provide larger and dedicated network services. It always tries to meet the services according to business requirements.
- The WANs has a lower data transfer rate when compared to the transfer rate of LAN.

Advantages:

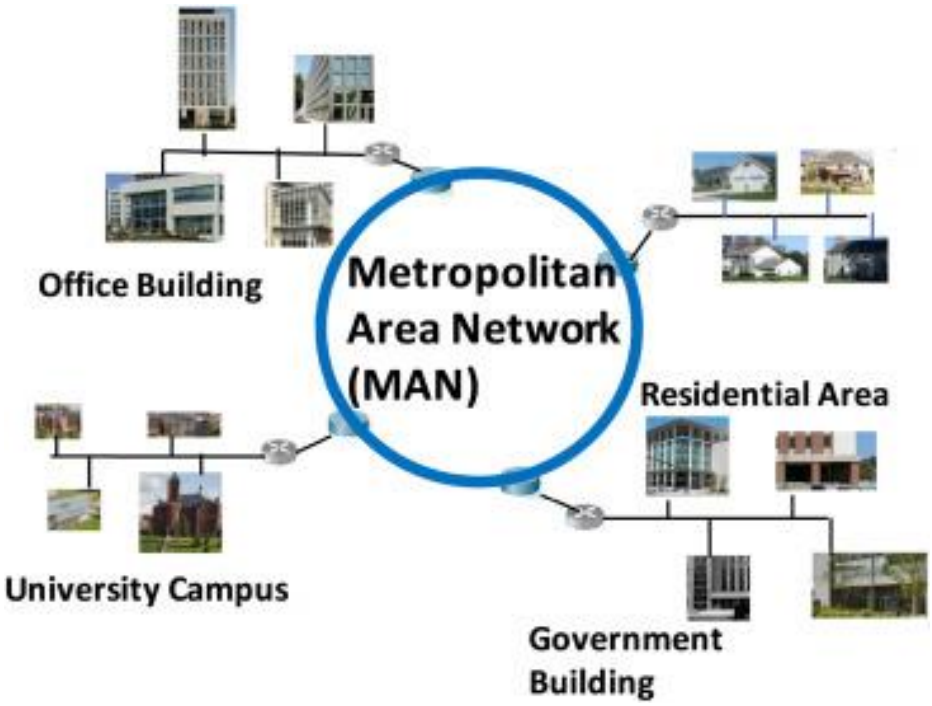
- A WAN connects places that are geographically apart from each other without a high costs and difficulties in implementation.

Disadvantages:

- Very complex in structure.
- Provides only lower bandwidth and has a higher risk of losing connections.

Metropolitan Area Network (MAN)

A MAN stretches for an even larger geographical area than a LAN, but less than that of a WAN. It refers to the interconnection of networks spread across a city or town. Several LANs grouped together form MANs. MANs provide secure, efficient communication by making use of fiber optic cables. The MAN provides shared network connections to its users.



Advantages:

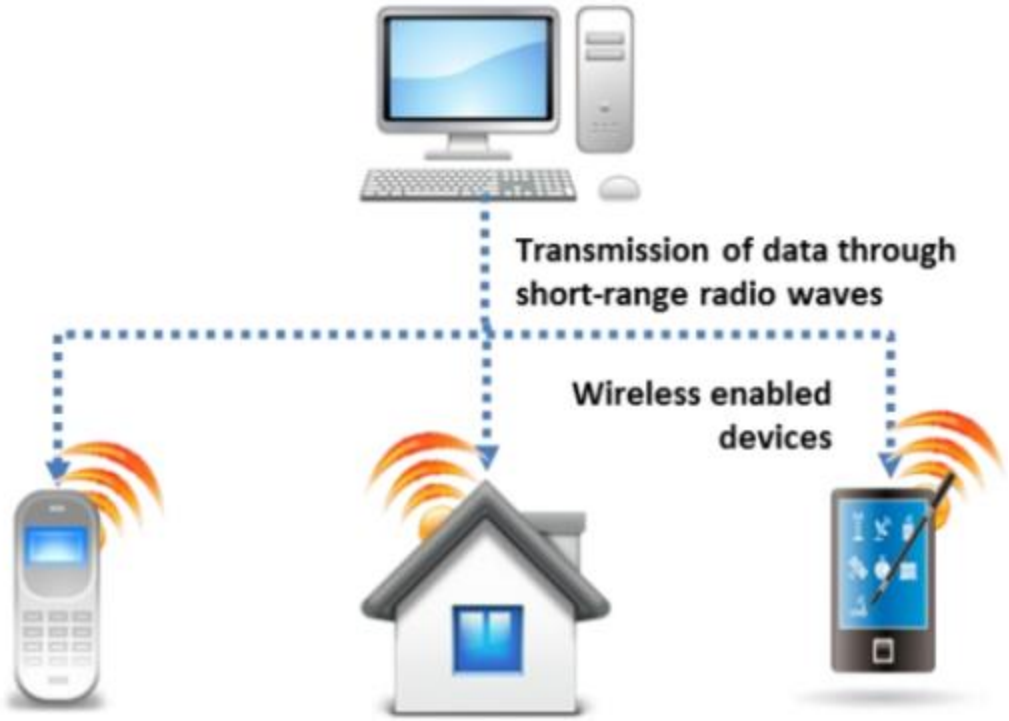
- The links connecting the computers in a MAN have a much higher bandwidth allowing for the easy sharing of data.
- Allows multiple users to share the data at the same speed.

Disadvantages:

- Requires installation before deploying it for the first time.
- Costly when compared to LANs.

Personal Area Network (PAN)

A Personal Area Network refers to the interconnection of devices within a certain range of distance. For example, a person can connect a laptop, mobile, tablet etc. to the wireless network within a certain distance without having to physically plug in anything to the devices. This allows for file and information sharing within the devices connected to that network.

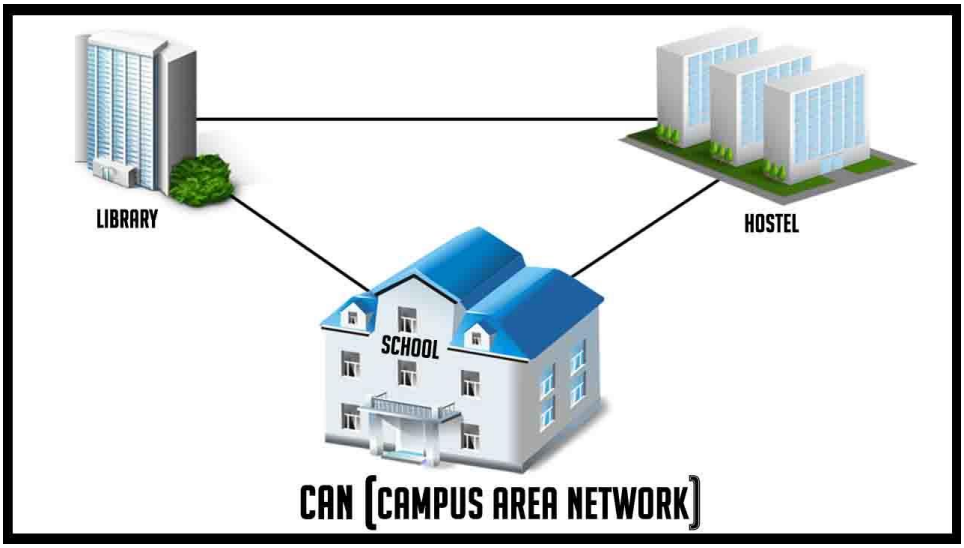


Campus Area Network (CAN)

A campus area network consists of multiple connected local area networks within a certain geographical area. Most government organizations and universities make use of the campus area network. The size of the campus area network is much smaller than a MAN or a WAN. It uses optical fiber in order to connect the nodes in a campus network. For example, different buildings in a campus can use campus area network for interconnection and thereby allows the sharing of information within different departments. The implementation of a CAN requires less cost, is highly beneficial and economical due to high speed data transfer from any section of the network.

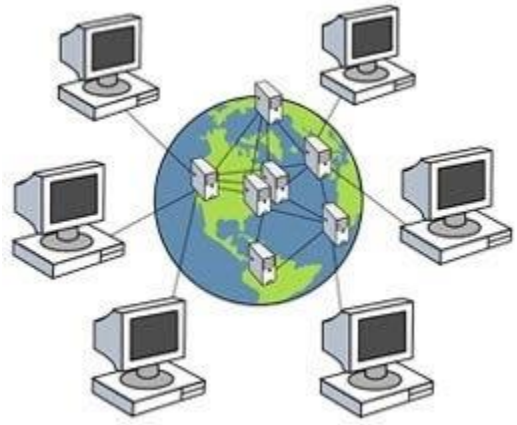
Features:

- Cost effective.
- Allows interconnection between various departments in a campus.
- It provides a single shared data transfer rate.
- Resistant to failure.
- The campus area network is highly flexible to the changes of an evolving network.
- CAN offers a highly secure network by implementing authentication of the users accessing the network



Global Area Network (GAN)

The Global Area Network consists of different interconnected networks extending over an unlimited geographical area. The GAN covers a more geographical area than a LAN and a WAN.

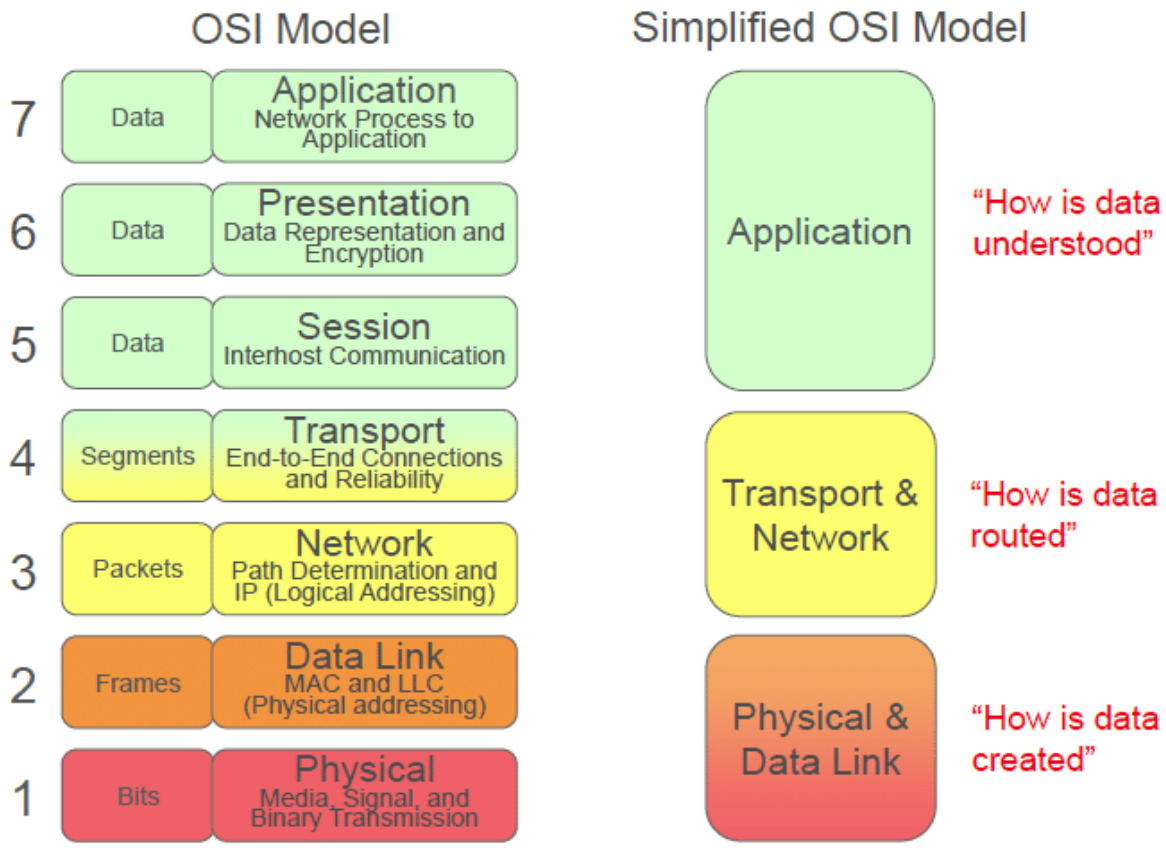


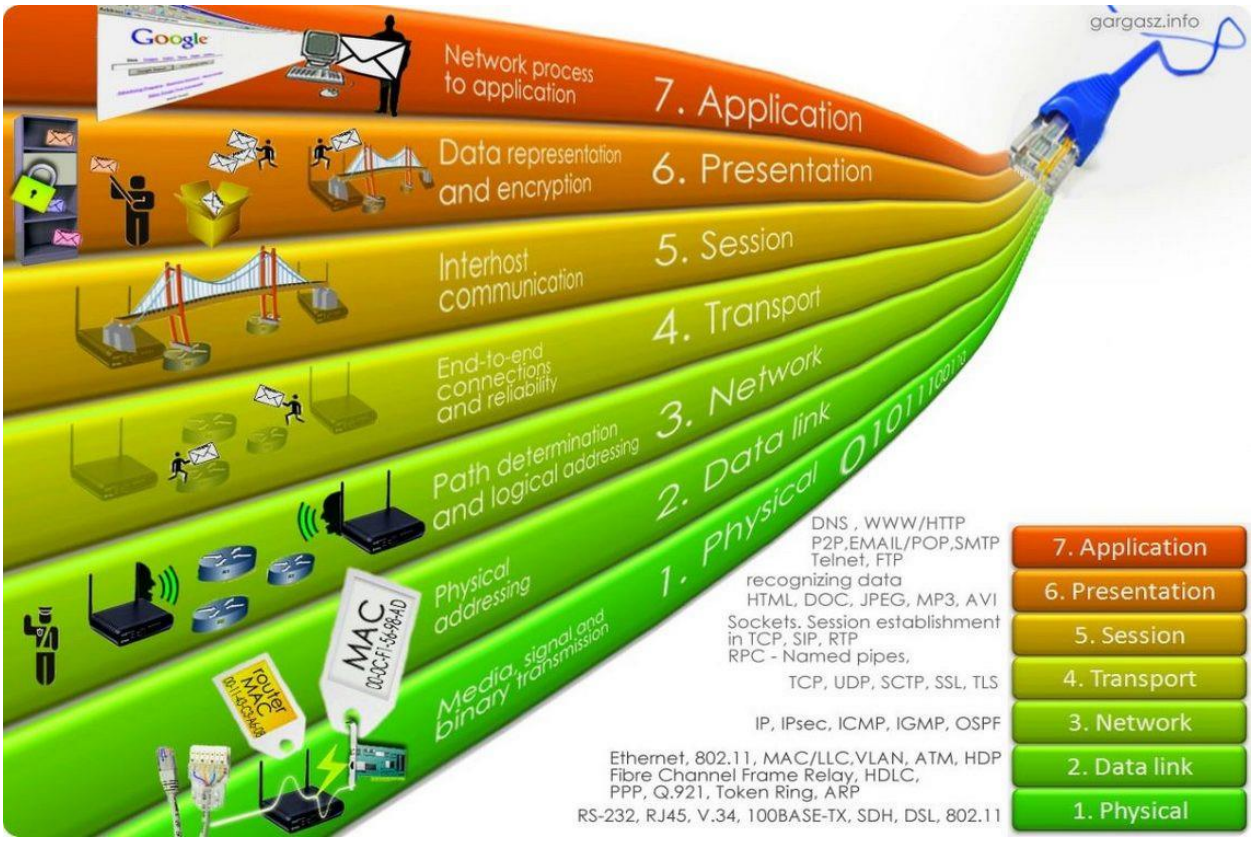
A GAN enables transfer of data from one point to another even when they do not connect directly with each together. The points can connect using a central server or each point can pass the data from one point to another till it reaches the destined point. The GAN supports mobile communication for a number of wireless LAN's. Broadband GAN is the most commonly used GAN. The BGAN uses portable terminals to connect the computers located at different locations to the internet.

Advantages of GAN:

- GAN allows the interconnection of multiple networks and it enables proper sharing of data without tampering with it.
- Enables the storage of files in a central server, thereby allowing easy access of files across different networks.
- GAN enforces the security of file access by imposing access restrictions.

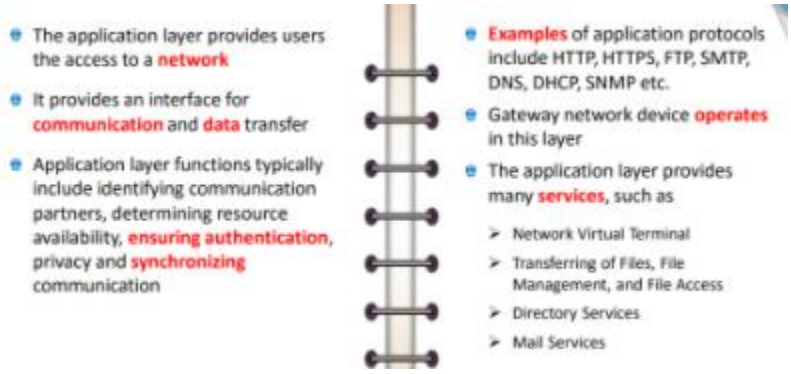
OSI (Open Systems Interconnection)





Open System Interconnection (OSI) is a reference model that defines the communication of data over the network. It is a framework that portrays the flow of data from one device to another over the network. The OSI model classifies the communication between two end-points into seven different groups of layers. The logic behind this division is that the communicating user provides functions of each of the seven layers. The communication between two users occurs as a downward flow of data through the layers of the source computer. Then, it traverses across the network and flows upwards through the layers of the destination computer. Each layer consists of hardware and/or software components and is responsible for certain function. Each layer has standard input and output data.

1. **Application Layer**



The application layer providers the users the access to any network. It provides services such as interfaces and help services for email distant file access. It also provides the database management for share systems and many other kinds of distributed systems.

The application layer provides many services, such as:

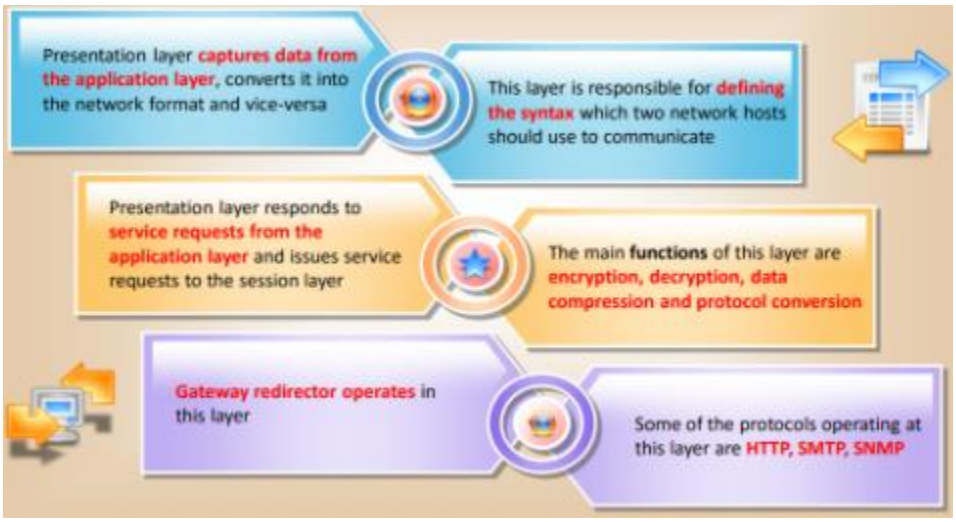
Network Virtual Terminal: A network virtual terminal is a software system of the actual terminal. It permits users to enter the systems that are distantly located for remote accessing. To achieve this, the application generates a software model of a terminal at the remote host. The user's terminal communicates with the software terminal, which again communicates with the original terminal that allows the users to log on to the system.

Transferring of Files, File Management, and File Access: The application layer permits a user to access the files in distant places to get the files from remote computers and to administer the files in an isolated computer.

Directory Services: The application layer provides distributed database facilities and access for retrieving the information worldwide.

Mail Services: This application provides the foundation of email sending and the storage of the email received.

2. **Presentation Layer**



The presentation layer deals with the syntax and semantics of the data interchanged between the two devices. The responsibilities of the presentation layer are:

Translation

The process of administering programs in two systems is exchanging the data like numbers, characters, symbols, etc. The information must be converted into streams of data before sending them. The information is to be changed into streams of data prior to sending it. As different computers have different encoding systems, the presentation layer deals with the interchange between the various systems of encoding. The entire

device's data is sent into a common format that the presentation layer at the receiving end and the format that is received is dependent on the receiver's format.

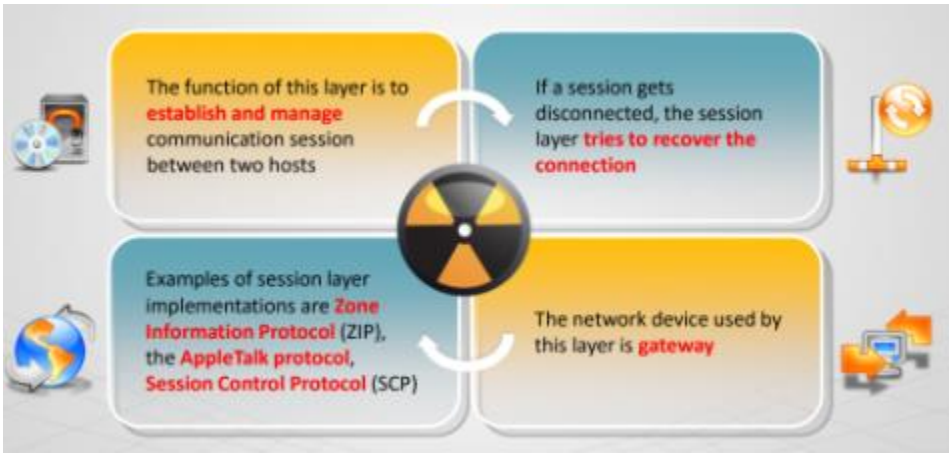
Encryption

To transmit confidential information, the system must be able to provide security. In encryption, the sender of the data changes the exact information into other format and broadcasts the resultant information.

