CCNA Routing and Switching Cisco

Special Thanks to

Mr. Raj Bhanushali (CCNA Trainer)

CCNA-ROUTING

TABLE OF CONTENTS

What is Networking?

Networking is a connection of 2 or more devices WITH THE SAME RANGE OF IP ADDRESS UNDER COMMON PROTOCOL.

Types of Networks :

- LAN [Local Area Network] : A **local-area network** (**LAN**) is a computer network that spans a relatively small area. Most often, a **LAN** is confined to a single room, building or group of buildings, however, one **LAN** can be connected to other **LANs** over any distance via telephone lines and radio waves.

- MAN [Metropolitan Area Network] : A **metropolitan area network** (MAN) is a **network** that interconnects users with computer resources in a geographic **area** or region larger than that covered by even a large local **area network** (LAN) but smaller than the **area** covered by a wide **area network** (WAN).

- WAN [Wide Area Network] : A computer **network** that spans a relatively large geographical area. Typically, a **WAN** consists of two or more local-area **networks** (LANs). Computers connected to a **wide-area network** are often connected through public **networks**, such as the telephone system. They can also be connected through leased lines or satellites.

- GAN [Global Area Network] : A global area network (GAN) refers to a network composed of different interconnected networks that cover an **unlimited geographical area**. The term is loosely synonymous with **Internet**, which is considered a global area network.

NETWORK TOPOLOGIES :

- BUS

- RING

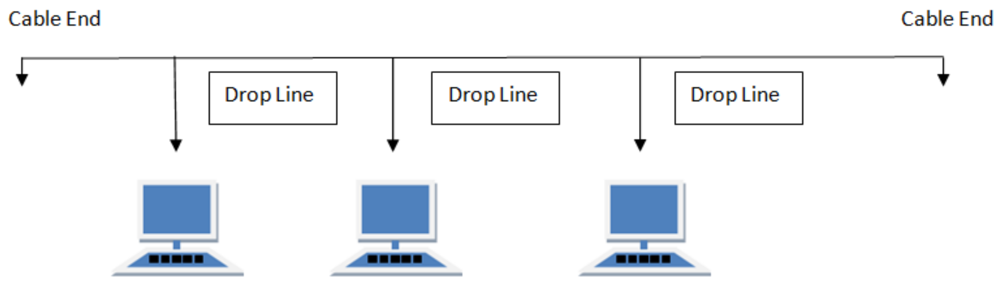
- STAR

- MESH

- HYBRID

BUS Topology :

Bus topology is a network type in where every computer and network device is connected to single cable.



Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

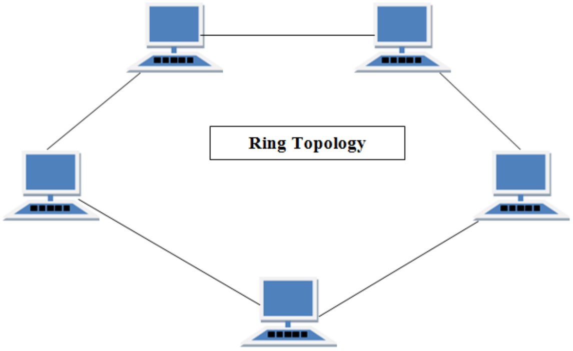
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

RING Topology:

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



Features of Ring Topology

1. A number of repeaters are used and the transmission is unidirectional.
2. Date is transferred in a sequential manner that is bit by bit.

Advantages of Ring Topology

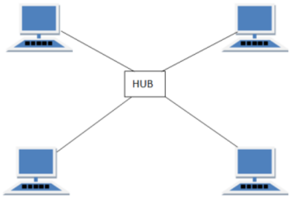
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

STAR Topology:

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

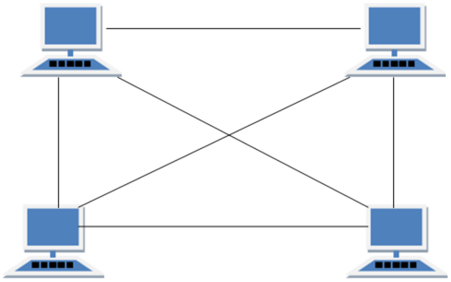
1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub is affected then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

MESH Topology:

It is a point-to-point connection to other nodes or devices. Traffic is carried only between two devices or nodes to which it is connected. Mesh has n (n-2)/2 physical channels to link h_n devices.



Types of Mesh Topology

1. **Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :** Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Not flexible.

