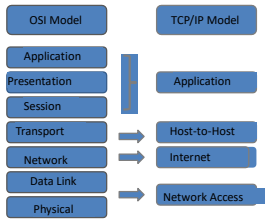
Logical Structure of Reference Models



Application Layer

- The seventh layer or topmost layer of OSI Reference Model is the Application layer.
- It provides the interface that a person uses to interact with the application. This interface can be command-line-based or graphics-based.
- Cisco IOS Routers and Switches have a command-line interface (CLI), whereas a web browser uses a graphical interface.
- It is the only layer where the user can directly interact with application or program.
- As we say it is responsible for users and network interaction so it receives commands from user and gives output as form of result to user.
- Protocols at Application Layer: **DNS, FTP, HTTP, HTTPS, NFS, DHCP, SMTP, SNMP, POP3, RDP, TFTP, Telnet** etc….

Presentation Layer

- The sixth layer of OSI Reference Model is Presentation layer. It is responsible for defining how information is presented to the user in the interface that they are using.
- It is responsible to present data to the next layer. While sending it receives data from upper layer, then convert it to appropriate format for next layer and while receiving assemble this data with the help of extensions, codes, formats to a readable format and sent to application layer.
- This layer defines how various forms of text, graphics, video or audio information are presented to the user. For example, text is represented in two different forms: ASCII and EBCDIC. ASCII (the American Standard Code for Information Interchange) uses seven bits to represent characters; it is used by most devices today. EBCDIC (Extended Binary Coded Decimal Interchange Code) developed by IBM and it is still used in Mainframe environments to represent characters.
- Additional Features:
  - ❑ Compression and Decompression
  - ❑ Encryption and Decryption
  - ❑ Encoding and Decoding
  - ❑ Protocols and Standards at Presentation layer: **ASCII, BMP, GIF, JPEG, WAV, AVI, MPEG** etc……..

Session Layer

- It is the fifth layer of OSI Reference Model.
- It is responsible to initializing the setup and teardown connections. The primary function of the session layer is to establish a session between source and destination before transmission, then maintain a session during transmission and in the end terminate the session after transmission.
- Session layer also keeps separate each session data with others by assigning a session ID to each session. Session layer works in all three modes of communication, such as, Simplex, Half-Duplex and Full-Duplex.
- Protocols at Session layer: **NetBIOS**

Transport Layer

- It is the fourth layer of OSI Reference Model.
- It is responsible for the actual mechanics of connection, where it can provide both reliable and unreliable delivery of data.
- For reliable connection, the transport layer provides error detection and error correction, when an error is detected, the transport layer will resend the data, thus providing the correction.
- For unreliable connections, the transport layer provides only error detection, and error correction is left up to one of the higher layers.
- Transport layer provides reliable connection with the help of TCP (Transmission Control Protocol) protocol, and with the help of UDP (User Datagram Protocol) protocol it provides unreliable connection.

Features:

- ❑ Provides additional connection below the session layer.
- ❑ It provides O/S to O/S or application to application communication.
- ❑ Manages the flow control of data between parties across the network.
- ❑ Divides streams of data into segments.
- ❑ Provides error-checking to guarantee error-free data delivery.
- ❑ Provides acknowledgement of successful transmissions, and requests retransmission if
  - some packets don't arrive error-free (TCP).
- ❑ TCP: Acknowledgement based communication
- ❑ UDP: Fast communication without error correction.
- ❑ Provides flow control and error-handling.
- ❑ Provides Port Addressing.
- ❑ Protocols at Transport layer: **TCP & UDP, SCTP**

Network Layer

It is the third layer of OSI Reference Model. Network layer provides logical topology of your network using logical addresses (IP Address). These addresses are used to group machines together.

These addresses have two components: a network component and a host component. The network component is used to group devices together.

Logical addresses allow devices that are on the same or different media types to communicate with each other.

Network layer is responsible to move information (data) from one network to another.

To move information between devices that have different network numbers, a Router is used. Routers use information in the logical address to make intelligent decisions about how to reach a destination.

Features:

- ❑ Translates logical network address to their physical address.
- ❑ Responsible to transmit information from one network to other network.
- ❑ Responsible to search routes for the network layer components.
- ❑ Responsible to convert segments into packets.
- ❑ Responsible for logical Addressing (IP Addressing).
- ❑ Protocols at Network layer: **IP, IPX, ICMP, IGMP, ARP, RARP, RIP, OSPF** etc…
- ❑ Devices at Network layer: Router, Brouter, Frame Relay Device, ATM Switch etc…

Data Link Layer

- It is the second layer of OSI Reference Model. Data link layer is responsible to define how a networking device accesses the media that it is connected as well as defining the media's frame type.
- This includes the fields and components of the data link layer. This communication is only for devices on the same data link layer media type (or same piece of wire).
- To traverse media types, like Ethernet to Token Ring, typically a router is used. It is also responsible for taking bits (binary 0's and 1's) from physical layer and reassemble them into the original data link layer frame.
- The data link layer does error detection and will discard bad frames. It typically does not perform error correction as TCP/IP's TCP protocol does; however, some data link layer protocols do support error correction functions.

Features:

- Responsible to define the methods used to transmit and receive data on the network and define how to access media.
- Responsible to convert packets into frames.
- Responsible to handles data frames between the Network and Physical layers.
- Responsible for error-free transfer of frames to other computer via the physical layer.
- Responsible to perform Physical Addressing (MAC Addressing).