Compression

The compression of data reduces the amount of bits to be sent. Data compression becomes significant in the transmission of information such as images, sound, and video.

3. **Session Layer**



The session layer monitors the communication between two devices.

The responsibilities of the session layer are:

Communication Control

The session layer permits two devices to establish a dialog between them. It permits the communication between the devices to take place in the form of duplex or half-duplex form.

Data Organization

The session layer permits the process to employ checkpoints. If a system is sending a file of some 1000 pages, checkpoints are inserted after every 100 pages to make sure that each 100p age unit is received and acknowledgement for the same is sent individually. The advantage of the check point system is that if any failure occurs in between the entire file need not be re-transmitted again except for the ones for which retransmission is needed.

4. **Transport Layer**

The transport layer is useful for sending the packets from the source to the destination. The transport layer makes sure that the entire message is transmitted without any deletions or modifications by helping in fault control and transmission control. For security enhancement transport layer can maintain a connection between the end points.

The responsibilities of the transport layer are:

Addressing

The transport layer's packet has a header that is useful for holding the address of the service point address. The network layer transmits the exact packet to the transport layer and makes the whole message arrive at the exact process on that device; the transport layer gets the whole message to the exact process on the computer.

Isolation and Re-gathering

A message is broken into many segments for transmission and each segment holds a sequence number. These numbers permit the transport layer to re-gather the message appropriately to the destination and to recognize and replace the packets that were lost in the communication.

Link Control

The protocols are of connectionless or connection-oriented. Connectionless transport layer considers each segment as an individual packet and sends it to transport layer at the destination. A connection-oriented transport layer establishes a connection with the transport layer at the end machine initially before sending a link.

Transmission Control

Fault control is performed from destination to destination than a single link. The sending transport layer ensures that the whole messages arrive at the receiving device without any errors.

Error Control

The transport layer is useful for fault control from source to destination. The sending transport layer ensures that the whole messages arrive at the receiving device without any errors.

5. **Network Layer**

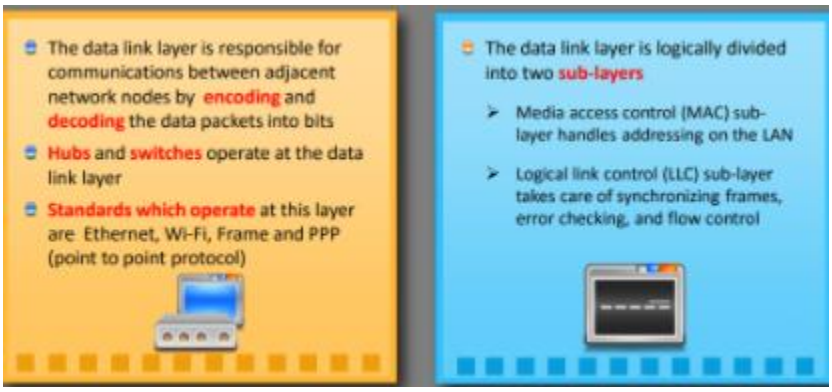
- The network layer establishes paths for data transfer through the network
- Routers operate at network layer
- Major protocols operating at this layer include IP and ICMP

The network layer is useful for source-destination transmission of packets across multiple networks. The network layer makes sure that individual packet initiated from the source reaches the destination.

The responsibilities of a network layer are:

- **Global Addressing**: Global addressing is executed through the data link layer, which deals with the addressing problem, locally. If the packet passes the network border another addressing system is essential to separate the source and destination systems. The network layer supplies a header to the packet that originates from the upper layers and includes the global address of the sender and receiver.
- **Routing of Data Packets**: The network layer is linked together to create an Internet work, which is a huge network, where the linking devices route the packets to the final destination.
- **Fault Handling**: The network layer is useful for fault control from source to destination. The sending network layer ensures that the whole messages arrive at the receiving device without any errors.
- **Traffic Control**: The network layer is useful for controlling the flooding of traffic from source to the destination so that the end user is not overwhelmed.

6. **Data-link Layer**



The data link layer changes the physical layer for furnishing the information to a secure data link layer that is responsible for device-to-device delivery. The objective of data link layer is to make the physical layer secure without any errors.

The responsibilities of the data link layer are:

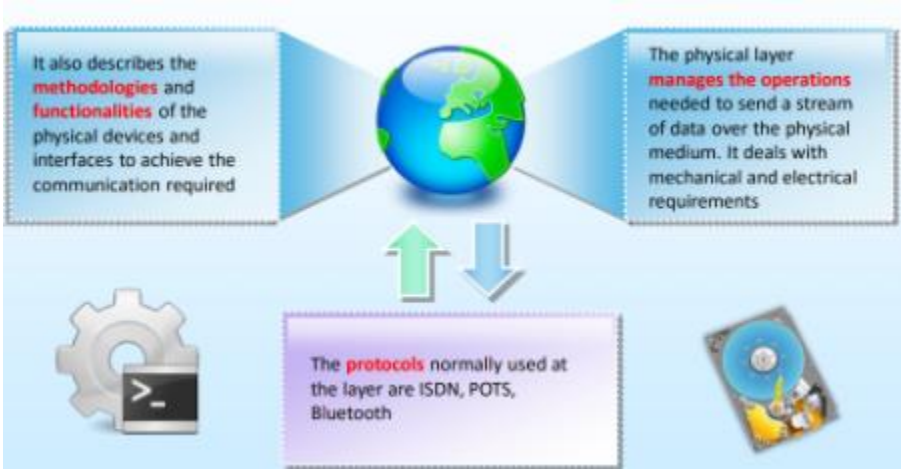
Grouping: The data link layer groups the bits of information received from the network layer into data packets called as frames.

Addressing: The data link layer adds a header to the packet to describe the original address of the sender or the receiver. If the packet is devised for a system that is exterior to a sender's network the receiver address is the address that links two subsequent addresses.

Fault Control: In fault control, the data is taken by the receiver is less than the rate generated by the sender. The data link layer employs the flow control mechanism to reduce the data flooding at the receiver's end.

Access Control: When more devices have the same connection, the data link layer employs certain protocols that are essential to determine the devices that are having authority on the other devices.

7. Physical Layer



The physical layer manages the operations needed to send a stream of data over the physical medium. It deals with mechanical and electrical requirements. It also describes the methodologies and functionalities of the physical devices and interfaces to achieve the communication required.

The responsibilities of the physical layer are:

Features of the interfaces and media: The physical layer defines the features of the interfaces between the devices and the communication media.

Depiction of data: The data is depicted in the form of 0's and 1's without any encryption when passed through the physical layer. The data is encoded into signals which may be of electrical signals or light signal

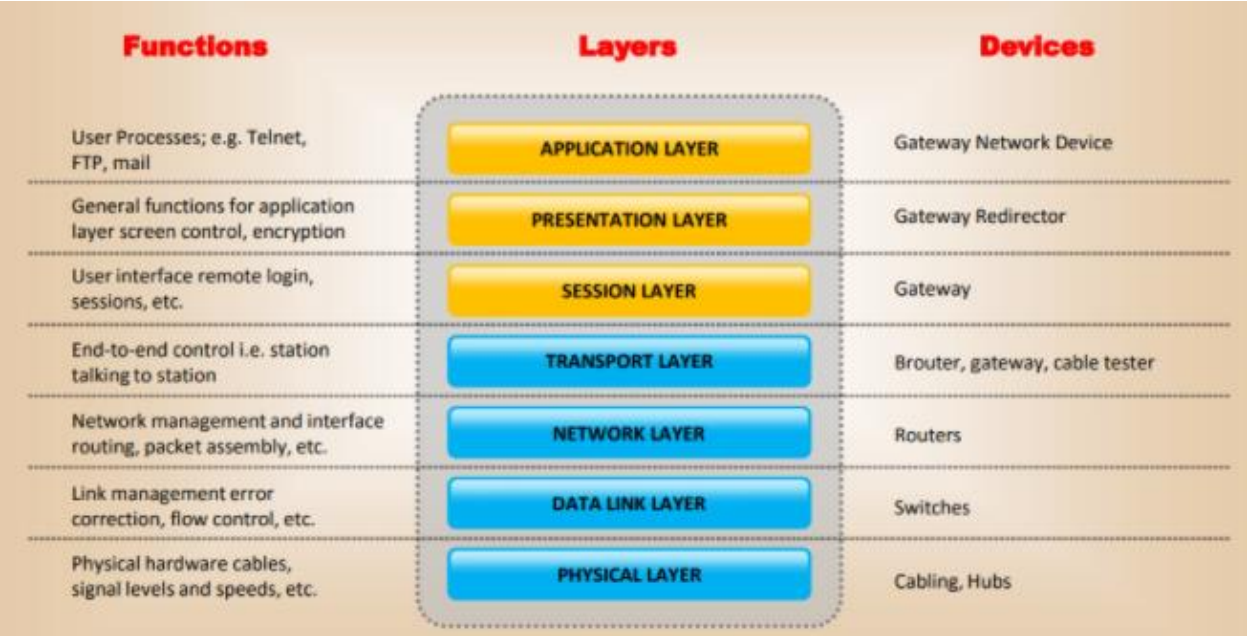
Organization of data bits: The sender and receiver must have their data organized at the bit stream level. The sender and the receiver possess a clock that must be organized.

Configuration of the links: The physical layer deals with the links of the devices to the medium. In a point-–to--point connection, the devices are attached through a single link. In a multipoint design, a link is divided amongst many devices.

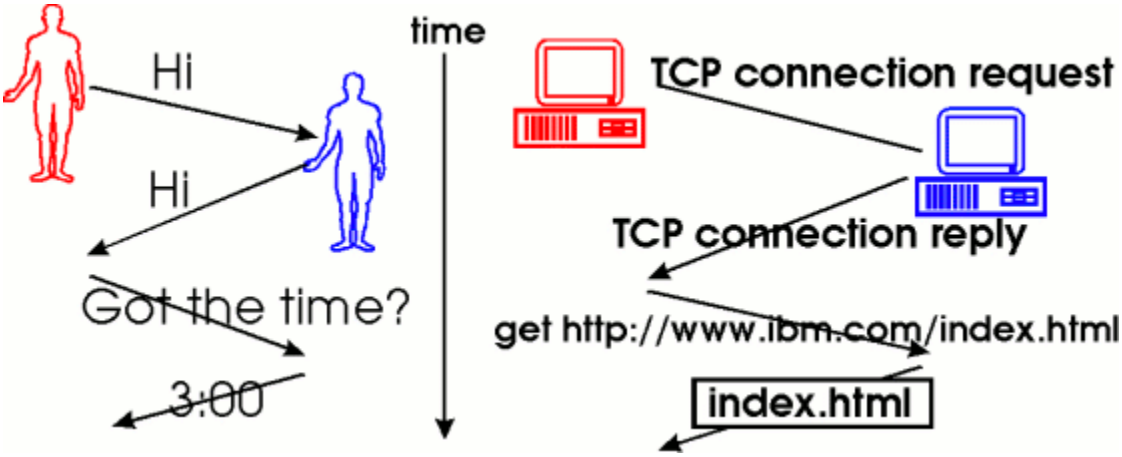
Topology of devices: The topology deals with the position of devices through which they form a network. The devices can be connected in the network using Mesh, Star, Ring, and Bus topologies.

The mode of communication: The physical layer also describes the mode of transmission between two devices. They are of simplex, duplex, and half-duplex types.

OSI Layers and Device Mapping



Protocols



Protocol stack is a set of OSI protocols, which synchronize their activities and work together with all the software and hardware to perform a specific task. The TCP/IP is an example for the protocol stack. There are four layers in the TCP/IP protocol stack, which map to the OSI model. They are:

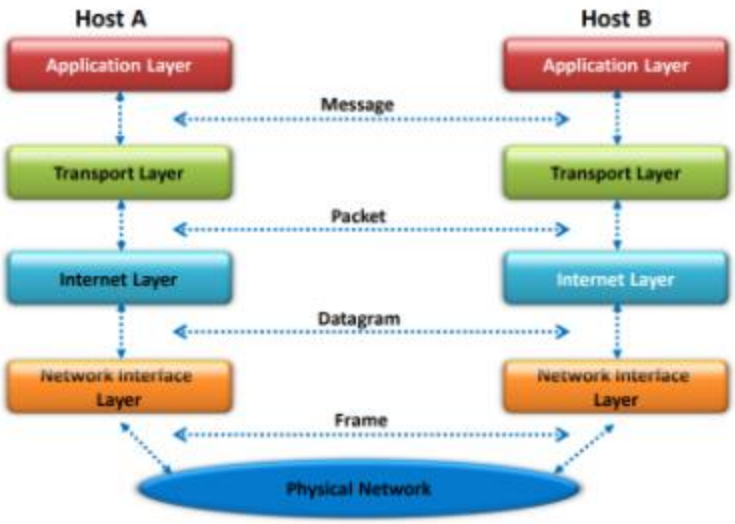
Network Interface Layer: This layer combines physical and data link layer and this layer is used to send the data from the source to the destination in the same network. It also performs the task of exchanging the data between the network and other devices.

Internet Layer: This layer communicates with the network layer. The address of the destination is determined using the information in the header.

Transport Layer: It communicates with the OSI transport layer. TCP is an important protocol that can be found in this layer. TCP is transmission control protocol that works by inquiring another device on the network if the device can accept the data.

Application Layer: In this layer, the user can interact with the network or device on the network. It provides various services such as e-mail, FTP, etc.

TCP/IP Model



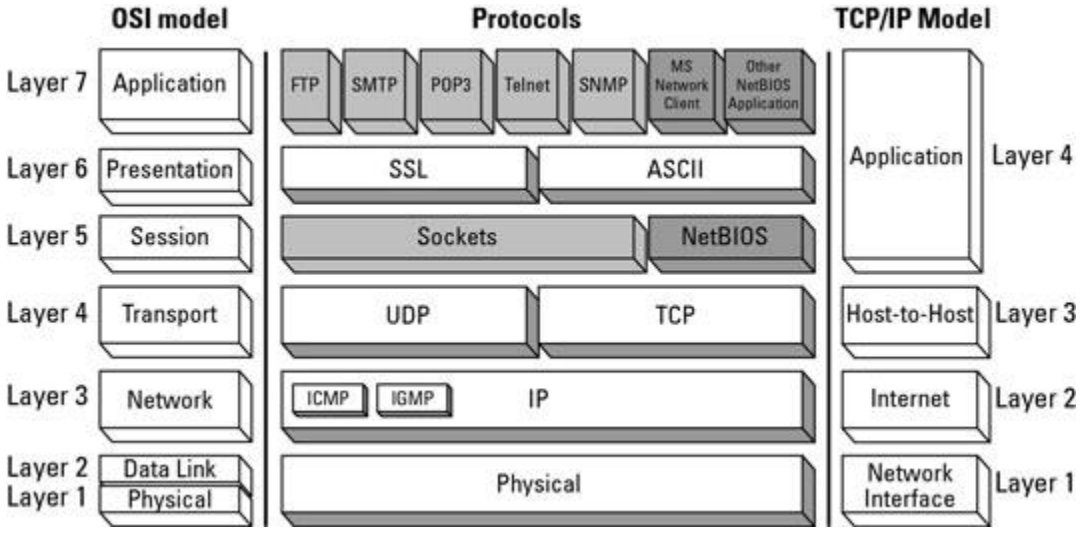
The TCP/IP protocol is a four-layered protocol developed by the Department of Defense (DOD). Each layer in this model performs a different function and the flow of data occurs from layer 4 to 1 (from the sending machine) and from layer 1 to 4 (in the destination machine). The TCP/IP model describes the end-to-end communication between two machines and thereby determining the addressing, routing, and transmission of the data. The four layers in the TCP/IP model include:

Application layer (Layer 4): Provides data access to applications.

Transport layer (Layer 3): Manages host-to-host interactions.

Internet layer (Layer 2): Provides inter-networking.

Network Access layer (Layer 1): Provides communication of data present in the same network



Advantages of TCP/IP model:

- It serves as a client-server architecture.

- It functions independently.
- It consists of many routing protocols.
- Initiates a connection between two computers.

Disadvantages of TCP/IP model:

- Complex to setup.
- No assurance of packet delivery in the transport layer.
- Not an easy task to replace protocols.
- No visible parting between the services, protocols, and interfaces.

TCP/IP Protocol Stack

TCP/IP Protocol Stack: Internet Protocol (IP)

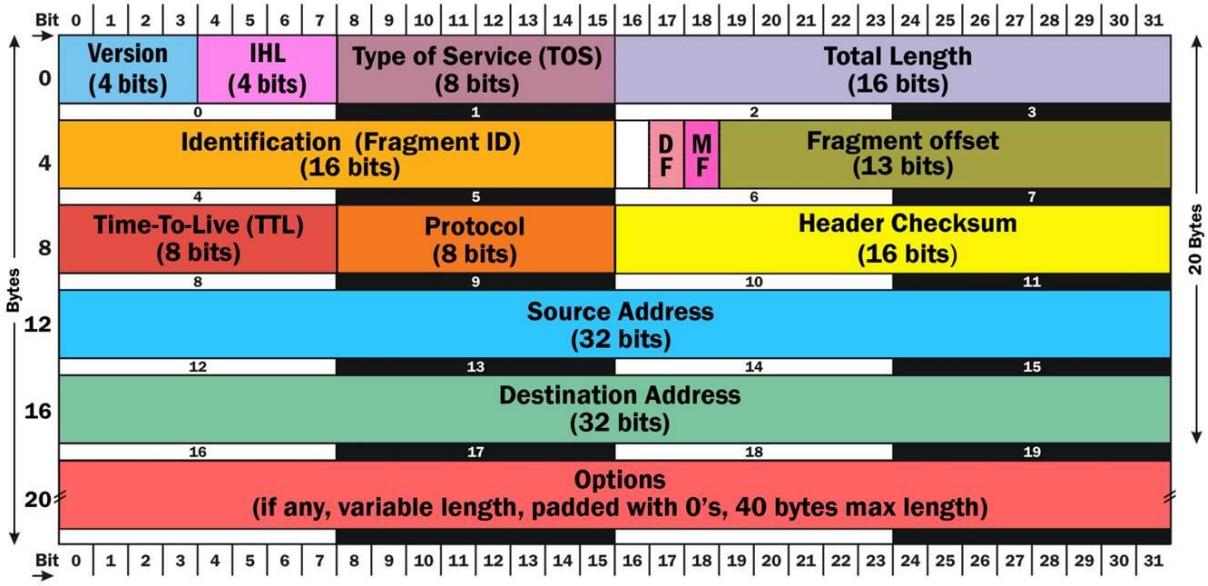
IP is a network layer protocol present in the TCP/IP communications protocol suite. The data is always sent as packets or datagrams in networking. IP provides a unanimously defined address that eliminates the need to create a connection before sending data. IP also provides a datagram service that carries information or data to the destination without much guarantee regarding the confirmed arrival of these packets at the destination. The packets can be lost on the way to the destination or can arrive at the destination in a completely or partially damaged form.

There are two versions of IP available: Internet protocol version 4 (IPv4) and Internet protocol version 6 (IPv6). The commonly used version is IPv4, which is represented using a 32-bit address. The IPv6 is an improved version of IPv4 and is represented using a 128-bit source and destination address. The IP header is an introduction to the IP packet that contains information like IP version, source IP, destination IP, TTL, etc. The header normally is responsible for holding data required to traverse the data over the Internet. The IP header has the same format as the data.

Various fields in the IP header are as follows:

- **IP Version (4 bits):** There are two types of IP packet and addressing—IPv4 and IPv6. This bit specifies the current IP protocol version. Always set the value as 4.
- **Header Length (4 bits):** Length of the IP header where the header represents 32-bit words along with IP options (if any). The minimum value of the IP header is 5.
- **Type of Service (TOS) (8 bits):** Provides quality-of-service features. The first three bits are for IP precedence, the next 4 bits are for TOS, and the last bit is left alone (not used).
- **Total Length (16 bits):** Specifies the length of the IP datagram in bytes. It includes the length of the header and the data.
- **Identification (16 bits):** Identifies the fragments of one datagram from those of another.
- **Fragment Offset (13 bits):** Used to reassemble the fragmented IP datagrams.

- **Time-O-Live (TTL):** It defines the lifetime of the IP datagram in the Internet system. The TTL field is initially set to a number and decremented by every router. When the TTL reaches zero, it discards the datagram (packet).
- **Protocol (8 bits)**: Identifies the next encapsulated protocol that sits above the IP layer.
- **Header Checksum (16 bits**): Identifies the errors during IP datagram transmission and is calculated based on the IP header.
- **Source IP Address (32 bit**s): This field represents the IP address of the sender.
- **Destination IP Address (32 bits):** This field represents the IP address of the receiver (destination).
- **Options (variable in length):** This is an optional field. List of options that are applicable for the active IP datagram.
- **Data (variable in length):** This field contains the data from the protocol layer that is handed over the data to the IP layer.