Data Link layer has two sub-layers:

- LLC (Logical Link Control) 802.2
- MAC (Media Access Control) 802.3

LLC (Logical Link Control): It is responsible to establish a virtual circuit over the physical line to identify physical addressing, session ID, Dialing and Acknowledgement etc…. It provides logical linking over physical wire:

PPP	-	Dial-up
PPPoE	-	Broadband
PPTP & L2TP	-	Tunnel (VPN)
HDLC & SDLC	-	For wired and wireless

MAC (Media Access Control): It is responsible to define how to access media, like network type; Token Ring, Ethernet, Wifi. How to access media means how many devices can use provided media at the same time. Bandwidth, no. of sessions, collision report performs at MAC layer It is responsible to communicate with the adapter card. Network access technologies like Token Ring, Ethernet, Wifi, ATM, Frame Relay, ISDN etc. works at MAC layer. It is also responsible to perform MAC Addressing.

- Protocols at Data Link Layer: **PPP, PPTP, L2TP, HDLC, SDLC**
- Devices at Data Link Layer: Bridge, Switch, Modem etc…

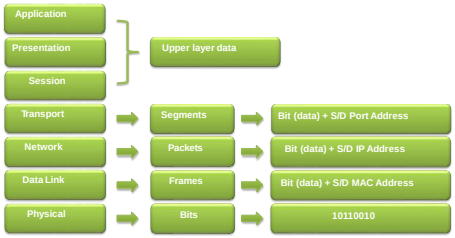
Physical Layer

It is the first layer of OSI Reference Model. All physical tasks to send information between nodes or devices are performs at physical layer.

Physical task like Amplification, Filtration, Broadcasting, Signal conversion (light to electrical, electrical to wifi, wifi to light). It is the only layer from where the actually data has been transmitted.

- Protocols at Physical layer: **RS232, V.35, V.32**
- Devices at Physical layer: Hub, Repeater, Amplifier, Interface, NIC, Media, Connector etc…

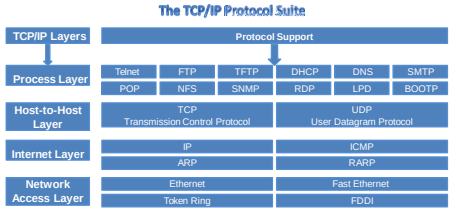
Data encapsulation



Layers	Protocols or Standards	Devices
Application	HTTP, HTTPS, FTP, TFTP, DNS, DHCP, BOOTP, SMTP, POP, IMAP, SNMP, NFS, TELNET, SSH, RDP, POP, IMAP	Gateway
Presentation	ASCII, BMP, GIF, JPEG, WAV, AVI, MPEG	Gateway Redirector
Session	NetBIOS, Named Pipes, Mail Slots, RPC	Gateway
Transport	TCP, UDP, SCTP	Gateway, Advanced Cable Tester, Brouter
Network	IP, IPX, ICMP, IGMP, ARP, RARP, RIP, OSPF etc…	Router, Layer 3 Switch, Brouter, Frame Relay Device, ATM Switch
Data Link	PPP, PPTP, L2TP, HDLC, SDLC	Bridge, Switch, NIC, ISDN Router
Physical	RS232, V.35, V.32	Hub, Repeater, Amplifier, Multiplexer

TCP/IP

- The Transmission Control Protocol/Internet Protocol (TCP/IP) was created by **Department of Defense** (DOD) to ensure and preserve data integrity as well as maintain communication.
- TCP/IP is made of interactive modules which provide specific functionality.



Protocols

Protocols are the Rules and Regulations for the network communication. Each and every communication is based on any of the network rule (Protocol) or we can say that a rule is defined for each and every communication.

Features:

- ✓ Set of Rules
- ✓ Carrier to carry data
- ✓ Carrier between nodes
- ✓ Convertor

Types of Protocols:

- ❑ Routing Protocols: Protocols are responsible to search and select a best route for the communication.
  Examples: RIP, IGRP, EIGRP, OSPF, BGP etc…
- ❑ Routed Protocols: Protocols are responsible to transmit data from the define route.
  Examples: IP, IPX, ICMP, FTP, UDP etc….

Types of Protocols on the basis of ownership:

Protocols are designed for special O/S, Program, Function, Device

Examples for Proprietary Protocols:

Novell Netware (O/S) -	IPX/SPX
Macintosh (O/S) -	Apple talk
Cisco Router (Device) -	IGRP, EIGRP
M/S, IBM -	NetBEUI

Free for all

Examples for Universal Protocols:

Department of Defense (DOD) - TCP/IP

Application or Process Layer Protocols

Telnet

- Telnet is a Protocol or Service which is used to access remote services.
- It allows user on a remote client machine, called the Telnet Client to access the resources of another machine, called the Telnet Server.
- Through Telnet a user can access the remote host through Command line Interface (CLI).
- The data has been transmitted between Telnet server and Telnet client in the form of plain text during the Telnet session.
- An Administrator can configure or manage the Telnet Service through the Telnet Program or Application.
- Telnet works on logical port no. 23...

SSH (Secure Shell)

- SSH is a Protocol or Service which is also used to access the remote hosts in the network or in the Internet.
- It allows user on a remote client machine, called the SSH Client to access the resources of another machine, called the SSH Server.
- Through SSH a user can access the remote host through Command line Interface (CLI).
- The main advantage of using SSH is that the data has been transmitted between SSH server and SSH client in the encrypted form during the SSH session, it makes SSH more secure then Telnet.
- SSH works on logical port no. 22…..

RDP (Remote Desktop Protocol)

- RDP is a Protocol or Service which is used to access remote hosts in the network or in the Internet.
- Through RDP a user can access the remote host through Graphical User Interface (GUI), it means through RDP a user can access or manage the remote host graphically.
- RDP works on logical port no. 3389…..

FTP (File Transfer Protocol)

- FTP is a Protocol or Service which is used to transfer files or directories from one host to another host.
- It is used to exchange files between hosts over the network (LAN) or Internetwork or Internet.
- A user on a client end, called the FTP Client, can download or upload the files or directories from the server end, called the FTP Server.
- It uses TCP to transfer data, so it is responsible for the reliable communication of data with acknowledgement.
- It uses TCP, so it provides security features.
- An Administrator can configure or manage the FTP Service through FTP Program or Application.
- FTP works on logical port no. 21 ….

TFTP (Trivial File Transfer Protocol)

- TFTP is a Protocol or Service which is responsible to transfer files.
- It is the older or simple form of FTP which is used to download or upload files between network hosts or Internet.
- It uses UDP to transfer files, so it is not responsible for the reliable communication.
- Because it uses UDP, so it does not provide acknowledgement and does not provide security features.
- TFTP works on logical port no. 69 …...

HTTP (Hyper Text Transfer Protocol)

- HTTP is a Protocol or Service which is used to transfer web information over the network or Internet.
- It is service which is used transmit web applications or web pages in the network or Internet.
- HTTP uses TCP to transmit web information. An administrator can configure or manage HTTP Service through Web or HTTP Application or program.
- HTTP works on logical port no. 80…..

HTTPS (Hyper Text Transfer Protocol)

- HTTPS is also a Protocol or Service like HTTP which is used to transfer web information over the network or Internet but it is more secure than HTTP.
- It is secure because it works on the basis of certificate.
- It is a service which is used transmit web applications or web pages in the network or Internet.
- HTTP uses TCP to transmit web information. An administrator can configure or manage HTTPS Service through Web Application or program.
- HTTPS works on logical port no. 443…..

SMTP (Simple Mail Transfer Protocol)

- ✓ SMTP is a Protocol or Service which is used to transfer e- mail messages across the network or Internet. It helps in sending e-mails messages such as text or message with an attachment file.
- ✓ Through SMTP a user can send mail to the multiple recipients at the same time.
- ✓ It uses TCP to send e-mail messages, so it provides reliable delivery of e-mails.
- ✓ SMTP works on logical port no. 25……

POP (Post Office Protocol)

- POP is a Protocol or service which is used to retrieve e-mails from e-mail database server.
- Like SMTP which is used to sending e-mails, POP is a service which is used to receive e-mails.
- POP has some versions like POP2, POP3 etc…
- POP2 works on logical port no. 109….. and POP3 works on logical port no. 110…..

IMAP
(Internet Message Access Protocol)

- It is also protocol or service which is also used to retrieve emails from E-mail database Server.
- IMAP is more advanced service than POP to receive mails.
- IMAP works on logical port no. 143

SNMP
(Simple Network Management Protocol)

- SNMP is a protocol or service which is responsible for the management of the network.
- It is responsible to provides means to manage and control network devices, performance and security of the network.
- It broadcast SNMP agents over the network and these agents are responsible to give the actual network report to the Network Administrator. If the network communication going properly then these agents are responsible to give the healthy report, and if they found any error or trouble in the network then these agents are responsible to provide the Trap report.
- SNMP works on logical port no. 161…

DNS
(Domain Naming Service)

- DNS is a Protocol or Service which is used to resolve the Internet Domain names of hosts into IP Addresses.
- It is a service which is used to resolves FQDN (Fully Qualified Domain Name) into IP Addresses and IP Addresses into FQDN.
- DNS uses both TCP and UDP .
- DNS works on logical port no. 53…

DHCP
(Dynamic Host Configuration Protocol)

- DHCP is a Protocol or Service which is used to provide automatic hosts TCP/IP configuration.
- TCP/IP configuration includes IP Address, Subnet Mask, Default Gateway and DNS IP Addresses.
- DHCP is used for the IP Addresses distribution over the network or in the Internet.
- The server which is responsible to provide IP Addresses in the network, known as DHCP Server, and the hosts which are taking IP Address from the Server, known as DHCP Client.
- DHCP uses UDP to provide TCP/IP configuration over the network.
- DHCP Server works on logical port no. 67….and DHCP Client works on logical port no. 68…

NFS
(Network File System)

- NFS is a Protocol or Service which is used to make communication possible between two different operating systems based hosts.
- It allows hosts on different operating system to share files and disk storage…..
- NFS works on logical port no. 944…

Transport or Host-to-Host Layer

TCP
(Transmission Control Protocol)

- TCP is a Protocol which is responsible for the transportation of data.
- TCP is a Connection-Oriented and Reliable Transport Protocol. Connection-Oriented means a virtual connection must be established between the sender and the receiver before the actual transmission occurs.
- It is a Reliable protocol because it gives the actual acknowledgement of each transmission of data and also responsible for the retransmission of data if some packets don't arrive error-free.
- It is also responsible for the error checking and error correction.
- Overall, it provides the reliable transport of data.
- It divides the data into segments each having a sequence number. These sequence numbers are useful at the receiving end to rearrange the segments into original order.
- **Protocol Number: 6**

UDP
(User Datagram Protocol)

- UDP is a Protocol which is responsible for the transportation of data.
- UDP is a Connection-less/stateless and unreliable Transport Protocol.
- Connectionless means UDP is not responsible to establish a virtual connection between sender and receiver before transmission.
- It provides unreliable transport protocol because it does not provide any acknowledgement of the transmission. It just adds port addresses and error control information to the data and delivers the data. So it is fast transport protocol compared to TCP.
- Unlike TCP, it does not provide error correction but it provides error checking on the data.
- **Protocol Number: 17**