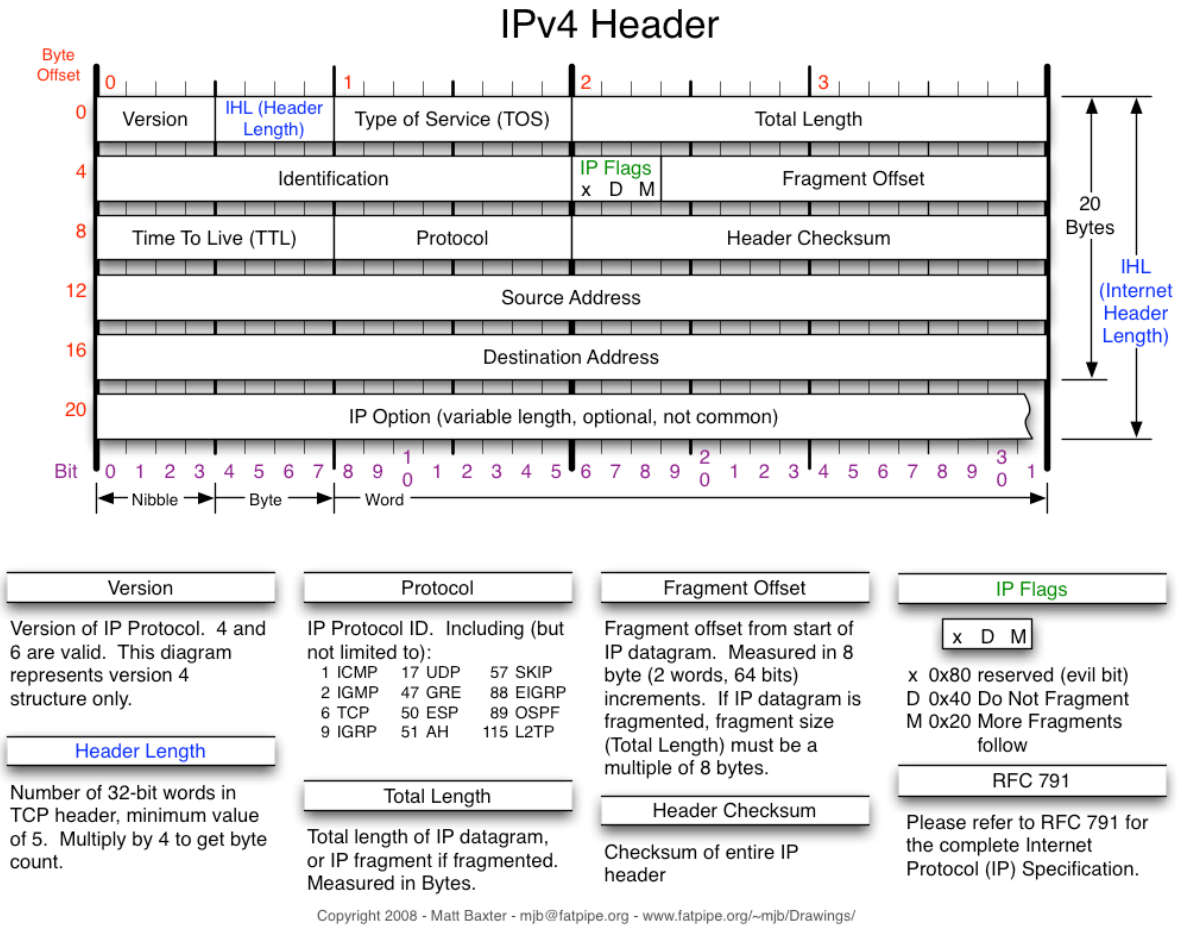


IP Header: Protocol Field

The protocol field in the IP header determines the services available in the next (higher) levels in the protocol stack. The protocol field is eight bits in length and includes 256 protocols. Multiple higher-layer protocols can use an IP (multiplexing). "Assigned Numbers" specifies the values for various protocols. Protocol and some common values (1 octet) are as follows:

- 0 (0x00) IPv6 Hop-by-Hop Option
- 1 (0x01) ICMP protocol
- 2 (0x02) IGMP protocol
- 4 (0x04) IP over IP
- 6 (0x06) TCP protocol

- 17 (0x11) UDP protocol
- 41 (0x29) IPv6 protocol



Internet protocol version 6 is the most recent version of the Internet protocol. The Internet protocol version 6 provides a mechanism for identifying the computers in the network and performs routing of the traffic across the Internet. To meet the increasing requirements, the Internet Engineering Task Force (IETF) started a working group called Internet Protocol next generation (IPng) to research, experiment, and generate recommendations for finding a new generation protocol for the IP. It eventually found the specification for Internet protocol version 6 (IPv6) described in the Internet standard document RFC 2460. Experts consider IPv6 as a replacement to IPv4. The IPv6 uses a source and destination address in order to carry data packets over the network, which is the same as in IPv4. IPv6 has a very large address space and consists of 128 bits as compared to 32 bits in IPv4.

The features of IPv6 include

- IPv6 internet layer protocol is for packet-switched inter-networking; it provides end-to-end transmission of data across multiple IP networks.
- IPv6 is capable of providing large address spaces for increasing demands of internet users.

- It has a new format for the packet header to minimize packet-processing problems with overhead routing entries. Routers can efficiently and easily process IPv6 headers.
- IPv6 has globally identified unique addresses with efficient, hierarchal, and routing infrastructure that relies on prefix length rather than address classes. This allows the backbone routers to create small routing tables.
- IPv6 simplifies host configuration with stateless and stately address configuration for network interfaces.
- In IPv6, hosts on a link are capable of automatically configuring themselves with a link (called link-local addresses) by responding to the prefixes mentioned by the local routers. When the host sends a link-local address request to a local router for connecting to that network, it then responds to the request by sending its configuration parameters. This lets the host configure automatically with the available router. IPv6 is even capable of configuring itself, even though there are no routers.
- IPv6 has an inbuilt security feature called integrated Internet protocol security (IPsec). It is a set of internet standards based on cryptographic security services providing confidentiality, data integrity, and authentication.
- IPv6 supports unicast and multicast communication along with a new communication type called anycast. In the anycast communication method, only the specific associated address in a network receives the messages.
- IPv6 provides better support for quality of service (QoS) with proper management of network traffic.

IPv6 Header

The IPv6 is four times larger than the IPv4. However, the header of IPv6 is only two times larger than the IPv4. The IPv6 header consists of one fixed header and zero or more extension headers. The extension headers consist of information that assists the routers in determining the flow of a packet. The IPv6 is 40 bits long and the fields in the fixed header consist of:

Version (4 bits): Specifies the version of the internet protocol.

Traffic class (8 bits): Identifies the data packets that belong to the same traffic class and distinguishes the packets with different priorities.

Flow label (20 bits): This field avoids reordering of data packets and maintains the sequential flow of data packets belonging to the communication.

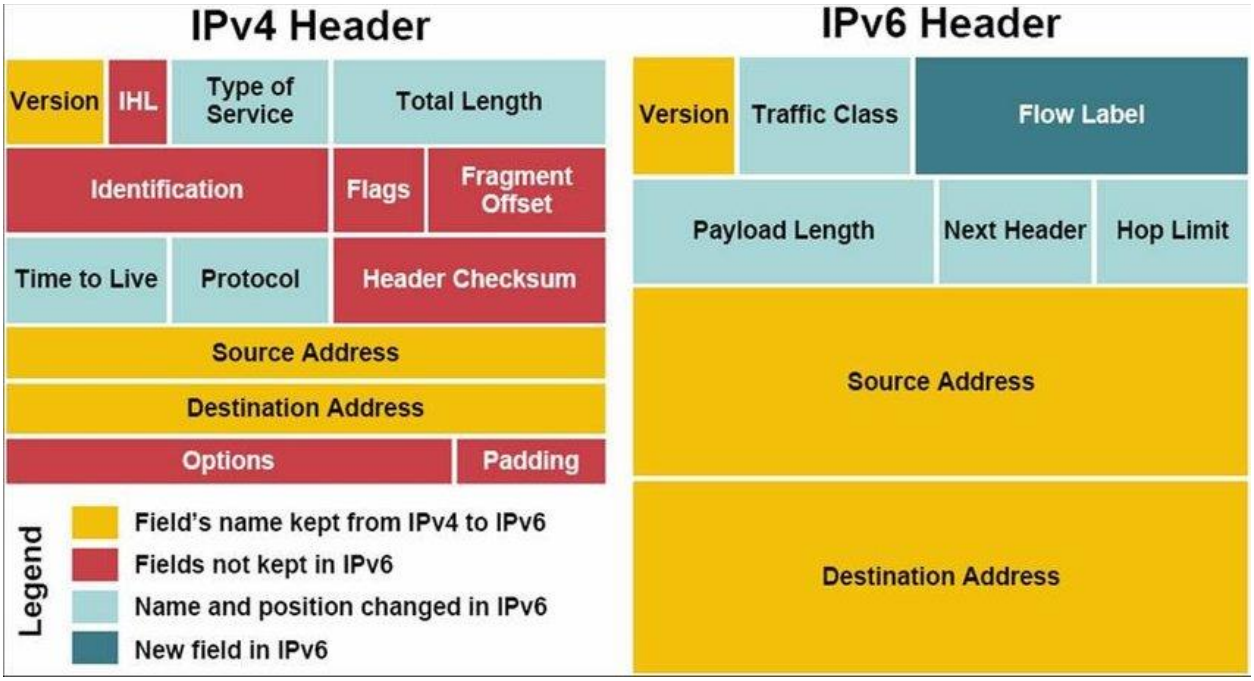
Payload length (16 bits): It informs the router about the length of the data that is present for a particular packet in its payload.

Next header (8 bits): Identifies the type of header following the IPv6 header and is located at the beginning of the data field (payload) of the IPv6 packet.

Hop limits (8 bits): Replacement of time-to-live field in IPv4. Identifies and discards the packets that are stuck in an indefinite loop due to any routing information errors. When the counter reaches zero, it discards the packet.

Source IP address (128 bits): IPv6 address of the sending host.

Destination IP address (128 bits): IPv6 address of the receiving host (Destination).



The following section describes the sections of the TCP/IP protocol stack.

Device Drivers

The device driver layer (also called the Network Interface) is the lowest TCP/IP layer and is responsible for accepting IP datagrams and transmitting them over a specific network. A network interface might consist of a device driver or a complex subsystem that uses its own data link protocol.

Internet Protocol (IP) Layer

The Internet Protocol layer handles communication from one machine to another. It accepts requests to send data from the transport layer along with an identification of the machine to which the data is to be sent. It encapsulates the data into an IP datagram, fills in the datagram header, uses the routing algorithm to determine how to deliver the datagram, and passes the datagram to the appropriate device driver for transmission.

The IP layer corresponds to the network layer in the OSI reference model. IP provides a connectionless, "unreliable" packet-forwarding service which routes packets from one system to another.

Transport Layer

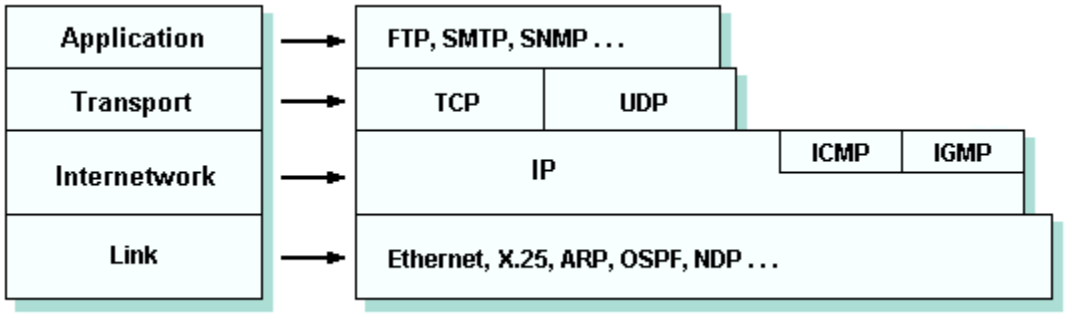
The primary purpose of the transport layer is to provide communication from one application program to another. The transport software divides the stream of data being transmitted into smaller pieces called packets in the ISO terminology and passes each packet along with the destination information to the next layer for transmission.

This layer consists of Transport Control Protocol (TCP), a connection-oriented transport service (COTS), and the user datagram protocol (UDP), a connectionless transport service (CLTS).

Application Layer

The application layer consists of user invoked application programs that access services available across a TCP/IP Internet. The application program passes data in the required form to the transport layer for delivery.

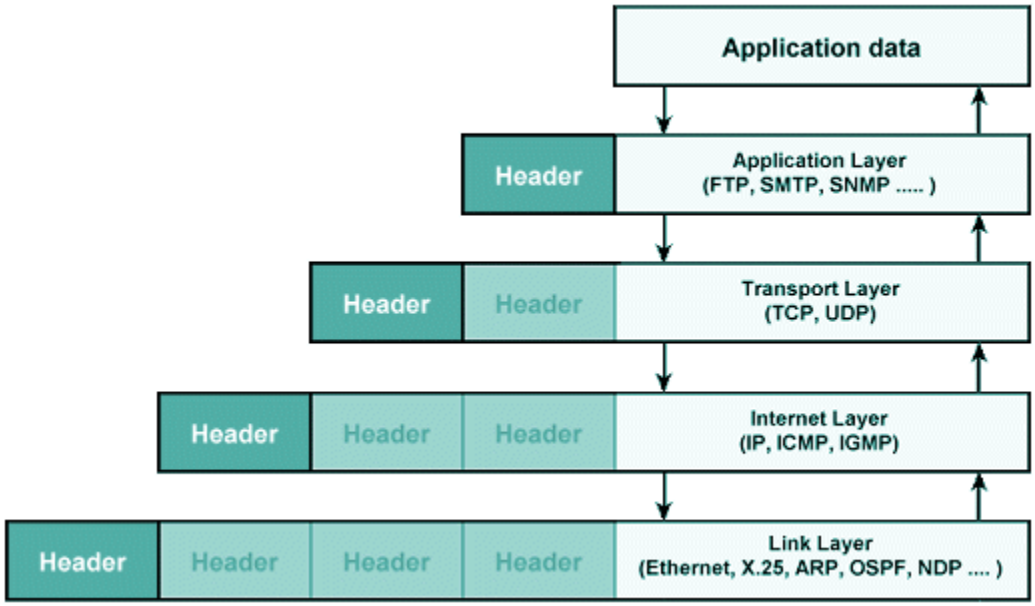
The TCP/IP protocol suite can be modelled as a layered protocol stack, allowing TCP/IP to be compared with other layered models such as the OSI Reference Model. The TCP/IP model has four layers. From lowest to highest, these are the link *layer*, the internet *layer*, the transport *layer*, and the application *layer*, as shown below.



- The full form or TCP/IP model explained as Transmission Control Protocol/ Internet Protocol.
- TCP supports flexible architecture
- Four layers of TCP/IP model are 1) Application Layer 2) Transport Layer 3) Internet Layer 4) Network Interface
- Application layer interacts with an application program, which is the highest level of OSI model.
- Internet layer is a second layer of the TCP/IP model. It is also known as a network layer.
- Transport layer builds on the network layer in order to provide data transport from a process on a source system machine to a process on a destination system.
- Network Interface Layer is this layer of the four-layer TCP/IP model. This layer is also called a network access layer.
- OSI model is developed by ISO (International Standard Organization) whereas TCP/IP model is developed by ARPANET (Advanced Research Project Agency Network).

- An Internet Protocol address that is also known as an IP address is a numerical label.
- HTTP is a foundation of the World Wide Web.
- SMTP stands for Simple mail transfer protocol which supports the e-mail is known as a simple mail transfer
- SNMP stands for Simple Network Management Protocol.
- DNS stands for Domain Name System.
- TELNET stands for Terminal Network. It establishes the connection between the local and remote computer
- FTP stands for File Transfer Protocol. It is a mostly used standard protocol for transmitting the files from one machine to another.
- The biggest benefit of TCP/IP model is that it helps you to establish/set up a connection between different types of computers.
- TCP/IP is a complicated model to set up and manage.

Encapsulation of data in the TCP/IP protocol stack



OSI Ref. Layer No.	OSI Layer Equivalent	TCP/IP Layer	TCP/IP Protocol Examples
5,6,7	Application, session, presentation	Application	NFS, NIS+,DNS, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP, and others
4	Transport	Transport	TCP, UDP
3	Network	Internet	IP, ARP, ICMP

OSI Ref. Layer No.	OSI Layer Equivalent	TCP/IP Layer	TCP/IP Protocol Examples
2	Data link	Data link	PPP, IEEE 802.2
1	Physical	Physical network	Ethernet (IEEE 802.3) Token Ring, RS-232, others

Most Common TCP/IP Protocols

Some widely used most common TCP/IP protocol are:

TCP:

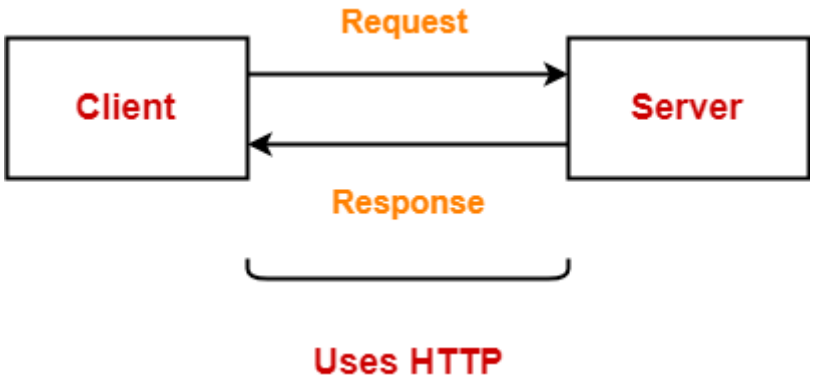
Transmission Control Protocol is an internet protocol suite which breaks up the message into TCP Segments and reassembling them at the receiving side.

IP:

An Internet Protocol address that is also known as an IP address is a numerical label. It is assigned to each device that is connected to a computer network which uses the IP for communication. Its routing function allows internetworking and essentially establishes the Internet. Combination of IP with a TCP allows developing a virtual connection between a destination and a source.

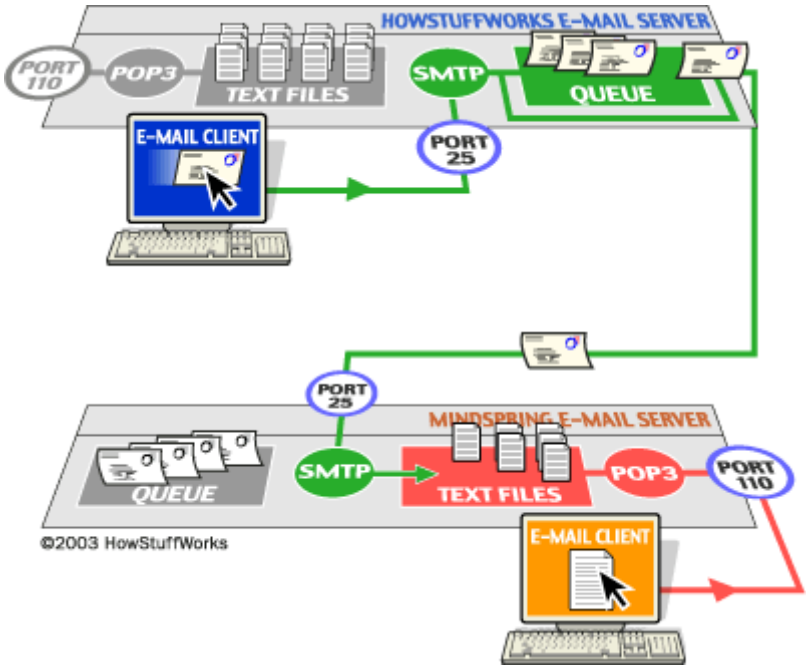
HTTP:

The Hypertext Transfer Protocol is a foundation of the World Wide Web. It is used for transferring webpages and other such resources from the HTTP server or web server to the web client or the HTTP client. Whenever you use a web browser like Google Chrome or Firefox, you are using a web client. It helps HTTP to transfer web pages that you request from the remote servers.



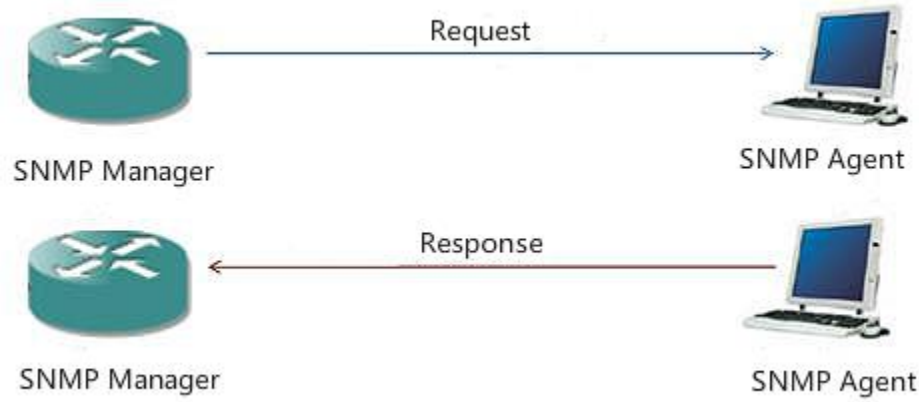
SMTP:

SMTP stands for Simple mail transfer protocol. This protocol supports the e-mail is known as a simple mail transfer protocol. This protocol helps you to send the data to another e-mail address.