SCTP
(Stream Control Transmission Protocol)

- SCTP is a Protocol which is also used for data transport.
- It is also Connection-Oriented and reliable transport protocol that offers acknowledgement, error-free and non-duplicated transmission of multiple streams of data.
- Unlike TCP, SCTP makes sure that multiple streams of data will be transmitted simultaneously.
- SCTP can be used to manage connections over wireless network and transmission of multimedia data.
- It supports new applications such as voice over the Internet.
- It combines the best features of TCP and UDP.
- **Protocol Number: 132**

Network or Internet Layers Protocols

IP
(Internet Protocol)

- IP is a transmission mechanism used by the TCP/IP protocol.
- IP is a connectionless and unreliable datagram protocol and provides no error-checking. IP transfers data in the form of packets called datagram. Datagrams can travel through various routes to reach the destination and may not arrive in the order in which they were sent.
- IP does not reorder the data once they reach the destination. Also, IP does not keep a track of the routes of the datagram.
- IP works on protocol no. 0…

ICMP
(Internet Control Message Protocol)

- ICMP is a protocol which is used by network hosts to send notification of datagram problems such as query and error reporting messages back to the sending device.
- Its only function is to report problems to the original sender not to correct them.
- Ping command is an example of ICMP protocol.
- ICMP works on protocol no. 1….

IGMP
(Internet Group Message Protocol)

- IGMP is a Protocol which is used for multicasting.
- It means to transmit message or information to multiple recipients at the same time.
- Class D IP Addresses is used for IGMP.
- **Protocol Number: 2**

ARP
(Address Resolution Protocol)

- ARP is a Protocol which is used to determine the physical address (MAC Address) of the device only when its IP Address is known.
- It is also used to translate the IP Address to the Ethernet MAC Address.
- Each device has a physical address imprinted on the NIC. ARP is used to associate an IP Address with the Physical Address.
- ARP works only in the same network.
- Each network device in the network maintains its own **ARP Table** in it.
- To view the arp table of any host : **arp -a**

RARP
(Reverse Address Resolution Protocol)

- RARP is a Protocol which is used to determine the IP Address of the device only when its Physical Address (MAC Address) is known.
- It is useful when the device is connected to the network for the first time.

List of Application Layer Protocols/Services with their

Protocol Name	Port Number	Transmission Protocol Support
FTP	20, 21	TCP
TFTP	69	UDP
TELNET	23	TCP
SSH	22	TCP, UDP
RDP	3389	TCP, UDP
HTTP	80	TCP
HTTPS	443	TCP
SMTP	25	TCP
POP 2	109	TCP
POP 3	110	TCP
IMAP	143	TCP
SNMP	161	UDP
NFS	944	UDP
DHCP Server	67	UDP
DHCP Client	68	UDP
DNS	53	TCP, UDP

List of Protocols with their related Protocol Number

Protocol Name	Protocol Number
IP	4
ICMP	1
IGMP	2
TCP	6
UDP	17
EGP	8
IGP	9
IPV6	41
IPv6-ICMP	58
EIGRP	88
OSPF	89
L2TP	115
SCTP	132
BGP	179
RIP	520
IGRP	9

List of Protocols with their related Protocol Number

Protocol Name	Protocol Number
IP	4
ICMP	1
IGMP	2
TCP	6
UDP	17
EGP	8
IGP	9
IPV6	41
IPv6-ICMP	58
EIGRP	88
OSPF	89
L2TP	115
SCTP	132

Addressing

Addressing

For the purpose of communication, or to identify a network device in the network, a unique address for that particular device is needed. Network Device like Computer, Router, Switch, Firewall etc.. must need a unique address for its identification in the network.

Classification of Addressing

Physical Address

- ✓ MAC Address
- ✓MAC stands for Media Access Controller
- ✓48-bit Address
- ✓Hexa-decimal form
- ✓Exist on Network Interface Card (NIC)

Logical Address

- ✓IP Address
- ✓IP stands for Internet Protocol
- ✓IP Version 4
  - ❑ 32-bit Address
  - ❑ Dotted-Decimal form
- ✓IP Version 6
  - ❑ 128-bit Address
  - ❑Hexa-Decimal form
- ✓Can be assign on Operating System

MAC Address

IP Address

A Device on the network needs an IP (Internet Protocol) Address to communicate with other devices. There are some features of IP Address:

- ✓IP Address is a address which is used to identify a network device in a network or Internet.
- ✓ An IP Address is used to communicate with various networking devices in the network.
- ✓ IP Address functioning on Network Layer of OSI Model.
- ✓ IP Address is same as telephone number which is unique.
- ✓ **IANA** (Internet Assigned Numbers Authority) is the organization for the development of IP Addresses.

Classification of IP Address

Version
- IP Version 4
- IP Version 6

Local/Global
- Private Address
- Public Address

Configuration
- Static
- Dynamic

Private IP Address

- ❑ It is generally used in Local Area Network or Private network. Any of the organization can use private IP address for its private network. If the organization does not want to communicate in the WAN or Internet and just want to create local network, then private IP address is the only suitable option for these organizations.
- ❑ Organization has to pay no cost for using private IP address to the Internet Service Provider (ISP). Private IP addresses are free all.
- ❑ A single private IP address is unique in a network. A single private IP address can be used in multiple local area networks if these networks are not connected to each other.