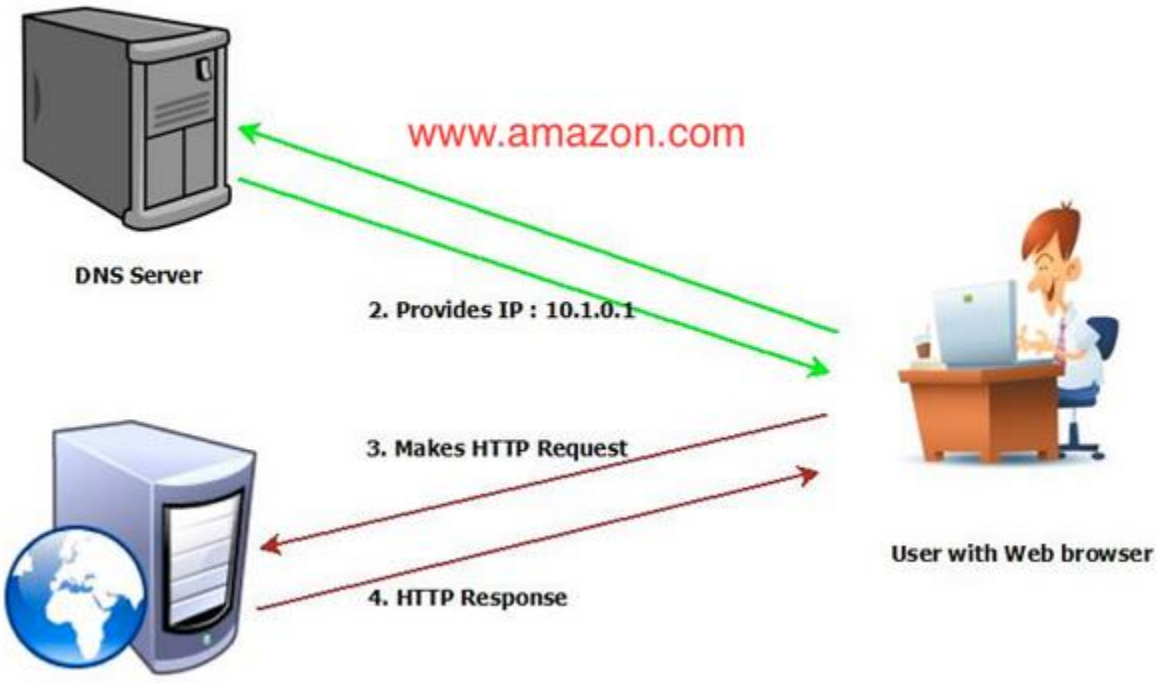
SNMP:

SNMP stands for Simple Network Management Protocol. It is a framework which is used for managing the devices on the internet by using the TCP/IP protocol.



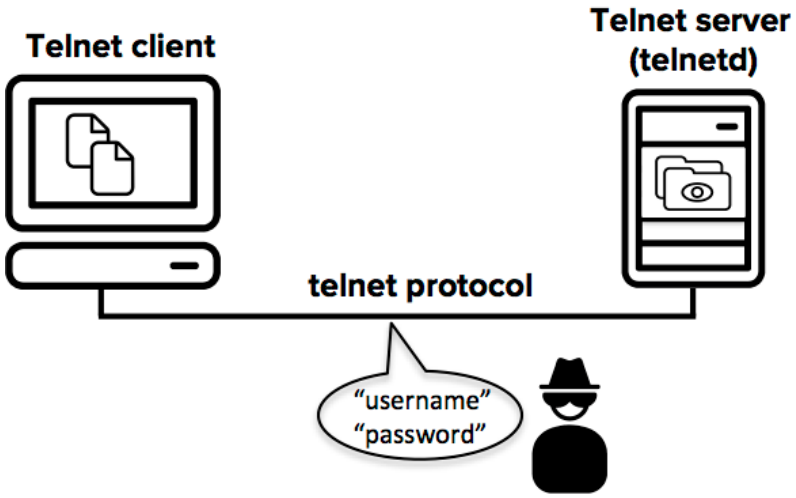
DNS:

DNS stands for Domain Name System. An IP address that is used to identify the connection of a host to the internet uniquely. However, users prefer to use names instead of addresses for that DNS.



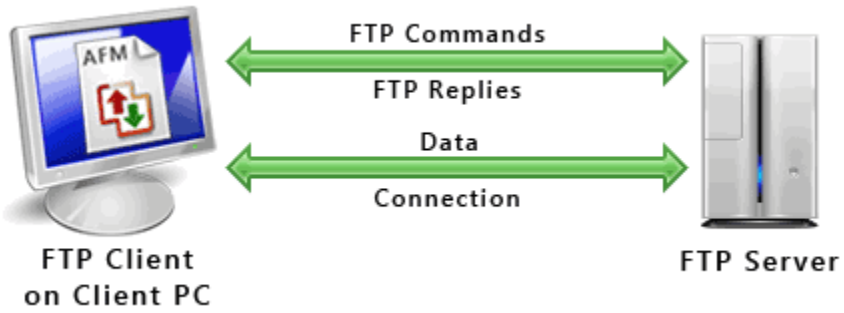
TELNET:

TELNET stands for Terminal Network. It establishes the connection between the local and remote computer. It established connection in such a manner that you can simulate your local system at the remote system.



FTP:

FTP stands for File Transfer Protocol. It is a mostly used standard protocol for transmitting the files from one machine to another.



Advantages of the TCP/IP model

Here, are pros/benefits of using the TCP/IP model:

- It helps you to establish/set up a connection between different types of computers.
- It operates independently of the operating system.
- It supports many routing-protocols.
- It enables the internetworking between the organizations.
- TCP/IP model has a highly scalable client-server architecture.
- It can be operated independently.
- Supports a number of routing protocols.
- It can be used to establish a connection between two computers.

Disadvantages of the TCP/IP model

Here, are few drawbacks of using the TCP/IP model:

- TCP/IP is a complicated model to set up and manage.
- The shallow/overhead of TCP/IP is higher-than IPX (Internetwork Packet Exchange).
- In this, model the transport layer does not guarantee delivery of packets.
- Replacing protocol in TCP/IP is not easy.
- It has no clear separation from its services, interfaces, and protocols.

TCP

The TCP stands for Transmission Control Protocol. If we want the communication between two computers and communication should be good and reliable. For example, we want to view a web page, then we expect that nothing should be missing on the page, or we want to download a file, then we require a complete file, i.e., nothing should be

missing either it could be a text or an image. This can only be possible due to the TCP. It is one of the most widely used protocols over the TCP/IP network.

Features of TCP

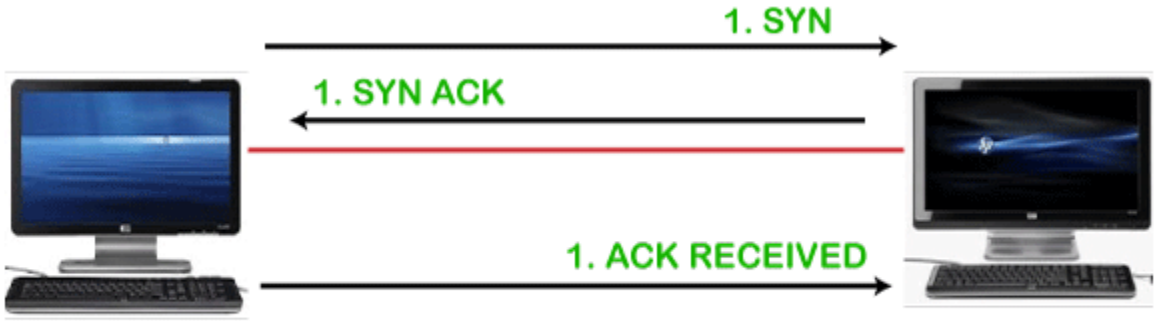
The following are the features of the TCP:

- **Data delivery**

  TCP protocol ensures that the data is received correctly, no data is missing and in order. If TCP protocol is not used, then the incorrect data can be received or out of order. For example, if we try to view the web page or download a file without using TCP, then some data or images could be missing.

- **Protocol**

  TCP is a connection-oriented protocol. Through the word connection-oriented**,** we understand that the computers first establish a connection and then do the communication. This is done by using a three-way handshake. In a three-way handshake**,** the first sender sends the SYN message to the receiver then the receiver sends back the SYN ACK message to confirm that the message has been received. After receiving the SYN ACK message, the sender sends the acknowledgment message to the receiver. In this way, the connection is established between the computers. Once the connection is established, the data will be delivered. This protocol guarantees the data delivery means that if the data is not received then the TCP will resend the data.

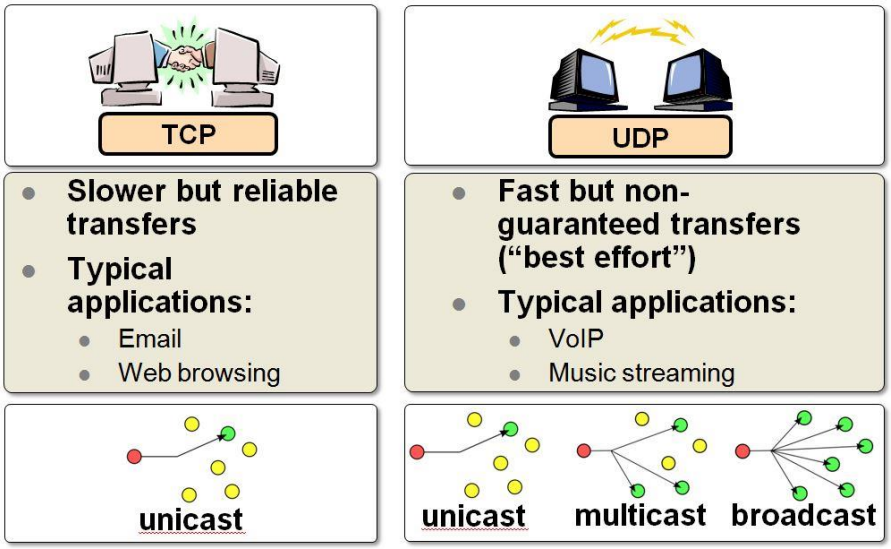


Connection oriented protocol

UDP

The UDP stands for User Datagram Protocol. Its working is similar to the TCP as it is also used for sending and receiving the message. The main difference is that UDP is a

connectionless protocol. Here, connectionless means that no connection establishes prior to communication. It also does not guarantee the delivery of data packets. It does not even care whether the data has been received on the receiver's end or not, so it is also known as the "fire-and-forget" protocol. It is also known as the "fire-and-forget" protocol as it sends the data and does not care whether the data is received or not. UDP is faster than TCP as it does not provide the assurance for the delivery of the packets.



UDP is best suited for applications that require speed and efficiency.

- VPN tunneling
- Streaming videos
- Online games
- Live broadcasts
- Domain Name System (DNS)
- Voice over Internet Protocol (VoIP)
- Trivial File Transfer Protocol (TFTP)

Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
It is a connection-oriented protocol, which means that the connection needs to be established before the data is transmitted over the network.	It is a connectionless protocol, which means that it sends the data without checking whether the system is ready to receive or not.

TCP is a reliable protocol as it provides assurance for the delivery of data packets.	UDP is an unreliable protocol as it does not take the guarantee for the delivery of packets.
TCP is slower than UDP as it performs error checking, flow control, and provides assurance for the delivery of	UDP is faster than TCP as it does not guarantee the delivery of data packets.
The size of TCP is 20 bytes.	The size of the UDP is 8 bytes.
TCP uses the three-way-handshake concept. In this concept, if the sender receives the ACK, then the sender will send the data. TCP also has the ability to resend the lost data.	UDP does not wait for any acknowledgment; it just sends the data.
It follows the flow control mechanism in which too many packets cannot be sent to the receiver at the same time.	This protocol follows no such mechanism.
TCP performs error checking by using a checksum. When the data is corrected, then the data is retransmitted to the receiver.	It does not perform any error checking, and also does not resend the lost data packets.
This protocol is mainly used where a secure and reliable communication process is required, like military services, web browsing, and e-mail.	This protocol is used where fast communication is required and does not care about the reliability like VoIP, game streaming, video and music streaming, etc.

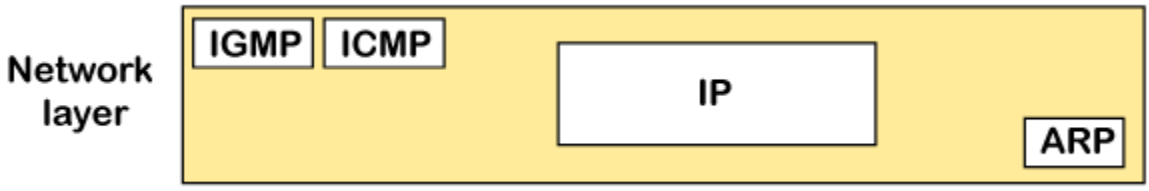
ICMP Protocol

The ICMP stands for Internet Control Message Protocol. It is a network layer protocol. It is used for error handling in the network layer, and it is primarily used on network

devices such as routers. As different types of errors can exist in the network layer, so ICMP can be used to report these errors and to debug those errors.

The primary purpose of ICMP is for error reporting. When two devices connect over the Internet, the ICMP generates errors to share with the sending device in the event that any of the data did not get to its intended destination. For example, if a packet of data is too large for a router, the router will drop the packet and send an ICMP message back to the original source for the data.

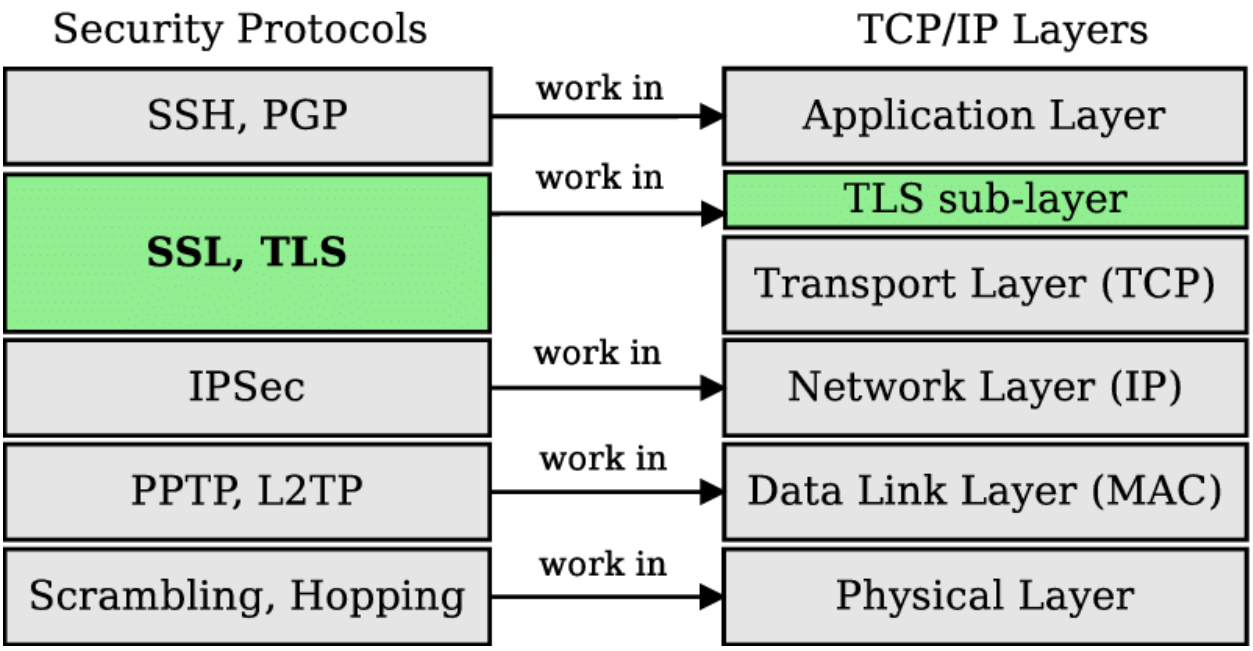
The ICMP resides in the **IP** layer, as shown in the below diagram.



The ICMP messages are usually divided into two categories:

ICMP messages

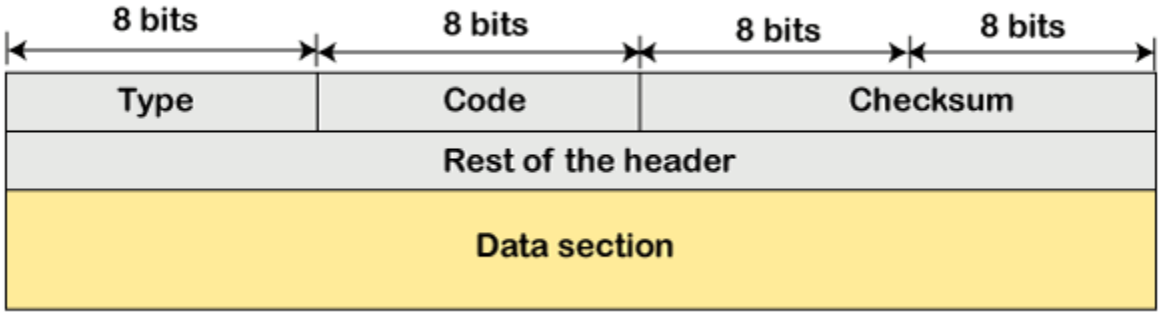
Category	Type	Message
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply



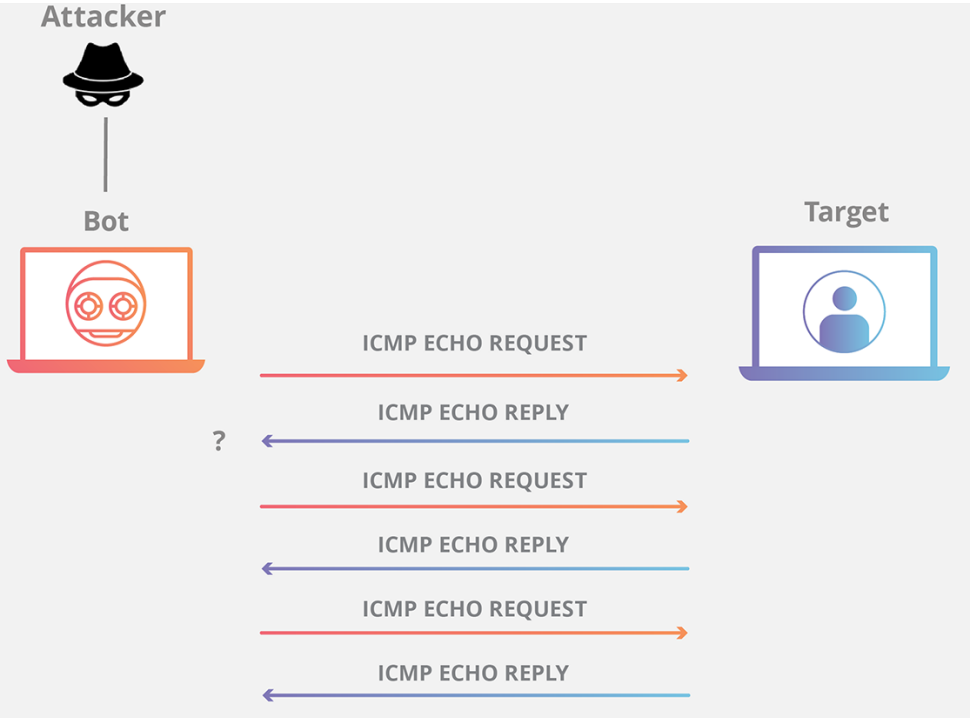
ICMP Message Format

The message format has two things; one is a category that tells us which type of message it is. If the message is of error type, the error message contains the type and the code. The type defines the type of message while the code defines the subtype of the message.

The ICMP message contains the following fields:



ICMP flood attack:



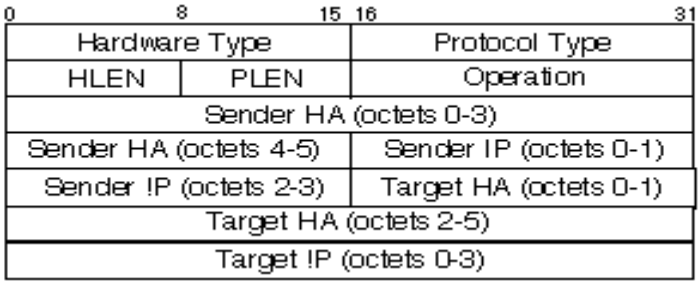
Address Resolution Protocol (ARP)

The Address Resolution Protocol (Arp) is a protocol used by the Internet Protocol (IP) [RFC826], specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol. The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer. It is used when IPv4 is used over Ethernet.