Public IP Address

- It is generally used in Wide Area Networks (WAN) or Internet.
- Public IP Address is needed if any of the device in any network wants to communicate in Public network or WAN. Without public IP address any of the device cannot be communicate in public network or WAN or Internet.
- Organization has to pay cost for each public IP address to the Internet Service Provider (ISP).
- Public IP address is unique in public network, a single public IP address cannot be used twice or more in public network or Internet.
- An organization can also use public IP addresses in its private network
  if that network is not connected to the public network.

Unicast IP Address

- Unicast means one to one communication. When a data packet is sent from a host with destination address which represents a single host, a unicast communication takes place.
- Hence, a Unicast IP address which uniquely identifies a host in a particular network. Each host present on the Internet has at least one unique unicast IP address.

Multicast IP Address

- Multicast means one to many communication. When a data packet is sent from a host to a group of hosts, a multicast communication takes place. Multicast addresses belongs to Class D addresses. These addresses define an address for a group.
- A host on a multicast network can have more than one Class D multicast address. If a host have five multicast addresses, then the host belongs to five different multicast groups.
- Multicasting on Internet is of two types, Local level and Global level. At local level, hosts on a LAN can form a group and can be assigned a multicast address. While at global level, hosts on different networks can form a group and can be assigned a multicast address.

Broadcast IP Address

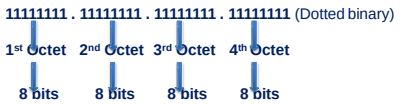
- Broadcast means one to all communication. A Broadcast address is an address that allows a data packet to be sent to all machines on a given network.
- Data packet is broadcast only at local level and not at global level. The broadcast address for a network is the last address of that network. Using broadcast IP address, a packet can be sent to the entire subnet using a private IP address space.
- For **Example**, to broadcast a packet to an entire class B subnet using a private IP address space, the broadcast address would be 172.16.255.255 for 172.16.x.x network.
- In some applications, the hosts in a network need to send messages to all the hosts in a network.
- For example, transmitting information such as weather report, stock market changes and live radio programs would work best by broadcasting the data over the network to all the hosts.
- The last IP address of any network is predefined as a Broadcast IP address of that particular network.
- The Broadcast IP address cannot be assign on the network computer.

Network IP Address

- The Network IP Address is the network address of any address. Network IP address is the identification of a network.
- To identify a network in an internetwork or in the Internet, a address must require, then the Network IP address provides the identification to a network in an internetwork or in the Internet.
- Each network or subnet has its own and separate Network address.
- The first IP address of any network is predefined as a Network address of that particular network.
- In an organization, if the administrator wants to implement a same permission on the entire network, then he can implement that permission on the entire network by simply using the first IP address of the running IP network.
- The Network IP address cannot be assign on the network computer.

IP Version 4

- Logical address in TCP/IP enabled network
- **32**-bit address
- Divided into **4** Octets
- Each Octet contains **8** bits
- Seen in two formats:
  - Dotted decimal – used by user and application
  - Dotted binary – used by o/s, protocols, n/w components
- Made up of two parts:
  - Network part – ID of network – represented by 1 in binary
  - Host part – ID of host (device) – represented by 0 in binary



Note: The decimal value of each octet can be of minimum zero (0) and maximum two hundred and fifty five (255). The value can only be between (**0 - 255**).

IP Version 4 Classes

Class	Range	Purpose
A	0.0.0.0 - 127.255.255.255	N.H.H.H
B	128.0.0.0 - 191.255.255.255	N.N.H.H
C	192.0.0.0 - 223.255.255.255	N.N.N.H
D	224.0.0.0 - 239.255.255.255	Multicasting
E	240.0.0.0 - 255.255.255.255	Research

Private and Public IP Ranges

Class	Range		No. of Networks	Local/Global
A	1.0.0.0	9.255.255.255	9	Public
	10.0.0.0	10.255.255.255	1	Private
	11.0.0.0	126.255.255.255	116	Public
B	128.0.0.0	172.15.255.255	11536	Public
	172.16.0.0	172.31.255.255	16	Private
	172.32.0.0	191.255.255.255	4832	Public
C	192.0.0.0	192.167.255.255	43008	Public
	192.168.0.0	192.168.255.255	256	Private
	192.169.0.0	223.255.255.255	2053888	Public

Calculation of Networks and Hosts

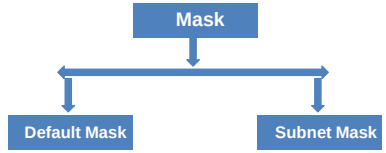
Class	No. of Networks	No. of Hosts/network
A	**126** networks	16777216-2 = **16777214** (256*256*256)
B	**16384** networks (64*256)	65536-2 = **65534** (256*256)
C	**2097152** networks (32*256*256)	256-2 = **254**

Subnet Mask

Subnet Mask is a number which is used to identify the number of hosts in a network. It is the number which is used to identify the number of available IP addresses in a network for the given IP address.

Features:

- It is responsible to define, which part is host part and which part is network part in a given IP address.
- It is responsible to define the no. of usable IP addresses for hosts.
- It is also responsible to define the number 0's and 1's bits in a given address.

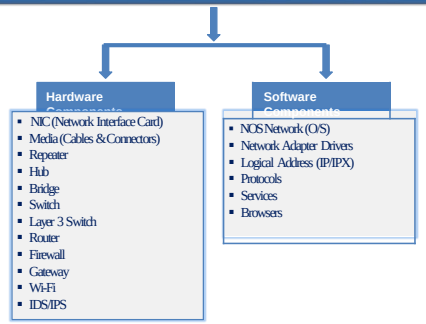


Class	Default Mask (binary)	Default Mask (decimal)
A	11111111.00000000.00000000.00000000	255.0.0.0
B	11111111.11111111.00000000.00000000	255.255.0.0
C	11111111.11111111.11111111.00000000	255.255.255.0

Note: The number of 1's must match the number of network address bits and the number of 0's must match the number of host address bits.