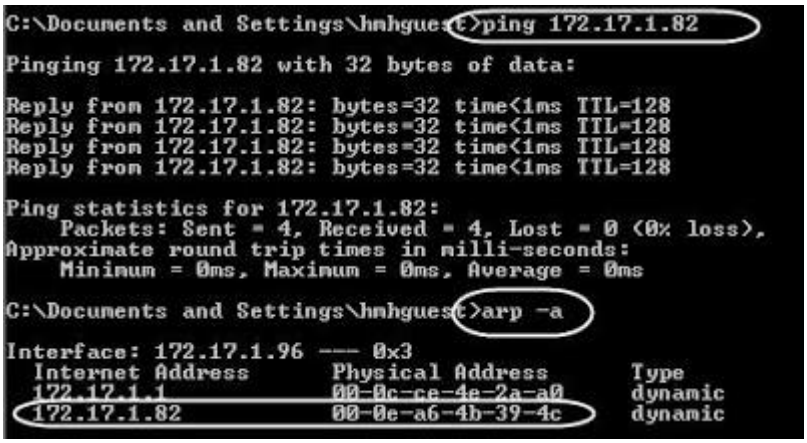
There are four types of arp messages that may be sent by the arp protocol. These are identified by four values in the "operation" field of an arp message. The types of message are:

1. ARP-Request (Broadcast, source IP address of the requester)
2. ARP-Reply (Unicast to requester, the target)

The format of an arp message is shown below:

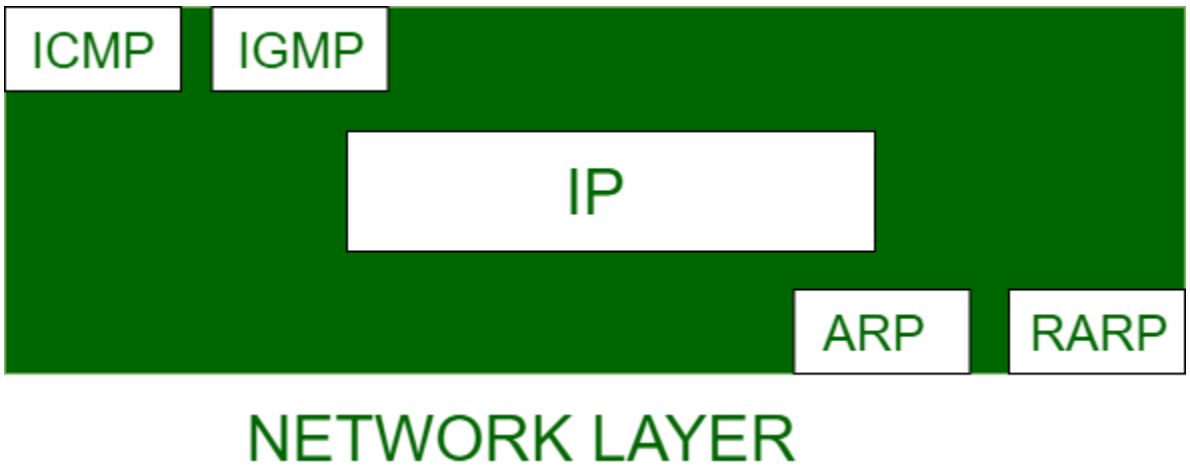


Most of the computer programs/applications use logical address (IP address) to send/receive messages, however the actual communication happens over the physical address (MAC address**)** i.e from layer 2 of OSI model. So our mission is to get the destination MAC address which helps in communicating with other devices. This is where ARP comes into the picture, its functionality is to translate IP address to physical address.



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

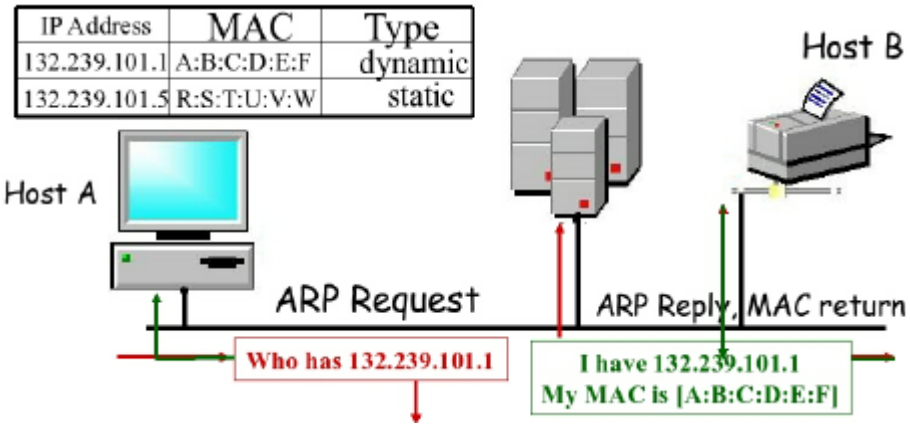
Note: ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address.



The important terms associated with ARP are:

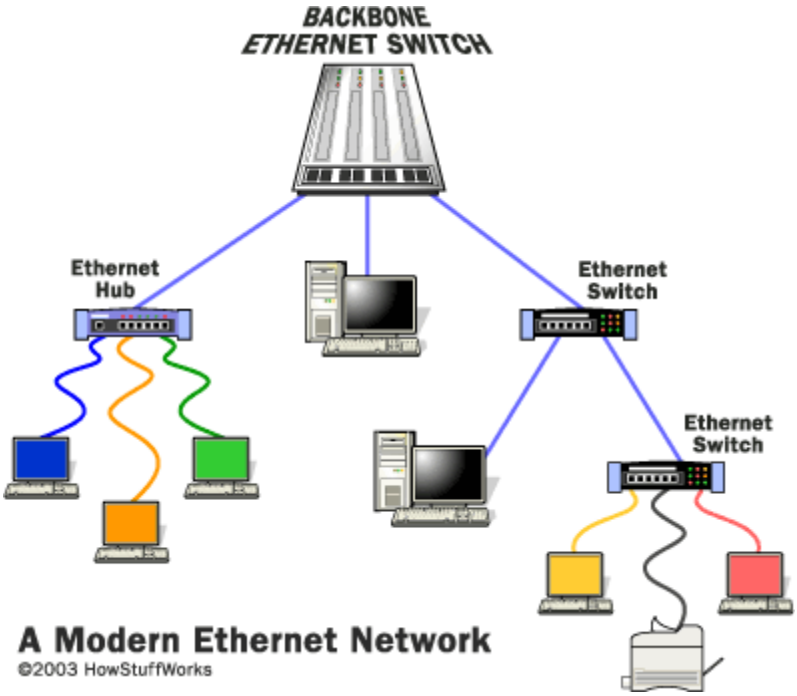
1. **ARP Cache:** After resolving MAC address, the ARP sends it to the source where it stores in a table for future reference. The subsequent communications can use the MAC address from the table
2. **ARP Cache Timeout:** It indicates the time for which the MAC address in the ARP cache can reside

3. **ARP request:** This is nothing but broadcasting a packet over the network to validate whether we came across destination MAC address or not.
    1. The physical address of the sender.
    2. The IP address of the sender.
    3. The physical address of the receiver is FF:FF:FF:FF:FF:FF or 1's.
    4. The IP address of the receiver
4. **ARP response/reply:** It is the MAC address response that the source receives from the destination which aids in further communication of the data.



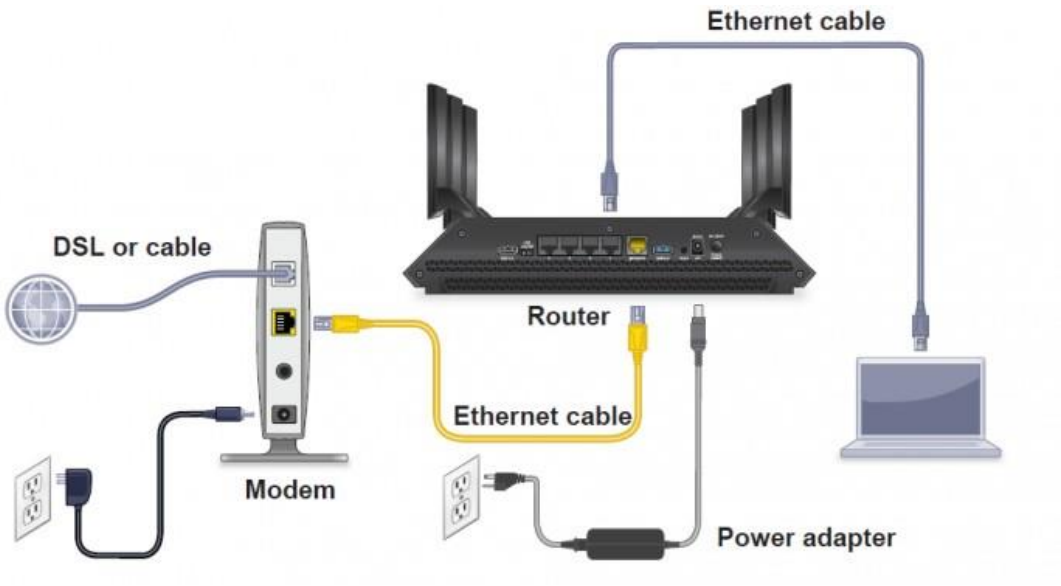
Ethernet

Ethernet is a technology that connects wired local area networks (LANs) and enables the device to communicate with each other through a protocol which is the common network language. This LAN is a network of computers and other electronic devices which covers a small area in your places like in the office, house, room or building. Unlike LAN, wide area network (WAN) covers much larger geographical areas. Furthermore, Ethernet is a protocol that controls the processes on how the data is transmitted through LAN. It also indicates how the network devices can transmit and format data packets so that the other network devices in the same area network segment can be able to receive, process and recognize them.



The following are the different types of Ethernet cables:

- 10Base2 – thin Ethernet
- 10Base 5 – thin Ethernet
- 10Base-T – Twisted-pair cable and can achieve a speed of 10 Mbps
- 100Base-FX- this makes possible in achieving a speed of 100 Mbps through multimode fiber optic.
- 100Base-TX- similar to twisted-pair cable but with a 10 times greater speed.
- 1000Base-T- double twisted-pair cable of category 5 cables that allows a speed up to one Gigabit per second.
- 1000Base-SX- this is based on multimode fiber optic that uses a short wavelength signal of 850 nanometers.
- 1000Base-LX – this is also based on multimode fiber optic but uses a long wavelength signal.



Ethernet Networks

The following are the different types of Ethernet networks:

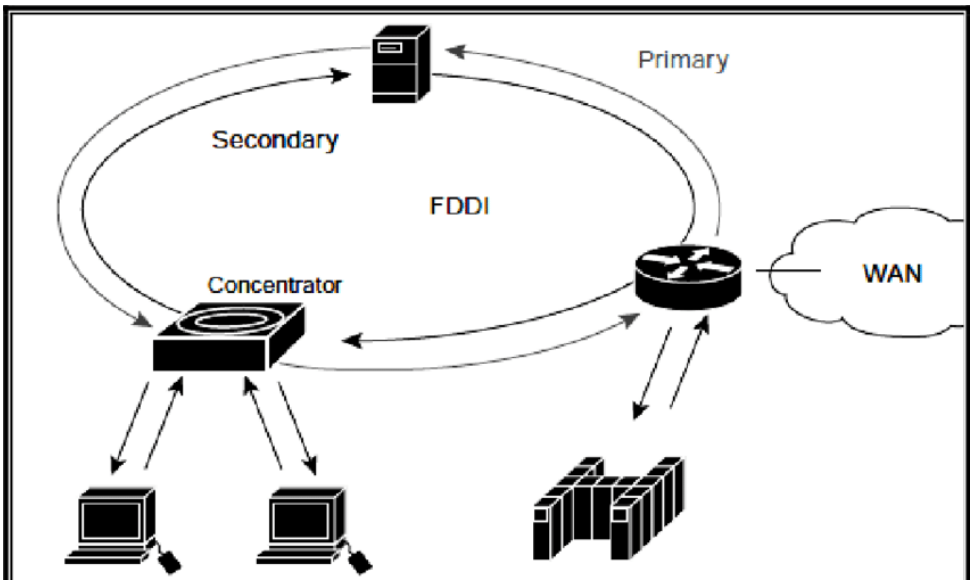
Fast Ethernet
This is a type of Ethernet network that can transmit data at a rate of 100 Mbps through a twisted-pair cable or fiber-optic cable. The data can be transferred from 10 Mbps to 100 Mbps with no protocol translation or changes in the application and networking software.

Gigabit Ethernet
This is a type of Ethernet network that has the capability to transfer data at a rate of 1000 Mbps based on a twisted-pair cable or fiber-optic cable. Among other types of Ethernet cable, this is the most popular one.

Switch Ethernet
This is a piece of network equipment that is required for multiple network devices in a LAN. In using this type of cable, a regular network cable shall be used instead of a crossover cable. This Ethernet cable forwards the data from one device to another device with the same network. Normally, this supports different data transfer rates. Ethernet is widely used as a network technology due to the fact that the cost of such a network is not too high

Fiber Distributed Data Interface (FDDI)

Fiber Distributed Data Interface (FDDI) is a standard for data transmission in a local area network. It uses optical fiber as its standard underlying physical medium, although it was also later specified to use copper cable, in which case it may be called CDDI (Copper Distributed Data Interface), standardized as TP-PMD (Twisted-Pair Physical Medium-Dependent), and also referred to as TP-DDI (Twisted-Pair Distributed Data Interface).



The FDDI data frame format is:

PA	SD	FC	DA	SA	PDU	FCS	ED/FS
16 bits	8 bits	8 bits	48 bits	48 bits	up to 4478×8 bits	32 bits	16 bits

Where **PA** is the preamble, **SD** is a start delimiter, **FC** is frame control, **DA** is the destination address, **SA** is the source address, **PDU** is the protocol data unit (or packet data unit), **FCS** is the frame check Sequence (or checksum), and **ED/FS** are the end delimiter and frame status.

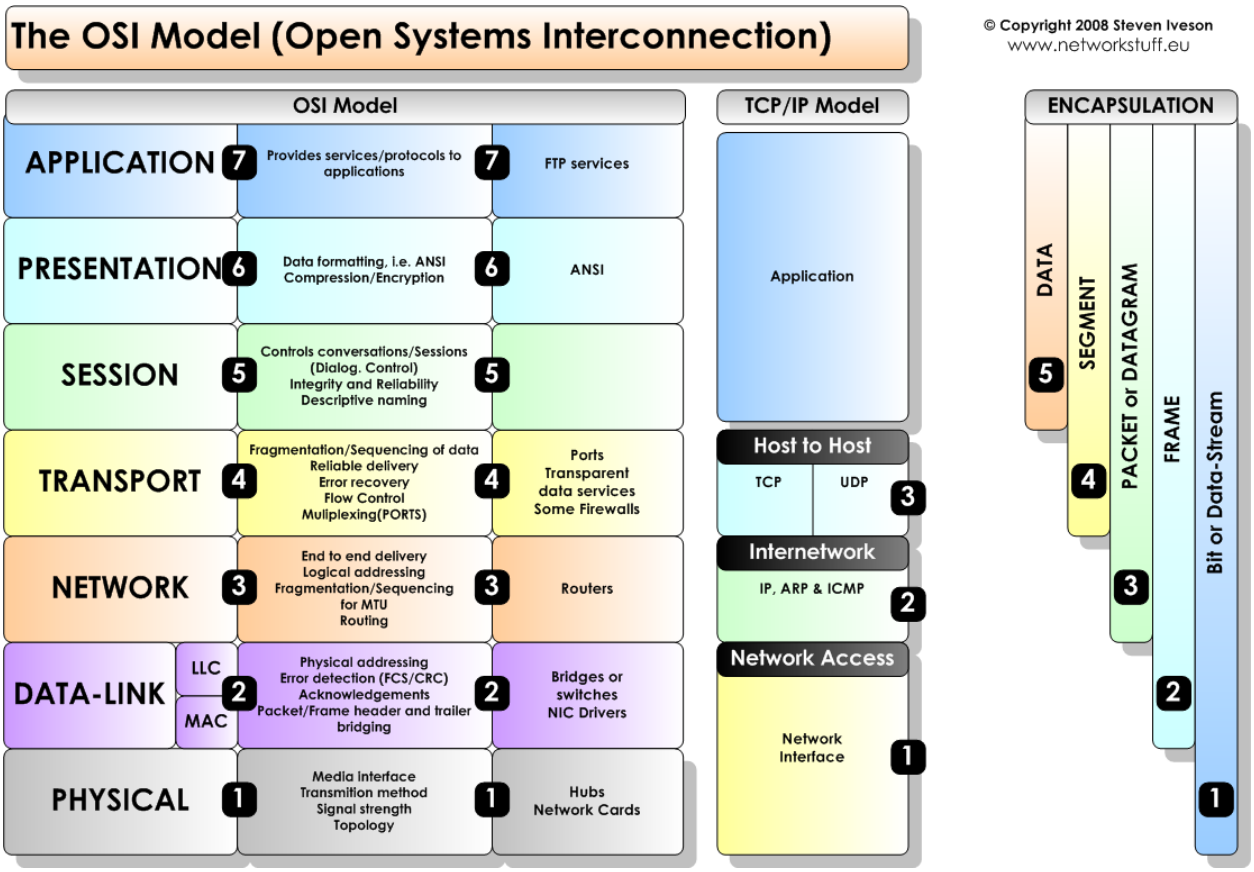
Token Ring

Token ring (IEEE 802.5) is a communication protocol in a local area network (LAN) where all stations are connected in a ring topology and pass one or more tokens for channel acquisition. A token is a special frame of 3 bytes that circulates along the ring of stations. A station can send data frames only if it holds a token. The tokens are released on successful receipt of the data frame.

Differences between Token Ring and Token Bus

Token Ring	Token Bus
The token is passed over the physical ring formed by the stations and the coaxial cable network.	The token is passed along the virtual ring of stations connected to a LAN.
The stations are connected by ring topology, or sometimes star topology.	The underlying topology that connects the stations is either bus or tree topology.
It is defined by IEEE 802.5 standard.	It is defined by IEEE 802.4 standard.
The maximum time for a token to reach a station can be calculated here.	It is not feasible to calculate the time for token transfer.

Comparing OSI and TCP/IP



The Internet protocol was developed prior to the development of the OSI reference model. That is the reason the OSI model and Internet protocol model does not match with each other. The Internet Protocol has four layers; they are physical layer, network layer, transport layer, and application layer. The first four layers provide physical standards,

network interface, internetworking and the transport procedures, which are similar to the function of the four layers of the OSI model.

In Internet protocol, the application layer, presentation layer, and session layer are put together as the application layer. The Internet protocol has specific interactive functions at each layer of the suite, whereas the OSI reference model has specific functions for each layer. The protocols of Internet protocol are comparatively independent when they are compared to the OSI model protocols. The interactions between the protocols of the TCP/IP suite depend on the needs of the system. The upper layer protocols are supported by one or lower layer protocols.

In the transport layer of the TCP/IP suite, two protocols have been defined; they are TCP (Transmission Control Protocol) and UDP (User Datagram protocol). At the network layer, the main protocol defined is Internetworking protocol (IP).

OSI Model	**TCP/IP model**
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI model use two separate layers physical and data link to define the functionality of the bottom layers.	TCP/IP uses only one layer (link).
OSI layers have seven layers.	TCP/IP has four layers.
OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In the OSI model, the data link layer and physical are separate layers.	In TCP, physical and data link are both combined as a single host-to-network layer.
Session and presentation layers are not a part of the TCP model.	There is no session and presentation layer in TCP model.

It is defined after the advent of the Internet.	It is defined before the advent of the internet.
The minimum size of the OSI header is 5 bytes.	Minimum header size is 20 bytes.

Network Security

Network security consists of all the processes, policies, and techniques to detect and prevent unauthorized access of a network and other network resources.

The Major Requirements of Network Security

Availability: Legitimate users have access when desired

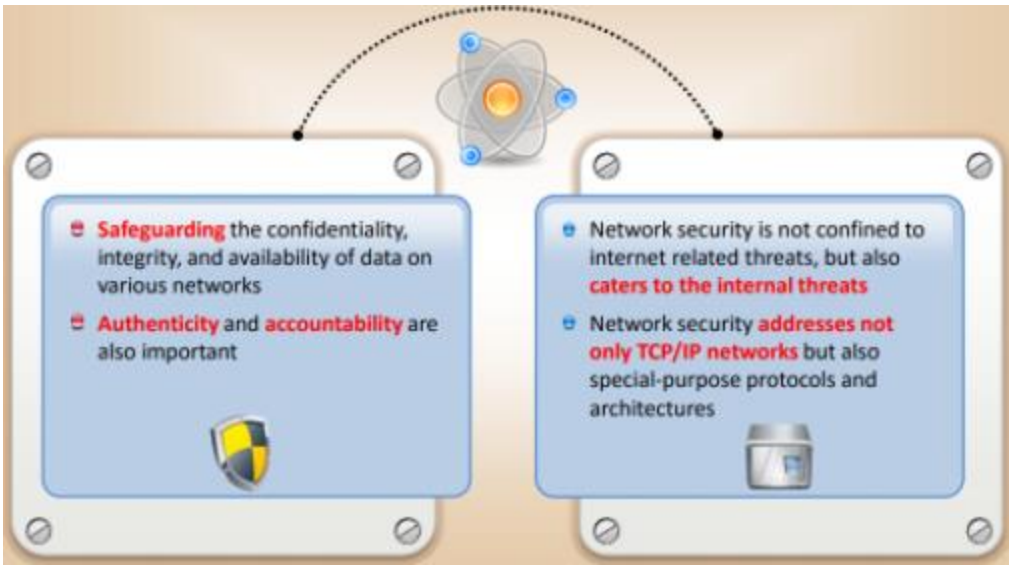
Non-repudiation: Unable to deny the action

Integrity Maintaining: Data consistency

Authentication: Verifying credentials

Access Control: Access only to authorized users

Confidentiality: Not disclosed to unauthorized users



The various essential components required for network security policy are:

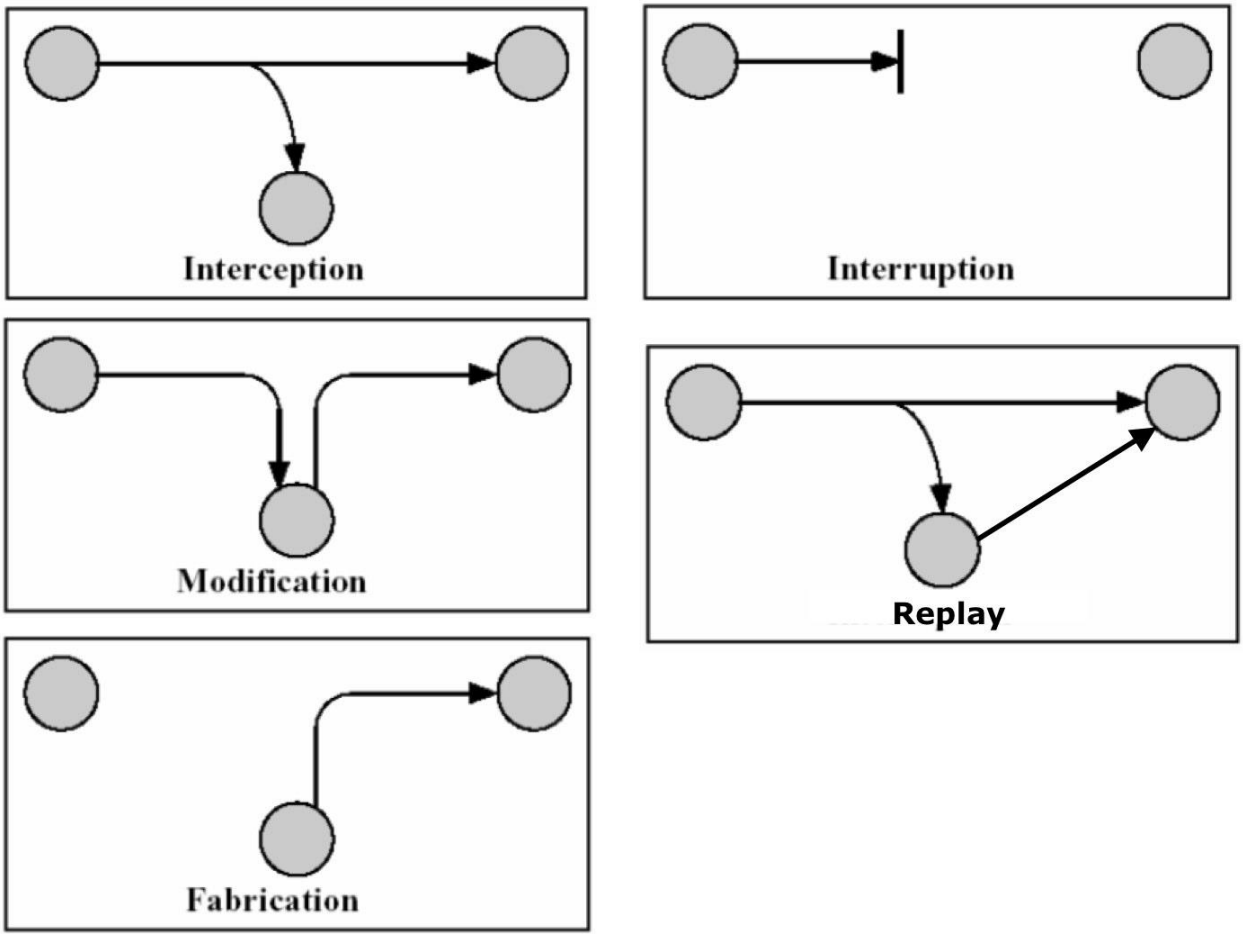
Physical Security: Network security works with the physical security as the physical characteristics of the network can cover a building, campus, country, or the world. If the physical security is threatened then the network security issues such as the confidentiality, availability, and integrity cannot be properly safeguarded. The physical security helps in protecting the network devices and other services that are offered by the network. It also helps in determining the authorization to the employees to the restricted areas.

Network Security: The network security addresses the issues regarding the protection levels that are employed for various assets. It also addresses various security procedures concerning access controls, firewalls, network auditing, remote access, directory services, Internet services, and file system directory structures.

Access Control: Access control decides who can access the network and to what extent the access is legal. An ingenious access control can access and manage the remote access and it also helps the administrator in performing their jobs efficiently. It should also ensure that the right person accesses the right resources or information.

Authentication: This component is an interface through which the user can identify him/her to the network. The authentication varies depending on the user and location.

Data Security Threats over a Network



Various data security threats that breach the network security policies are:

Data Interruption

This threat occurs when an unauthorized end user interrupts data transmission on a network. As a result, the transmitted data does not reach the intended recipient.

Data Modification

This threat occurs when an unauthorized end user intercepts the transmitted data, modifies it, and then retransmits the modified data to the intended recipient. The intended recipient does not receive the original data.

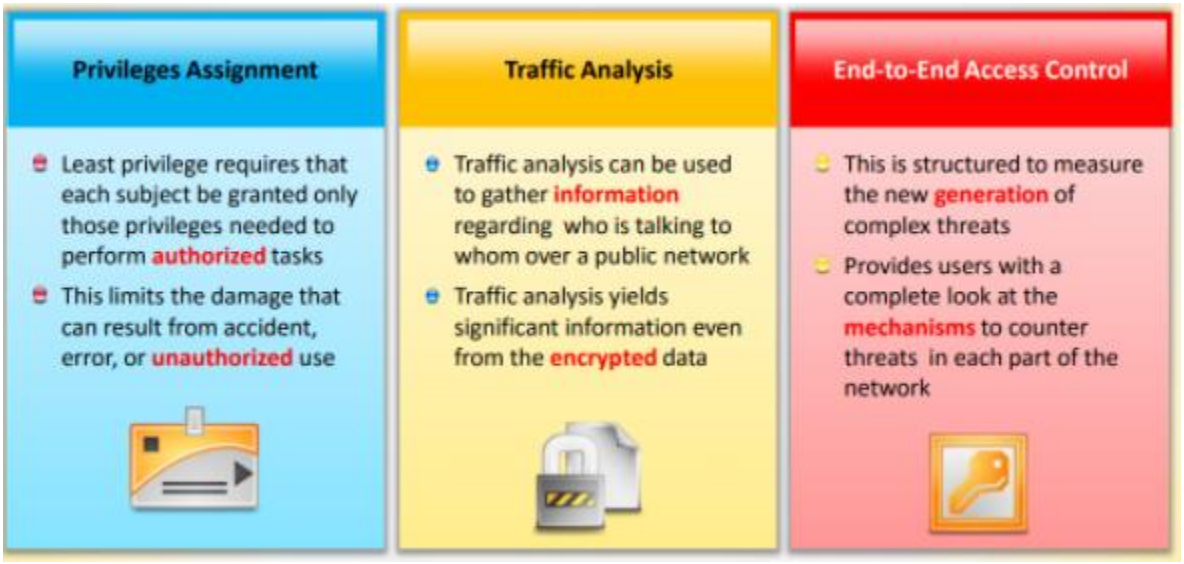
Data Fabrication

This occurs when an unauthorized end user transmits data using the identity of an authorized sender. In this case, the authorized sender is unaware of the data transmission. The recipient receives the data and presumes that the authorized sender has sent it.

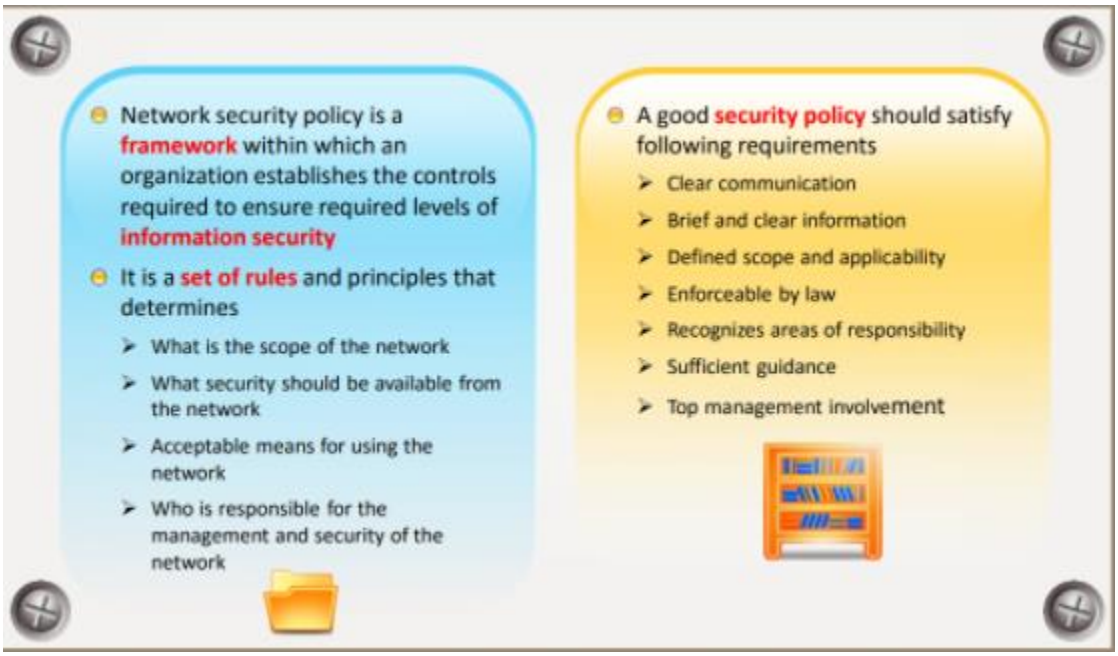
Data Interception

This occurs when an unauthorized end user intercepts data transmission. As a result, the unauthorized end user, in addition to the intended recipient, can access the transmitted data.

Basic Network Security Procedures



Network Security Policies



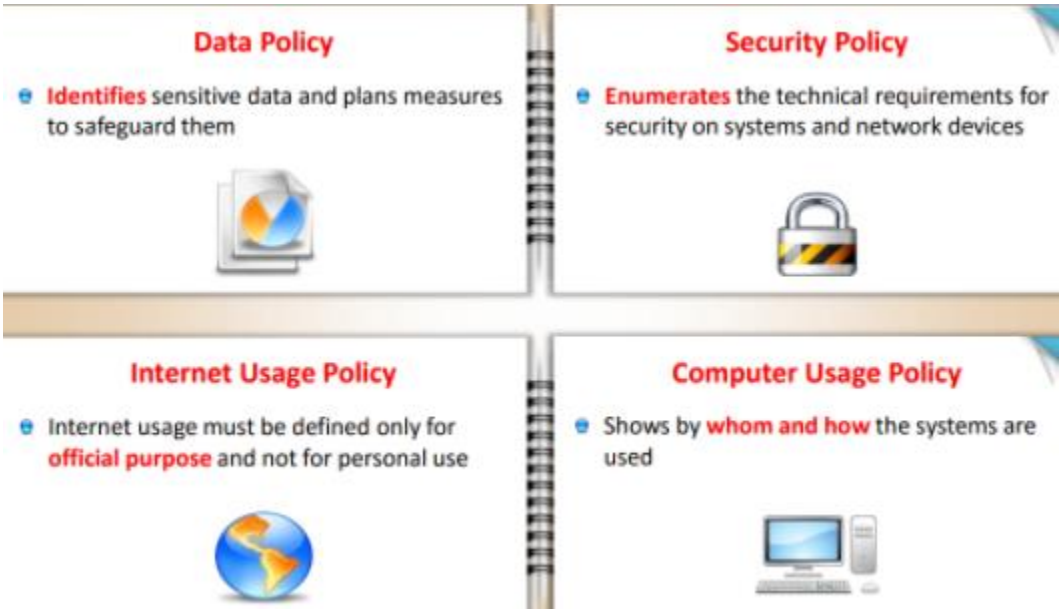
To establish a secured network, a well-designed network policy has to be established.

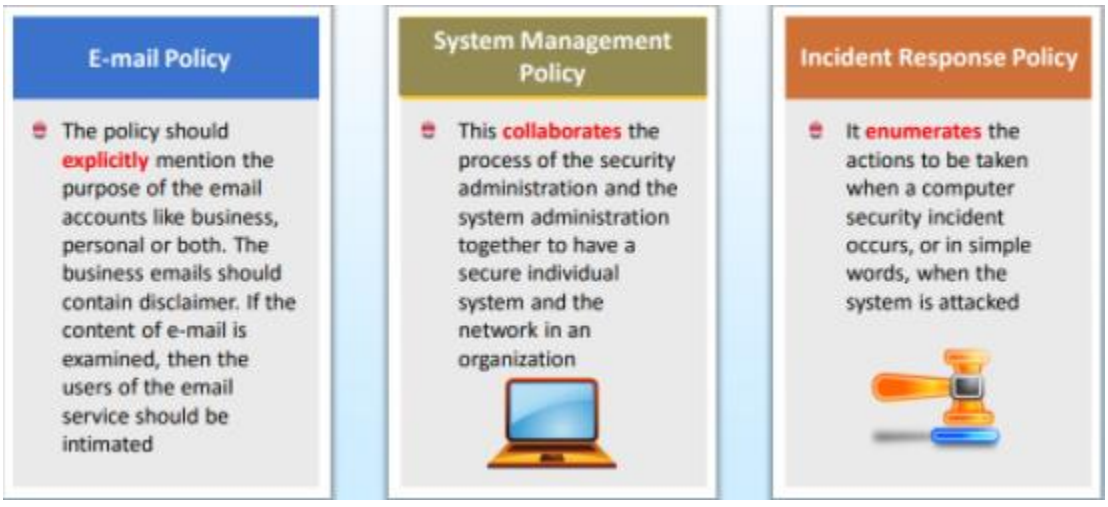
The network policy characterizes the organization's idea of an apt computer, usage of the network, and measures to deal with the network incidents. The organizations rely heavily on the network security as it summarizes the assets, which require maximum security and the strategy is formulated based on the actions and inactions that threaten

the assets. Hence, network security policy is considered as the base of the organization's security. The policy helps in determining the probable threat to the personal productivity and efficiency. It also determines the various corporate assets and suggests levels of security to protect the assets. A well-designed network security policy helps in establishing a proper network security framework. Permitting the employees to access the established standards and security controls can augment the efficiency. The employees and the third party users must be communicated about the network security policy to avoid the complications after breaching the policy unknowingly. It is a set of rules and principles that determines:

- What is the scope and objective of the network and what is not?
- What are the levels of security that should be available from the network?
- What are the various acceptable means for using the network?
- Who is responsible for the management and security of the network?

Types of Network Security Policies





IP Addressing

IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32 bit unique address having an address space of 2^{32}. Generally, there are two notations in which IP address is written, dotted decimal notation and hexadecimal notation.
An IP address (*internet protocol address*) is a numerical representation that uniquely identifies a specific interface on the network.
Addresses in IPv4 are 32-bits long. This allows for a maximum of 4,294,967,296 (2^{32}) unique addresses. Addresses in IPv6 are 128-bits, which allows for 3.4 x 10^{38} (2^{128}) unique addresses.

The total usable address pool of both versions is reduced by various reserved addresses and other considerations.

IP addresses are binary numbers but are typically expressed in decimal form (IPv4) or hexadecimal form (IPv6) to make reading and using them easier for humans.

Dotted Decimal Notation:

Classful Addressing
The 32 bit IP address is divided into five sub-classes. These are:

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

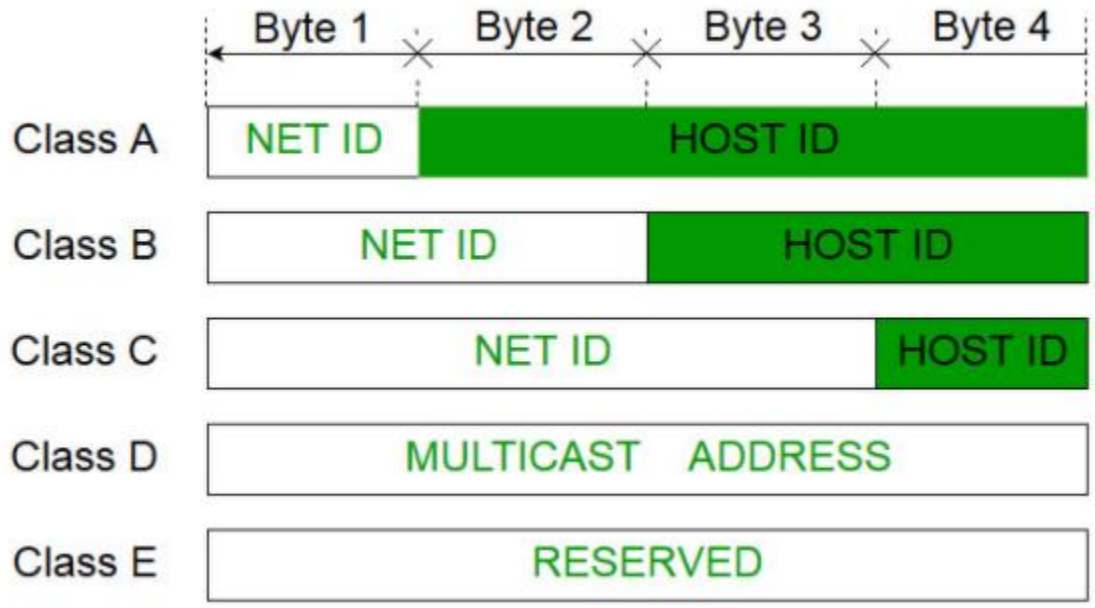
Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.

Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental
Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback testing.		

IPv4 address is divided into two parts:

- **Network ID**
- **Host ID**

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns IP address to each device that is connected to its network.



Note: IP addresses are globally managed by Internet Assigned Numbers Authority (IANA) and regional Internet registries (RIR).
Note: While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

Class A:

IP address belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

The higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for class A is 255.x.x.x. Therefore, class A has a total of:

- 2^7-2= 126 network ID(Here 2 address is subracted because 0.0.0.0 and 127.x.y.z are special address.)
- 2^24 – 2 = 16,777,214 host ID

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

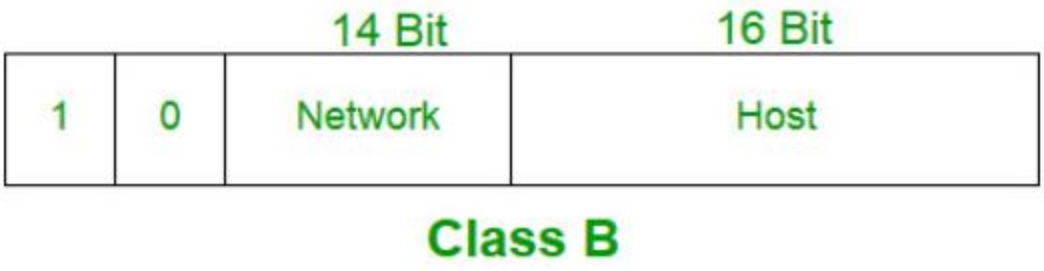
Class B:
IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.

- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network. The default sub-net mask for class B is 255.255.x.x. Class B has a total of:

- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address

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



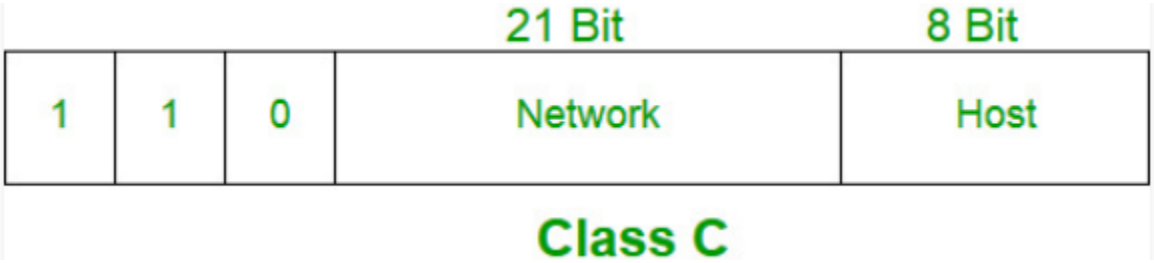
Class C:
IP address belonging to class C are assigned to small-sized networks.

- The network ID is 24 bits long.
- The host ID is 8 bits long.