Internetworking Devices

Internetworking Devices/Components



NIC (Network Interface Card)

NIC is a component which provides us port to connect to network. It is a interface through which data can be send or receive in the network. There are several components on the NIC which are as follows:

- Internal Connection Bus
- MAC ROM
- PROM
- EPROM
- Buffer
- Transceiver
- External Port

Repeater

Repeater is a device which is used to boost or regenerate the data signals at the time of communication. Repeater is a physical layer device which is responsible to filter the data signals along with regenerating the data signals. It is a update version of Amplifier, amplifier were regenerate data signals but not responsible to filtration.

- Amplifier = Regenerate
- Repeater = Regenerate + Filtration

Hub

It is a physical layer device. It is also known as multiport repeater.

Features:

- It is a network device which is used to connect devices together in the network
- In the Hub created network, when any single communication takes place, then hub is responsible to forward the data to all its ports. Simply, it is not responsible to forward the data up to the actual host.
- It works on the basis of broadcast.

Bridge

Features:

- Layer 2 device
- Used to connect two Lan segments, means if u have two hubs in the network, then network broadcast can be limit by placing bridge between hubs.
- Bridging occur at the data link layer. This layer controls data flow, handles transmission errors, provides physical addressing and thes functions access to the physical network. Bridge provides e
- Responsible to create **Mac table**.
- Bridge uses a Software program to store Mac table.
- It has less number of ports than other layer 2 devices
- Bridge provides its ports speed between 10 to 100 mbps.

Switches

It is a interconnectivity device which is used to connect devices together in the network like hubs, but it is more advanced than hubs. It is also known as Intelligent Hub.

Features:

- ✓ Layer 2 device
- ✓ It is responsible to filter and forwarddata packets through the network.
- ✓ It is a update version of bridge, it includes superior throughput performance, higher port density and greater flexibility.
- ✓ Responsible to forward data frames on the basis of mac-address.
- ✓ Responsible to maintain **Mac-table**, in which it stores the mac addresses of all connected hosts.
- ✓ Because it maintains mac-table, so it also known as intelligent hub.
- ✓ It has in-built chip named **ASIC** (Application specific Integrated Circuit) to store mac-table.

- ✓ Perform switching between network devices.
- ✓ Responsible to forward the data packet up to the correct or actual host in the network by verifying the mac-address of source and destination in its mac-table, and not responsible to broadcast the data packet to all its ports like hubs.
- ✓ It has higher number of ports then hub and bridges.

Types of Switches:

- Manageable Switches
- Non- manageable Switches

Types of Switches on the basis of error handling:

- Cut-through Switches
- Store and Forward Switches
- Straight or Fragment free Switches.

Comparison between Bridge and Switch

S.no	Bridge	Switch
1	Layer 2 device	Layer 2 device
2	It stores mac-table in a software program.	It stores mac-table in a chip named ASIC.
3	Has less number of ports.	Has higher number of ports than bridges
4	Supports port speed between 10 – 100 mbps.	Supports port speed from 10 to 1000 mbps and more.
5	Responsible to connect two Lan segments.	Responsible switching of data packets between actual source and destination.

Routers

Router is a interconnectivity device which is used to forward the data packets between from one network to another network.

Features:

- ✓ Layer 3 device
- ✓ WAN connectivity device.
- ✓ Its primary function is to forward the packets by checking its destination address (IP).
- ✓ Responsible to forward the data packets from one IP based network to another.
- ✓ It is an intelligent device, because it maintains the **Routing Table** for the path selection, through which it can choose the best path for the communication.
- ✓ It understands IP address, so it forwards the data packets on the basis of IP address of source and destination.

- ✓ It stores the network number information in its routing table.
- ✓ Responsible to perform path selection.
- ✓ Never forwards broadcast packets.
- ✓ Perform Packet Switching (switch packet from one subnet to another).
- ✓ Also responsible for Packet Filteration (Access-Control List)
- ✓ Also responsible for Address Translation (NAT).

Types of Routers:

- ❑ Modular
- ❑ Non-modular (Fixed)

Router Ports and Interfaces

S.no.	Port/Interface	Description
1	**Console**	To configure router locally
2	**Auxilary**	To configure router remotely
3	**Ethernet/Fast Ethernet/Gigabit Ethernet**	Used to connect LAN (LAN Interface).
4	**Serial**	Used to connect with WAN (Router) (WAN Interface)
5	**Basic Rate Interface**	Used to connect ISDN

Ethernet	**10 mbps/e0,e1**
Fast Ethernet	**100 mbps/fa0/0, fa0/1**
Gigabit Ethernet	**1000 mbps**
Serial	**s0/0, s1/1**
Basic Rate Interface	**bri0**

Router Memory Components

S.no	Components	Description
1	**ROM**	Router boot up sequence stores in it.
2	**Flash Memory**	Router IOS (operating system) stores in it.
3	**DRAM**	Temporary configuration stores in it. Note: It stores all configuration in **running-config** file.
4	**NVRAM**	Permanent configuration stores in it. Note: It stores all configuration in **startup-config** file.
5	**Rommon Memory**	Router Mini operating system stores in it.