The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:

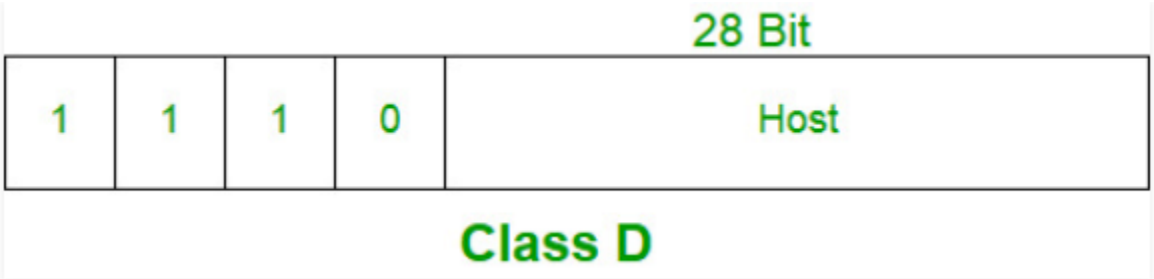
- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address

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



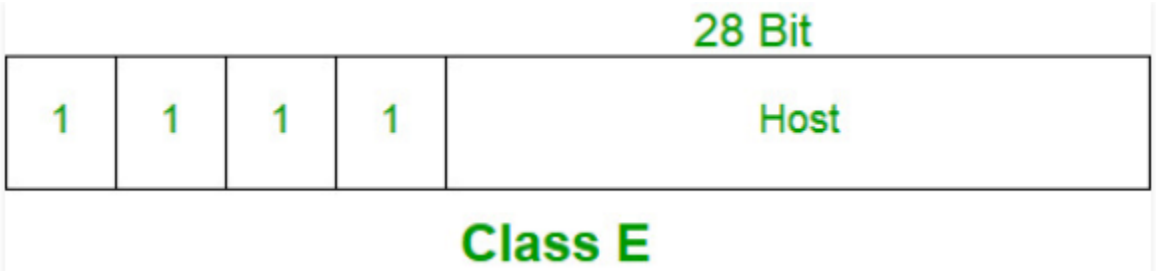
Class D:
IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.

Class D does not possess any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.



Class E:
IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254. This class doesn't

have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.



Range of special IP addresses:

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

Rules for assigning Host ID:

Host ID's are used to identify a host within a network. The host ID are assigned based on the following rules:

- Within any network, the host ID must be unique to that network.
- Host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

Rules for assigning Network ID:

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:

- The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loop-back functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Classful addressing

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Important terms in IP addressing

Default Network: The default IP address is 0.0.0.0 in the default network.

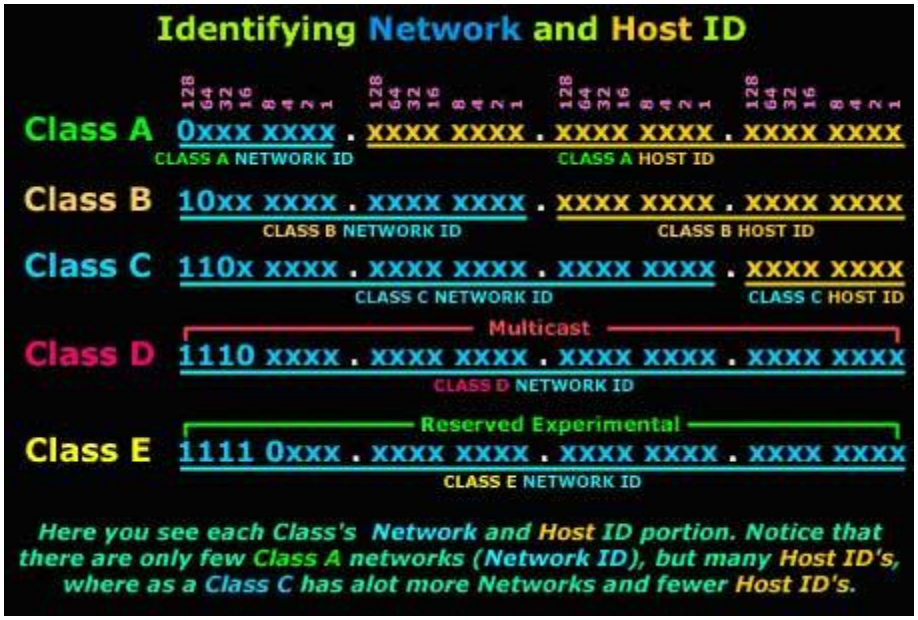
Loopback Address: The loopback address is a unique IP address (127.0.0.1) designed for network testing, where a network administrator sends packets to the device to identify problems during transmission.

Broadcast Address: A broadcast address is a unique IP address (255.255.255.255) designed for sending messages to all the nodes in a network. A network administrator uses this address to send a common message to all the hosts residing in a network.

Internet Corporation for Assigned Names and Numbers (ICANN): The Internet Corporation for Assigned Names and Numbers (ICANN) is the authority that manages the assignment of IP addresses, IP address spaces, and Protocol Identifier Assignments. The aim of ICANN is to ensure that all the users have valid addresses. ICANN does not look after Internet content control, data protection, or unsolicited mail, but ICANN is responsible for the management of the new gTLDS (generic Top Level Domains).

Making the Address Space Friendly: In order to make the address space friendly, it is necessary to make the address familiar and short. The information in the Internet includes only two symbols: “1” and “0.” These describe the two possible states: on/off. The base10 number system is user friendly. Imagine that a computer’s address is 4.27.28.123.12. It is easier to remember the binary equivalent of that address in the Base2 system: 10010000, 11111010, 01010101, and 10111011.

Purpose of Dots: It can be difficult to remember a particular decimal number address. To make it easier to remember, the decimal is divided into four parts. With the logical classification of the address, it is easier to identify a particular host on the network. The scheme depends on the decimal number and the address space using binary. Certain schemes use binary numbers; others use the decimal numbers directly. Therefore, the 32-bit address space has four equal components of 8 bits each, such as 202.53.13.138.



Subnet Masking

A subnet mask provides information about the division of bits between the subnet ID and the host ID, as well as the host ID containing the routing traffic. It is a 32-bit binary number. A subnet mask separates the IP address into two components, namely the network address and the host address. Use the subnet calculator to retrieve the subnet mask information. The subnet mask performs bitwise AND operations on the net mask to identify the network address of a particular IP address. Subnet mask bits are defined by setting network bits to all "1s" and setting host bits to all "0s." Subnet masks are expressed using dot-decimal notation like an address. Every host on the TCP/IP network requires a subnet mask. Use a default subnet mask for the class-based network IDs and use custom subnet masks when subnetting and supernetting is configured.

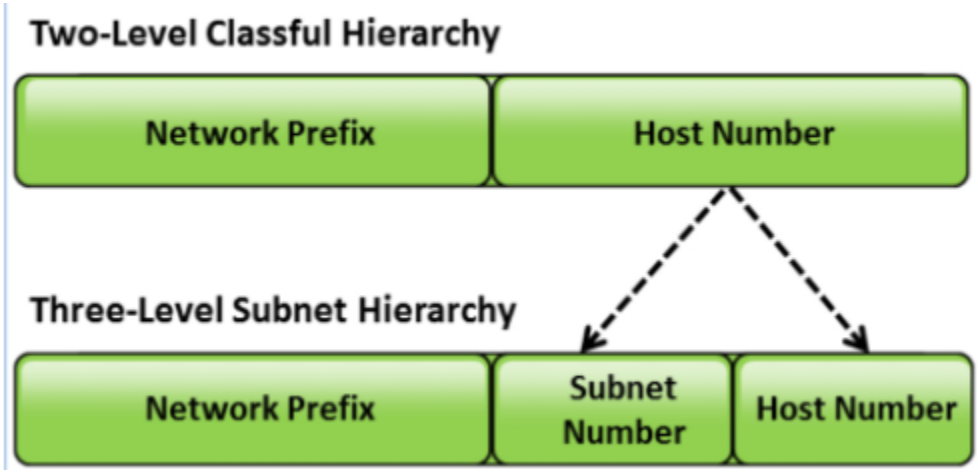
IP Address Class	Total # bits for Network ID/Host ID	Default Subnet Mask			
		First Octet	Second Octet	Third Octet	Fourth Octet
Class A	8/24	11111111	00000000	00000000	00000000
Class B	16/16	11111111	11111111	00000000	00000000
Class C	24/8	11111111	11111111	11111111	00000000

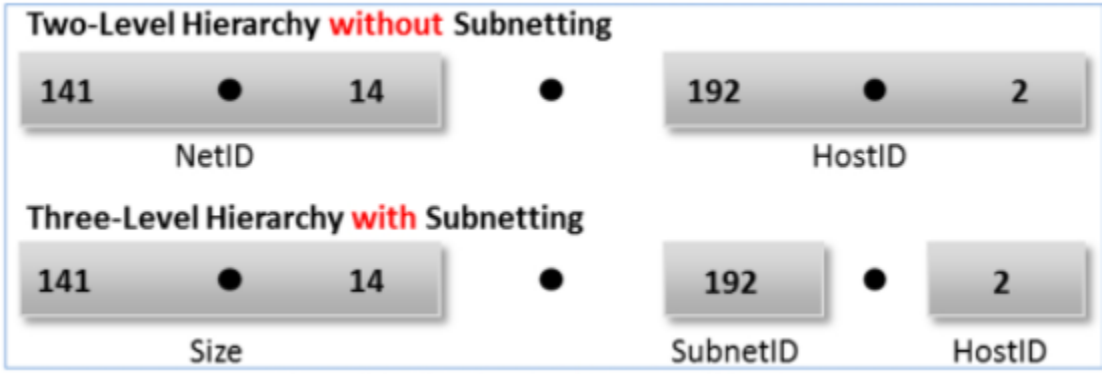
Subnetting

The original Internet designers did not foresee the rapid growth of the Internet and the change it created as a communication system. Today, organizations are facing many problems with allocation of IP addresses, as the IP address space, especially IPv4, as it is in the depletion stage. This problem has occurred due to early decisions made by the Internet designers in the formative stages. In the early evolution stage of the Internet, organizations were allocated address space based on their request rather than on their requirements. This has led to the eventual depletion of the IP address space. Many

organizations that predicted the future of networking invested in the Internet; however, organizations that ignored the significance of the Internet later realized and obtained addresses, but had to face problems with address-shortage issues. Emerging organizations that are in the evolving stage have to face address-storage problems due to premature depletion of the IPv4 address space. In order to overcome the problems of IP address space depletion, one can perform IP subnetting.

Subnetting allows an organization's network to be divided into a two-level structure—hosts and subnets. An organization's system administrator divides the host network, specifically the internal network, into two segments in order to make it unavailable to the external networks. The main advantage of subnetting to the organization is that they can divide the classful host number into a subnet ID and host ID based on their preferences and requirements



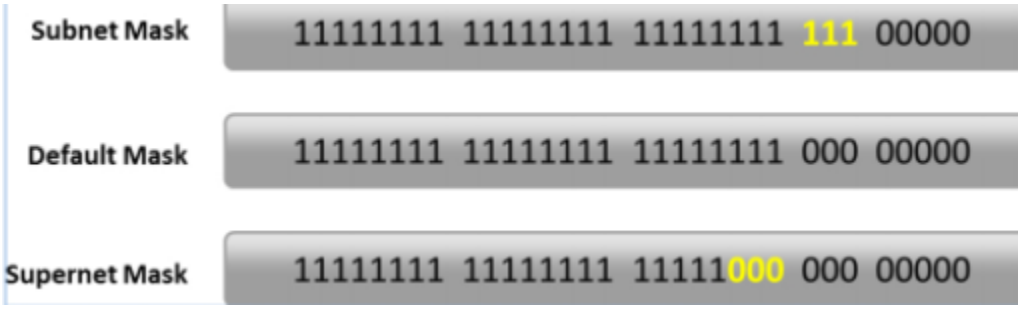


Supernetting

With the growth of the Internet, classful addressing is a big problem for many organizations. The problems with classful addressing are a lack of flexibility in dividing addresses for an internal network and improper distribution of allocated address space that requires a router to create more and more routing table entries. Subnetting solves these problems to a certain extent, but IPv6 addressing brought a 128-bit addressing system to eliminate addressing issues appropriately. This new system eliminates the need for address classes and creates a new addressing scheme to match the growing

demand of Internet users. This system advocates creating a new classless addressing scheme known as Classless Inter-Domain Routing (CIDR). This system uses a concept of subnetting as a base and takes it a step further. Subnetting divides a single network into subnets, whereas CIDR applies the subnetting principle to large networks. It aggregates networks into larger supernets with a concept known as supernetting.

Advantages of CIDR: With CIDR, organizations can allocate address space efficiently as per their requirements and preferences. In classful addressing, there are class A, B, and C networks. The class A network has around 16,277,214 addresses per network, class B network has 65,534, and class C has only 254 addresses. The address classes in this addressing system are disproportionate. CIDR eliminates the problem with class imbalances and routing entries by creating small entries for large networks. Network prefixes based on CIDR help the router in determining the dividing point between the net ID and the host ID. Subnetting requires a subnet mask to determine the network ID and the host ID. CIDR does not support a 32-bit binary subnet mask. Instead, CIDR uses "/" slash notation (known as CIDR notation) along with prefix length to show the network size.



IPv6 Addressing

IPv6 is capable of providing a large address space of 128 bits for the increasing demands of Internet users. It has a new format for the packet header to minimize problems with overhead routing entries. IPv6 has globally identified unique addresses with efficient, hierarchal, and routing infrastructure that relies on prefix length rather than address classes. This allows the backbone routers to create small routing tables. IPv6 simplifies host configuration with stateless and stateful address configuration for network interfaces. In IPv6, hosts on a link are capable of automatically configuring themselves with a link called link-local addresses by responding to the prefixes mentioned by the local routers. The host sends a link-local address request to a local router for connecting to that network, which then responds to the request by sending its configuration parameters. This lets the host configure automatically with the available router. IPv6 is capable of configuring itself, even though there are no routers. IPv6 supports unicast and multicast communication along with a new communication type called anycast.

Unicast Address: It is used to identify a single node in the network. The four different categories of Unicast address are:

- Global unicast addresses are globally unique on the Internet.

- Link-local addresses are not meant for routing, but are confined to a single network segment.
- Unique local addresses. These assist in private addressing and also avoid the chances of collision between two subnets

Anycast Address: In the anycast communication method, only specific associated addresses in a network receive the messages. IPv6 provides better support for quality of service (QoS) with proper management of network traffic.

Multicast Address: IPv6 packets sent to a multicast address identifies the group of interfaces, usually on different nodes. Only those hosts that are members of the multicast group can receive the multicast packets. The IPv6 multicast is a routable address and the routers forward these multicast packets to all the members of the multicast groups.

Difference between IPv4 and IPv6 Internet Protocol Version 4 (IPv4)

The fourth version of the Internet protocol that identifies devices on a network through the technique of addressing. IPv4 mainly works in the packet-switched link-layer networks. It uses a 32-bit address scheme, thereby permitting 2^32 addresses. The sender and the forwarding routers perform the fragmentation. There is no method to identify the process of packet flow. Checksum fields and option fields are available in IPv4. The IPv4 address uses IGMP to manage multicast messages. It is possible to broadcast messages. Configuration of IPv4 requires either manual configuration of IPv4 addresses or DHCP configuration. Internet Protocol Version 6 (IPv6) Also known as IPng (Internet Protocol Next Generation), this is the advanced version of IPv4 and replaces IPv4. The IPv6 protocol allows better handling of hosts and data flowing on the Internet. The main advantage of using IPv6 is that it reduces the exhaustion of IP addresses. The IPv6 addresses are 128 bits long and represented using hexadecimal. The sender performs the fragmentation part. The flow label field in the packet header of the IPv6 address format assists in identifying the flow of the packet. The IPv6 address headers do not consist of any checksum or options field. The IPv6 consists of an auto-configuration mode that eliminates the need for manual configuration (as in IPv4).

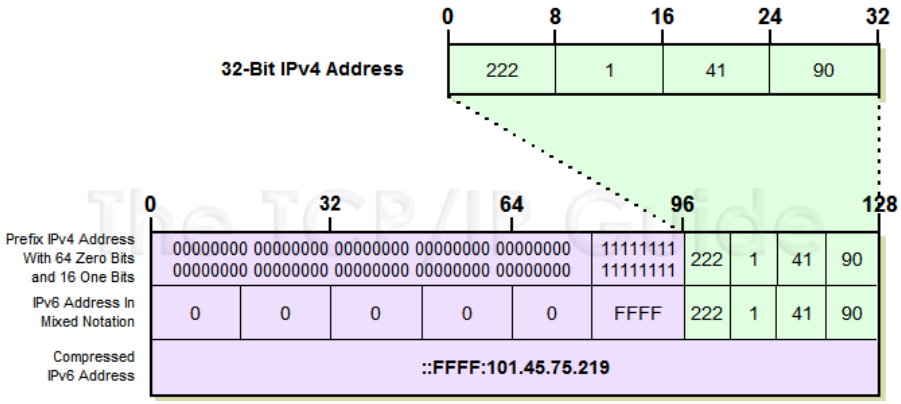
Advantages of IPv6 over IPv4:

- IPv6 provides a simplified method for the router task when compared with IPv4.
- IPv6 is more reliable to use than IPv4 and can handle more payloads.
- IPv6 is more compatible for use in mobile networks than IPv4.

IPv4-Compatible IPv6 Address

IPv4-compatible addresses obtained from IPv4 public addresses allow connecting of IPv6 hosts over the IPv4 Internet infrastructure. The Ipv6 address is compressed within the Ipv4 header to eliminate the additional use of Ipv6 routers.

The IPv4-compatible IPv6 allows the IPv6 devices to insert IPv4 addresses in the IPv6 address through the IPv4-connected network. The IPv4-compatible IPv6 has a different address format with the first 96 bits set to all zeroes, followed by a dotted decimal IPv4 address.



They can be written as 0:0:0:0:0:0:A.B.C.D or ::A.B.C.D, where "A.B.C.D" represents the embedded IPv4 address.

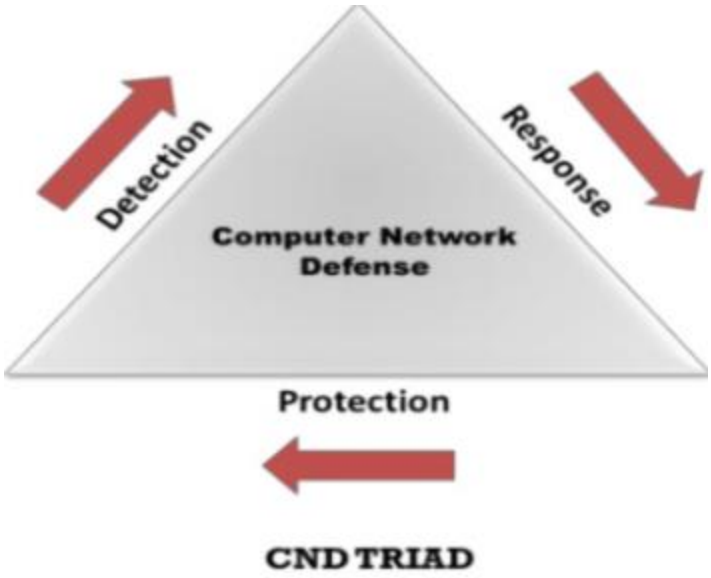
The host or router at each end of an IPv4-compatible tunnel must support both the IPv4 and IPv6 protocol stacks. IPv4-compatible tunnels must configure between border-routers or between a border-router and a host. Using IPv4-compatible tunnels is an easy method to create tunnels for IPv6 over IPv4, but the technique does not scale for large networks.

Computer Network Defense (CND)

Computer network defense (CND) is a set of processes and protective measures that use computer networks to detect, monitor, protect, analyze and defend against network infiltrations resulting in service/network denial, degradation and disruptions. CND enables a government or military institute/organization to defend and retaliate against network attacks perpetrated by malicious or adversarial computer systems or networks.

CND enables network administrators to defend and act against network attacks performed by malicious or adversarial computer systems or networks.

CND is part of Computer Network Operations (CNO), which deals with the overall network security achieved through detection, prevention, analysis, and response to various network attacks.



CND TRIAD

CND Fundamental Attributes

CND employs an Information Assurance (IA) principle which enforces taking appropriate countermeasures and response actions upon the threat alert or detection. Network operators should consider IA principles to evaluate if the data is sensitive or not—and to handle the situations when security consequences occur on the network. This assists them in identifying network security vulnerabilities, monitoring the network of any intrusion attempts or malicious activity, and defending the network by mitigating vulnerabilities.

CND should address the following Information Assurance (IA) principles to achieve a defense-in-depth network security:

Availability: Availability is the process of protecting the information systems or networks that hold the sensitive data to make them available for the end users whenever they request access.

Confidentiality: Confidentiality allows only authorized users to access, use, or copy information. Authentication works closely with confidentiality; if the user is not authenticated, they will not be granted access to confidential information. If a non-authorized user accesses the protected information, it implies that a breach of confidentiality has occurred.

Integrity: Integrity protects the data and does not allow modification, deletion, or corruption of data without proper authorization. This IA principle also works closely with authentication to function properly.

Non-Repudiation: Non-Repudiation is a service that validates the integrity of a digital signature's transmission—starting from where it originated to where it arrives. Non-repudiation grants access to the protected information by authorizing that the digital signature is from the intended party.

Authentication: Authentication is a process in which credentials are provided to authorize user and are compared to those files in database within an authentication server. If the credentials match, then the process is completed and user can access the data or file. It guarantees that the files or data passing through the network are safe.

CND Layers

The network defense is achieved with the appropriate implementation of technology, operations, and people in the organization. These elements play an important role in attaining the proper defense-in-depth network security for the organization. Technology is not enough to protect the network from a variety of attacks. Certain operations are needed in order to configure these technologies and skilled individuals are required who can perform those operations. The combined use of these elements contributes to achieving defense-in-depth network security.

CND Layer 1: Technologies

Implementations of the following technologies help an organization to protect their assets

Physical security: The main aim in implementing physical security is to secure the hardware, personnel, networks, data, and information. Physical security can prevent all kinds of physical damage, theft, or loss to an organization (or an enterprise). It also provides protection from fire, vandalism, and other natural disasters.

Access control mechanism: The main aim in implementing the access control mechanism is to impose certain restrictions in users accessing the resources in the network. Controlling the access to devices and other resources can actually secure the network as well as prevent the use of any rogue devices.

Firewalls/IDS implementation: The main aim in implementing a firewall or IDS is to execute certain security policies for communication in the network. Firewalls can actually filter the trusted and untrusted network traffic and then allow the passage of traffic (depending on those policies). The IDS system can identify and monitor any kind of illegal activities in the network level, as well as in the host level.

Proxy servers: The main aim in placing a proxy server in the network is to conceal the original IP address from the attackers and thereby increase the level of security in the network. The proxy servers can also execute the user requests at a faster rate by caching.

OS hardening/patching: The main aim in performing operating system hardening or patching is to prevent vulnerability levels in the network. The process of patching and hardening provides the latest security updates and issues at the application level, thereby enabling network administrators to solve the issue at a faster rate.

Packet/content filtering: The main aim in implementing packet/content filtering is to prevent any kind of intrusion in the network. The content packet-filtering method filters or searches for viruses, worms, intrusions, or any other non-compliant protocols in the network. It blocks or prevents passage of packets based on the source and the destination addresses.

Antivirus protection: The main aim in implementing antivirus protection in the system is to secure the data and systems from viruses, botnets, Trojans, etc. These malware programs can actually gain the username and passwords of the user on the victim machine or compromise the data contained in a system. The antivirus protection can alert the user regarding the presence of any malware program in the system.

Product evaluation based on common criteria: The main aim in implementing the product evaluation is to ensure that the IT products meet the security standards required for deployment in the networks. The IT products need to meet the common criteria defined for each specific product. Meeting the common criteria ensures the security of the IT products deployed in the network.

Encryption mechanism: The main aim in implementing the encryption mechanism is to provide the confidentiality and integrity of the information passed on the network. The encryption process confirms that only the sender and receiver of a message can actually read the message and prevents all kinds of unauthorized access. The mechanism also includes the use of an encryption key—without which the sender and receiver cannot access the message

Passwords security: The main aim in implementing the password security is to ensure complete security of the passwords from all types of password attack. It protects the passwords from brute-force attacks and eavesdropping mechanisms. The password-security mechanism persuades the user to use long and complex passwords. It also brings in certain mandatory policies that each user needs to follow while creating passwords, thereby minimizing the chances of an attack on passwords.

Authentication mechanism: The main aim in implementing the authentication mechanism is to ensure the authenticity of the user requesting access to a resource. The authentication mechanism checks the identity of the user against various methods like credentials, biometrics, etc. The method of authentication can restrict unauthorized access from the users.

ADMZ (demilitarized zones): The main aim in implementing the DMZ is to ensure the security of an organization's local area network from an untrusted network. The demilitarized zone can provide an extra layer of security to the network and prevent the attackers from accessing the internal servers and data through the Internet.

Configuration management: The main aim in implementing configuration management is to provide consistency in performance, functionalities, and physical components of the resources in a network. It prevents the chances of any failure of equipment or any adverse changes in the system. Configuration management also provides an idea regarding the updates and upgrades required for a resource.

Network logs audit: The main aim in implementing the network logs audit is to monitor the activities of a network. The review of network audits can actually increase the security of the network.

CND Layer 2: Operations

Performing the following operations helps organizations to maintain the security of their assets:

Creating and enforcing security policies: Network operators need written security policies to monitor and manage a network efficiently. These policies set appropriate expectations regarding the use and administration of information assets on a network. Security policies describe what to secure on the network and the ways to secure them.

Creating and enforcing standard network-operating procedures: Standard network-operating procedures are instructions intended to document the routine network activity. Network operators should rely on these procedures to ensure efficiency and security of the network. The main goal of network operating procedures is to carry out the network operations correctly and always in the same manner

Planning business continuity and disaster recovery: There are various threats and vulnerabilities to which a business is exposed—such as natural disasters, acts of terrorism, accidents or sabotage, outages due to an application error, hardware or network failures. Planning business continuity and disaster recovery is the act of proactively working out a way to prevent and manage the consequences of a disaster, limiting it to a minimum extent.

Configuration control management: Network operators encounter many problems due to the lack of configuration management capabilities. Configuration control management involves initiating, preparing, analyzing, evaluating, and authorizing proposals for changes to a system.

- Configuration control management includes:
- Device hardware and software inventory collection.
- Device software management.
- Device configuration collection, backup, viewing, archiving, and comparison.
- Detection of changes to configuration, hardware, or software.
- Configuration change implementation to support change management.

Creating and implementing incident-response processes: Network operators create and implement an incident-response process through planning, communication, and preparation. Incident-preparation readiness ensures quick and timely response to incidents. Network managers should determine whether or not to include law enforcement agencies during incident response; it can affect the organization positively or negatively.

Conducting forensic activities on incidents: Computer forensic investigators examine the incident and conduct forensic analysis by using various methodologies and tools to ensure the computer network system is secure in an organization. While conducting forensic activities on incidents, people responsible for network management should:

- Ensure that the professionals they hire are prepared to conduct forensic activities.
- Ensure that their policies contain clear statements about forensic considerations.
- Create and maintain procedures and guidelines for performing forensic activities.
- Ensure that their security policies and procedures support the use of forensic tools.

Providing security awareness and training: Some of the threats to network security come from within the organization. These inside attacks can be from uninformed users who can do harm to the network by visiting websites infected with malware, responding to phishing e-mails, storing their login information in an unsecured location, or even giving out sensitive information over the phone when exposed to social engineering. Network managers should make sure that the company's employees are not making costly errors that can affect network security. They should institute company-wide security-awareness training initiatives including training sessions, security awareness website(s), helpful hints via e-mail, or even posters. These methods can help ensure employees have a solid understanding of the company security policy, procedures, and best practices.

Enforcing security as culture: Network operators should enforce security as a culture in the organization. It helps knowing what behavior compromises security and how to educate employees to change their unsecure behavior. The culture within an organization will have a significant influence on the likelihood of risks occurring and the degree to which varying control approaches will be successful.

CND Layer 3: People

Network defense relies on the people involved in network operations. People are a crucial element of any organization's network security approach. The degree to which people embody a culture of security will significantly influence that organization's ability to protect key assets. The people involved are responsible for maintaining, repairing, and managing network and computer systems to improve their performance. They explore and solve network problems logically and consistently. They monitor the network for vulnerabilities before an outsider can exploit it. These people make use of CND technologies and operations to design and implement a robust network—as well as secure the network.

People involved in computer network defense include:

Network Administrator: The network administrator manages the whole network in an organization. They coordinate all systems and software, as well as help in running the network of an organization smoothly.

Network Security Administrator: The network security administrator is responsible for maintaining all the cybersecurity of an organization. They fix, control, and monitor the security solutions of an organization.

Network Security Engineer: The network security engineer mainly develops the countermeasures required for any cyber-related issues in an organization. They monitor and manage the IT issues.

Security Architects: The security architect supervises the implementation of the computer and network security in an organization. They need to find methods to implement the network and computer security in an efficient manner.

Security Analysts: The security analyst maintains the privacy and integrity of the internal network in an organization. They need to evaluate the efficiency of the security measures implemented in an organization.

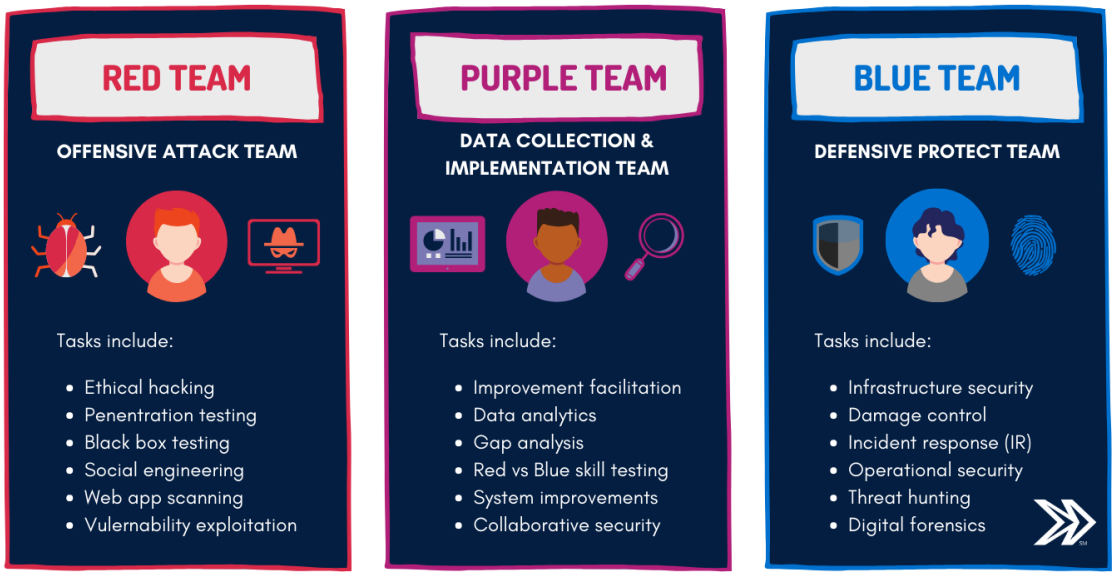
Network Technicians: The network technician manages the hardware and software components of an organization. They fix and repair the issues related to these components.

End Users: The end user refers to the people who use the end product deployed by an organization. The end user can access the developed products through a desktop, laptop, iPad, smartphones, etc.

Informed Leadership: The informed leadership can help an organization in making exemplary decisions regarding the security of the network and systems in an organization. They need to be proactive enough to find the weaknesses and strengths in a network.

Blue Teaming

A blue team is an internal security team who helps in building a strong Computer Network Defense (CND) for the network. Blue team is a part of the red/blue team exercise to defend the network. The blue team defends the network from both real and red team attacks. Blue team security professionals have direct access to the network. The blue team is responsible for detecting the attacks and, in a limited form, for protecting the hosts. They identify known vulnerabilities on systems and do not address the requirements for an overarching security infrastructure. The goal of the blue team is to detect the attacks and execute some countermeasures to slow down or confuse the attackers.



Roles and Responsibilities:

- Blue team protects the network against the attacks by the red team.
- Use tools to monitor and protect the network.
- Implement preventive measures to minimize the attacks.
- Create reports of the incidents to be sent to the management.
- Blue team must gain knowledge of the threat actor's Tactics, Techniques, and Procedures (TTPs) and prepare counter approaches to defend the network.
- Understand advanced threat-actor activities on the network using defensive techniques against these actors.
- Understand the network using a realistic advanced attacker viewpoint.
- Find the operational readiness and incident-response capabilities of the network using various tools and techniques.
- Assess the ability of internal network defenses in eliminating attacks from advanced threat actors.

Advantages of Blue Teaming:

- Enhance the security of the organization network.
- Blue team members gain complete knowledge of the existing network defense.
- Validate existing network defense and help use them effectively.
- Blue teams are more vigilant against attacks.
- Forming blue teams helps by improving the training for network defenders to protect the network.
- Help structure a realistic security process for monitoring threats in advance.

Best Practices with CND

There are some proven methods for making sure CND approaches are rock solid for organizations everywhere. Adhering to these best practices is the best way to ensure your network stays protected from hackers and those with malicious intent.

- **Utilize a firewall**. One of the first and best defenses your network can employ is a firewall. A firewall acts as a barrier between an organization's valuable data and the criminals trying to steal it. Firewalls provide an extra layer of security to the layers already in place. At the same time, your assets don't always stay behind the corporate firewalls, so it is also important to have a good understanding of what those assets are doing while not behind a firewall.
- **Visibility.** Having visibility into and across your entire network is critical today. You need to know what traffic is on your network, should it be there, and has it always been there? You also need to have solid visibility into your cloud products you use today, Office 365, Google Gmail and Salesforce.com to name a few. Knowledge and awareness of who is accessing your systems, when they are and if they are the intended user accessing those systems. If they are not the intended user, you need to be alarmed immediately. Having this type of visibility is a minimum requirement with today's technology landscape.
- **Document and outline your cybersecurity practices**. Have every plan, from incident response to the types of plans in place for different types of attacks, well documented and outlined. This will help in the review of CND practices, as well as help adapt these security policies to new problems that arise over time. Having a solid and adaptable plan for security is one of the best ways that organizations can keep their systems air-tight.
- **Have a plan for mobile devices**. If your organization relies on mobile devices such as smartphones and tablets, it is important to have a plan to support those as well. Keep an outline of who is issued which device, and ensure that every device is up to date with the latest software and security patches. Mobile devices can be updated through their app stores or settings dependent on which operating system they run. Check for updates for Google's Android using Google Play Protect in the Google Play Store, or through the Android system settings. Apps for Apple's iPhones can be updated through the Apple App Store, and system updates can be applied through the iPhone system settings by clicking "Check for Updates."
- **Educate employees on the importance of cybersecurity best practices**. Make sure all employees are aware of the organization's security practices. This will help make sure members of staff aren't influenced by phishing scams to click on unknown links or install malicious files onto their systems.

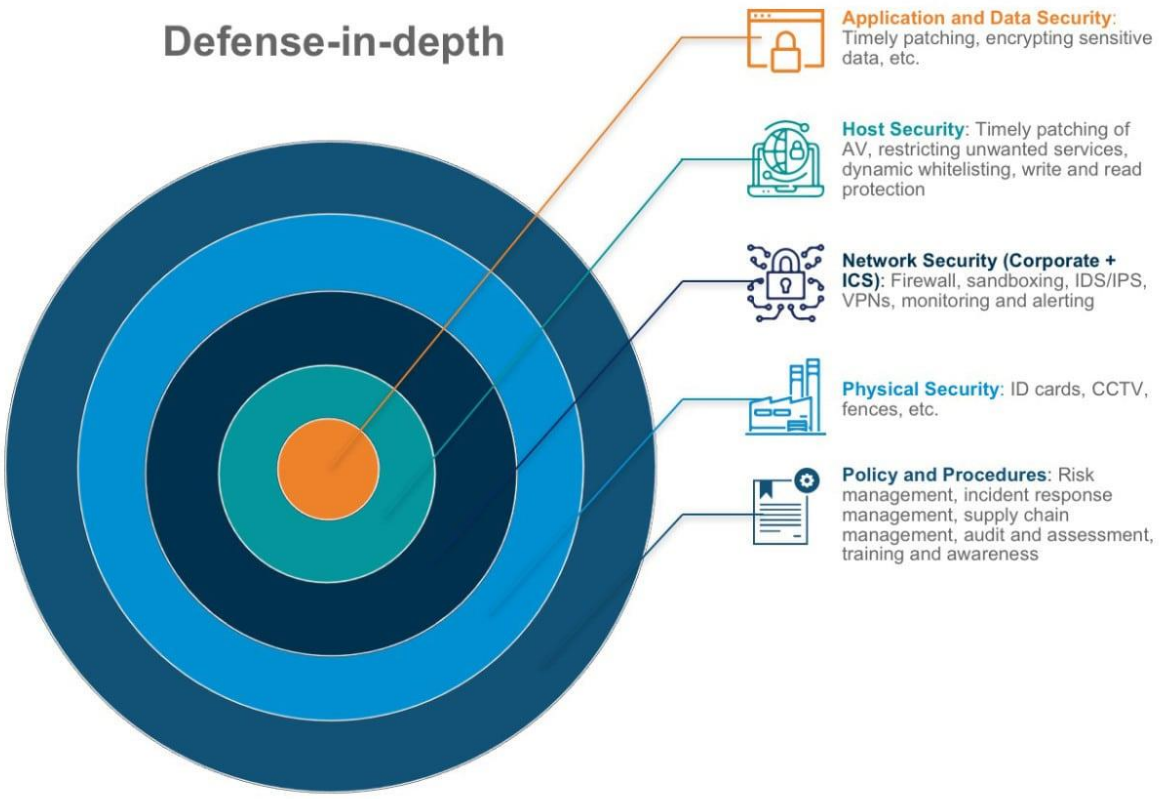
CND services:

- Database administration, backup, and network performance tuning
- Troubleshooting and resolving HBSS integration and ensuring compliance etc.
- McAfee point product security applications such as Host Intrusion Prevention System
- Deploying and configuring HBSS modules and servers
- Performing maintenance release updates
- Monitoring servers for email data loss prevention to prevent emails containing personally identifiable information from being released to the public

- Security maintenance of Sonic-walls, Cisco switches and firewalls, F5, Juniper, and RSA appliances, servers, desktops and laptops, IPS/IDS, and end-point protection.

Network Defense-In-Depth

Defense in depth is a security strategy in which several protection layers are used throughout an information system. Defense in depth involves implementing security controls at different layers of network stack. It imposes a complex defense layered structure thereby making it difficult for the attackers to penetrate into the system and achieve their goal. This strategy uses the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier. Defense in depth helps to prevent direct attacks against an information system and its data because a break in one layer leads the attacker only to the next layer. If a hacker gains access to a system, defense in depth minimizes any adverse impact and gives administrators and engineers time to deploy new or updated countermeasures to prevent a recurrence of intrusion or stop an intrusion from going any deeper.



Typical layers of a defense-in-depth approach include:

Policies, Procedures, and Awareness: This is the first level of countermeasures that every organization must design and implement. It includes enforcing security policies to

avoid misuse of resources or restrict unauthorized operations on the organization's resources.

Physical: It involves ensuring security of the organization's assets from various physical threats.

Perimeter: It involves the design and implementation of appropriate security measures at the perimeter level.

Internal Network: It includes the design and implementation of security measures for an internal network.

Host: It involves implementing security measures at each individual host level.

Application: It involves implementing security measures at the application level.

Data: It involves implementing security measures to data whether it is at rest or in transit.

Defense-in-Depth Network Design

The first line of defense against attacks is the firewall, which can be configured to allow/deny traffic. Installing and configuring the next-generation firewalls with capabilities such as application control, identity awareness, IPS, web filtering, and advanced malware detection can increase complexity for the attacker to bypass them.

IDS/IPS is the second line of defense for a network, even though it is included in the firewall as the first line of defense. Having your IPS properly optimized and monitored is a good way to detect and block attackers who get past the first castle defense.

The network administrator should consider the following factors while developing and designing a secured network:

- The network topology and location of the hosts in a network.
- The right selection of hardware and software security technologies.
- Proper configuration of each component.

Network designers should always monitor and examine common security issues found in the network set-up of a company to establish a secure network. They should also identify some best practices to secure the network.

The challenges encountered by the network designer are:

- Protecting the network from attacks that come from the Internet.
- Protecting public servers such as web, email, and DNS servers.
- Containing damage when a network or system is compromised.
- Preventing internal attacks against the network.
- Protecting highly important and sensitive information like customer databases, financial records, and trade secrets.
- Developing guidelines for the administrators to handle the network in a secure manner.
- Enabling intrusion detection and logging capabilities.

Network designers need to take care of certain policies that help in the careful and efficient management of the organization. The policies created should follow the company standards and should include criteria like number of human resources needed, cost for securing the network etc. The network designer can proceed with the network design after the creation of these policies

CND Process

The CND process specifies the prevention, detection, and response actions to security incidents in order to ensure complete computer network defense. It should be a continuous process. The following phases of the CND process assist network administrators in implementing network security effectively:

- **Protecting**: It includes a set of prior defensive actions (countermeasures) taken toward eliminating all the possible vulnerabilities on the network. It includes security measures (such as Security Policies, Physical Security, Host Security, Firewall, and IDS) used to offer network protection.
- **Monitoring**: It involves examining and assessing the network for any abnormalities such as attacks, damages, unauthorized access attempts, modifications, etc. It includes regular monitoring of network traffic using network monitoring and packet-sniffing tools.
- **Detecting**: It involves determining and identifying any abnormalities and their location in the network. It includes identifying what is abnormal to the network.
- **Analyzing**: It involves actions, which includes confirming the incidents, finding their root causes, and planning a possible course of actions for an incident. It includes deciding whether the incident is an actual security incident or a false positive
- **Responding**: It involves a set of actions taken to mitigate the impact of an attack on the network. It includes incident response, investigation, containment, and eradication steps for responding to the incidents.

CND Approaches

There are three main classifications of security defense techniques used for identification and prevention of threats and attacks in the target network.

Preventive Approach: The preventive approach basically consists of methods or techniques that can easily avoid the presence of threats or attacks in the target network. The preventive approaches mainly used in the network are as follows:

- Access control mechanisms such as a firewall.
- Admission control mechanisms such as NAC and NAP.
- Cryptographic applications such as IPSec and SSL.
- Biometric techniques such as speech or facial recognition.

Reactive Approach: The reactive approach is complementary to the preventive approach. The reactive approach prevents those attacks and threats that the preventative approach failed to defend against. (For example, a DoS and DDoS attack.) Implementing both preventive and reactive approaches will confirm the security of the

network. The reactive approaches include security monitoring methods such as IDS, SIMS, TRS, IPS, etc. Retrospective Approach: The retrospective approach examines the reasons for attacks in the network. The approaches include:

- Fault-finding mechanisms that include a protocol analyzer and traffic monitors.
- Security forensic techniques such as CSIRT and CERT.
- Post-mortem analysis mechanism that includes a legal/risk assessor