DHCP (Dynamic Host Configuration Protocol)

Features-

- Dynamic Host Configuration Protocol (DHCP) allows devices to dynamically acquire their addressing information.
- It is a service which is responsible to provide **automatic TCP/IP configuration** to the network hosts. TCP/IP Configuration includes, **IP address, Subnet Mask, Default Gateway, DNS addresses** etc.…
- It has two components, DHCP **Server** and DHCP **Client**. If DHCP client requests for the IP configuration, then DHCP server responds to it by providing the TCP/IP configuration to that particular client.
- DHCP uses **UDP** as its transmission protocol.
- DHCP Port Numbers-
  - DHCP Sever - **67**
  - DHCP Client - **68**

Advantages-

- ✓ It reduces the amount of configuration on network devices.
- ✓ It reduces likelihood of configuration errors.
- ✓ It gives you more control by centralizing IP addressing information.

IP Routing

IP Routing

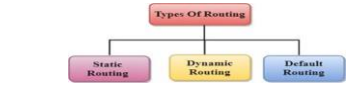
IP Routing is a process of communicating two or more different IP based networks. WAN connects different LANs with each other to communicate and
to share the data and resources. For this, routers must be used on each network or backbone to route the IP packets. For this, IP Routing should be enabled on routers. Routers must learn the destinations that are not directly connected by building and maintaining routing tables. Once the routing table is built, the router switches packets by matching the destination address of an incoming packet with the "longest match" in the routing table.

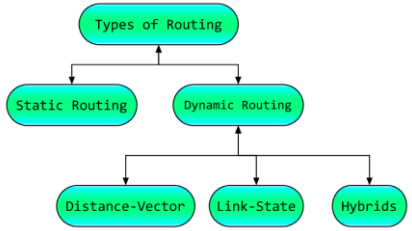
Types of IP Routing

A router can find best route to the destination by exchanging the routing information. This is possible only when any kind of IP Routing is enabled on the routers.

There are three types of IP Routing:

- ❑ Static Routing
- ❑ Default Routing
- ❑ Dynamic Routing





Static Routing

Features:

- ✓ Static Routing is the most reliable type of routing, although it is not very scalable.
- ✓ It is suitable for small internetwork.
- ✓ It uses a route that a network administrator enters into the router manually. In static routing, if an administrator wants to communicate with any network, in this case, administrator has to manually add that particular network (network number) in the routing table. It will appear in the routing table with an administrative distance of 1.
- ✓ The static IP Routing enabled no extra overhead and the cost of the network is comparatively reduced. So it will not cost much, because it does not require much CPU processes and bandwidth on the network links comparatively.

An Internetwork

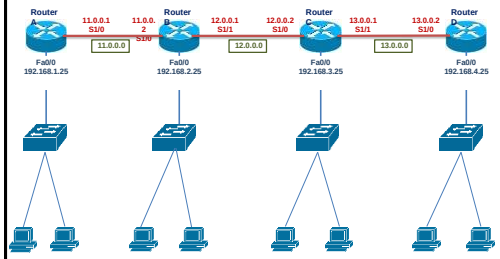


Figure - **An Internetwork**

Dynamic Routing

Features:

- ✓ Dynamic Routing is a routing in which some protocols are used to find the networks and update routing tables on routers. The router used routing protocols for Dynamic routing.
- ✓ Dynamic routing is easier than using static or default routing, but it will cost you in terms of router CPU processes and bandwidth on the network links.
- ✓ A routing protocol defines the set of rules used by a router when it communicates routing information between neighbor routers.

Routing Protocols

Routing Protocols are the protocols which are used to find or searchth e available paths for the data communication.

Types of Routing Protocols:

- ✓ Distance Vector
- ✓ Link State
- ✓ Hybrid

Distance Vector Routing Protocols

Features:

- ✓ The protocols which find the best path to a remote network by judging distance.
- ✓ Each time a packet goes through a router, that's called a **hop**. The route with the least number of hops to the network is determined to be the best route.
- ✓ It is also responsible to broadcast the entire routing table in such time of intervals.

Example: -

- **RIP** (Routing Information Protocol)
- **IGRP** (Interior Gateway Routing Protocol)

Link State Routing Protocols

Features:

- ✓ Link-state protocols use an algorithm called the Shortest Path First to find the best path to a destination.
- ✓ It prepares three separate tables. One of the tables keeps track of directly attached neighbors, one determines the topology of the entire internetwork, and one is used as the routing table.
- ✓ Link-state routers know more about the internetwork than any distance vector routing protocol. Well, Link-state protocols are normally used in large Internetworks.

Example: -

- **OSPF** (Open Shortest Path First)

Hybrid Routing Protocols

Features:

- ✓ A Hybrid protocol takes the advantages of both distance vector and Link- state protocols and merges them into a new protocol.
- ✓ They take the best features and avoid the pitfalls of both Distance Vector and Link State routing protocols.
- ✓ Hybrid Routing Protocols has more features than the distance vector and Link State routing protocols.

Example: -

- **EIGRP** (Enhanced Interior Gateway Routing Protocol)

Virtual LAN (VLAN)

Now days, Broadcast domain is a major problem in the pure switched networks. To solve this problem, we can create a Virtual Local Area Network (VLAN). A VLAN is a logical grouping of network users and resources connected to administratively defined ports on a switch. When you create VLAN's, you are given the ability to create smaller broadcast domains within Layer 2 Switched Internetwork by assigning different ports on the switch to different subnetworks. A VLAN treated like its own subnet or broadcast domain, meaning that frames broadcast onto the network are only switched between the ports logically grouped within the same VLAN. Switch maintains its own database for the VLAN's and its information.

The two simple reasons to create VLAN's on a switch are:

- **To minimize the broadcast domain**
- **To reduce the cost of the network**

You can solve many of the problems associated with Layer 2 switching with VLAN's. Here's a list of ways VLAN's simplify network management:

- ✓ Network adds, moves and changes are achieved with ease by just configuring a port into the appropriate VLAN.
- ✓ A group of users that need an unusually high level of security can be put into its own VLAN, so that users outside of the VLAN's can't communicate with them.
- ✓ As a logical grouping of users by function, VLAN's can be considered independent from their physical or geographic locations.
- ✓ VLAN's greatly enhance network security.
- ✓ VLAN's increase the number of broadcast domains while decreasing their size.

Types of Virtual LAN (VLAN)

- Static VLAN
- Dynamic VLAN

Static VLAN: Creating static VLAN is the most common way to create a VLAN, and one of the reasons for that is because static VLAN's are the most secure. This security terms from the fact that any switch port you have assigned a VLAN association to will always maintain it unless you change the port assignment manually.

Dynamic VLAN: A dynamic VLAN determines a node's VLAN assignment automatically. Using intelligent management software, you can base VLAN assignments on hardware (MAC) addresses, protocols, or even applications that create dynamic VLAN's.

A switch port can belong to only one VLAN at a time if it is an access port or all VLAN's if it is a trunk port. You can manually configure a port as an access or trunk port, or you can let the **Dynamic Trunking Protocol** (DTP) operate on a per-port basis to set the switchport mode. DTP does this by negotiating with the port on the other end of the link.

Ports	Port Description
Access Ports	An access port belongs to and carries the traffic of only one VLAN. Traffic is both send and received in native formats with no VLAN tagging whatsoever. Anything arriving on an access port is simply assumed to belong to the VLAN assigned to the port.
Voice Access Ports	An access port can be assigned to only one VLAN is really only sort of true. Nowadays, most switches will allow you to add a second VLAN to an access port on switch port for your voice traffic; it's called voice VLAN. The voice VLAN used to be called the auxiliary VLAN, which allowed it to be overlaid on top of the data VLAN, enabling both types of traffic through the same port.
Trunk Ports	The term trunk port was inspired by the telephone system trunks that carry multiple telephone conversations at a time. So it follows that trunk ports can similarly carry multiple VLAN's at a time. A trunk link is a 100-1000 Mbps point-to- point link between two switches, between switch and router or even between a switch and server. It carries the traffic of multiple VLAN's – from 1 to 4094 at a time (though its really only up to 1005 unless you are going with extended VLAN's.)

An VLAN Configured Network

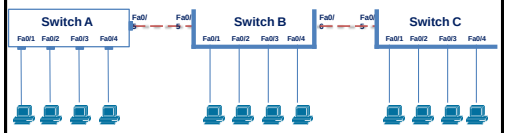


Figure – **VLAN Management**

Switch A	Switch B	Switch C
VLAN 2 - Sales	VLAN 2 - Sales	VLAN 2 - Sales
VLAN 3 - Accounts	VLAN 3 - Accounts	VLAN 3 - Accounts
Fa0/1 - Fa0/2 belongs to VLAN 2 Fa0/3 - Fa0/4 belongs to VLAN 3 Fa0/5 - Trunk Port	Fa0/1 - Fa0/3 belongs to VLAN 3 Fa0/4 belongs to VLAN 2 Fa0/5, Fa0/6 -Trunk Port	Fa0/1 - Fa0/3 belongs to VLAN 2 Fa0/4 belongs to VLAN 3 Fa0/5 - Trunk Port

VLAN Identification Methods

- **InterSwitch Link:** ISL is a Cisco Proprietary VLAN identification protocol that can be used only on Fast Ethernet and Gigabit Ethernet ports. Because the protocol is proprietary, it can only be used to trunk between Cisco devices. ISL actually re- encapsulates the entire original frame with a new header and new CRC value.

- **IEEE 802.1q**:The IEEE 802.1q is the industry standard method of VLAN identification. This protocol doesn't entirely re-encapsulate a frame, but instead adds VLAN identification information into Ethernet frames. This in turn can make Ethernet frames as large as 1522 bytes. When you want to use VLAN identification on a network that includes equipment from different vendors, 802.1q should be used.

Frame Tagging

- Frame tagging is a technique where additional VLAN identification information as added to a frame. Two main protocols exists for the purpose of Ethernet frame tagging- Inter Switch Linking (ISL) and IEEE 802.1q. Both modify a frame in frame in different ways to add VLAN identifiers. Once implemented, VLAN tagging allows ports on the same VLAN (but on different switches) to communicate as though they were part of a single physical switch.

VLAN Trunking Protocol (VTP)

VLAN Trunking Protocol (VTP) is a Cisco Layer 2 messaging protocol that manages the addition, deletion and renaming of VLAN's on a network-wide-basis. Virtual Local Area Network (VLAN) Trunking Protocol (VTP) reduces administration in switched network and is also maintain the consistency of the switched network. When you configure a new VLAN on a VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere. VTP is a **Cisco Proprietary Protocol** that is available on most of the Cisco Catalyst Family products.

VTP ensures that all switches in the VTP domain are aware of all VLAN's. There are occasions, however, when VTP can create unnecessary traffic. All unknown unicasts and broadcasts in a VLAN are flooded over the entire VLAN. All switches in the network receive all broadcasts, even in situations where few users are connected in that VLAN. VTP pruning is a feature used to eliminate (or prune) this unnecessary traffic.