Advantages of Mesh Topology

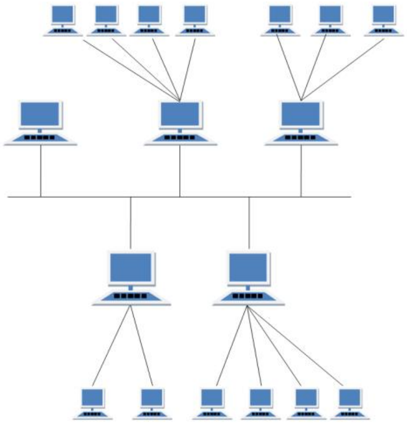
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

HYBRID Topology :

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

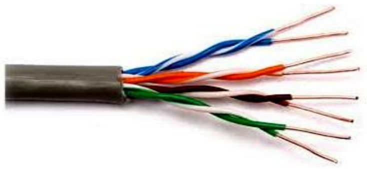
1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

Twisted Pair Cable:

Twisted pair cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of canceling outelectromagnetic interference (EMI) from external sources; for instance, electromagnetic radiation from unshielded twisted pair (UTP) cables, and crosstalk between neighboring pairs. It was invented by Alexander Graham Bell.



UTP Cable

STP Cable

UTP vs STP

Twisted pair cables are widely used in transmitting information, especially across great distances. The twist in the wire cancels out any magnetic interference that may develop in the wiring. There are two common types of twisted pair cabling, STP and UTP. The S stands for Shielded, the U stands for Unshielded, and the TP stands for twisted pair for both. STP simply has additional shielding material that is used to cancel any external interference that may be introduced at any point in the path of the cable. UTP cables have no protection against such interference and its performance is often degraded in its presence. Using STP cables ensure that you get the maximum bandwidth from your cabling even if the external condition is less than ideal.

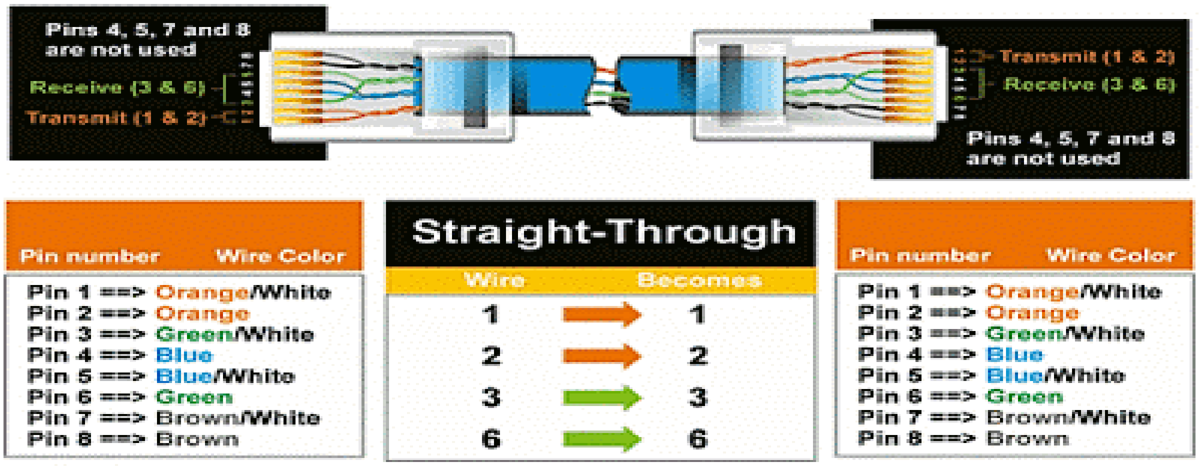
The biggest drawback to using STP cables is the higher cost. The shielding is an additional material that goes into every meter of the cable, thereby raising its total cost. The shielding also makes the cable heavier and a bit more difficult to bend or manipulate in any way. This is not a big issue but something that users should know when choosing between STP and UTP. In terms of usage, UTP is the more prevalent and popular cabling that is used in most homes, offices, and even in large scale businesses due to its lower cost.

STP is commonly used by large scale companies in high-end applications that require the maximum bandwidth. STP cables are also used in outdoor environments where the cables are exposed to the element sand man made structures and equipment that may introduce additional interference.

Good examples of this would be the telephone/internet cables that run from your home, to the junction box, down to the establishments of your provider or ISP. For most common uses, it does not really matter whether you use STP or UTP as both would probably perform well. UTP is the more logical choice as it is cheaper and much easier to find in the majority of computer equipment retailers.

Straight Cable:

You usually use straight cable to connect different type of devices. This type of cable will be used most of the time and can be used to:
1) Connect a computer to a switch/hub's normal port.
2) Connect a computer to a cable/DSL modem's LAN port.
3) Connect a router's WAN port to a cable/DSL modem's LAN port.
4) Connect a router's LAN port to a switch/hub's uplink port. (normally used for expanding network)
5) Connect 2 switches/hubs with one of the switch/hub using an uplink port and the other one using normal port.



Pin number	Wire Color
Pin 1 ==>	Orange/White
Pin 2 ==>	Orange
Pin 3 ==>	Green/White
Pin 4 ==>	Blue
Pin 5 ==>	Blue/White
Pin 6 ==>	Green
Pin 7 ==>	Brown/White
Pin 8 ==>	Brown

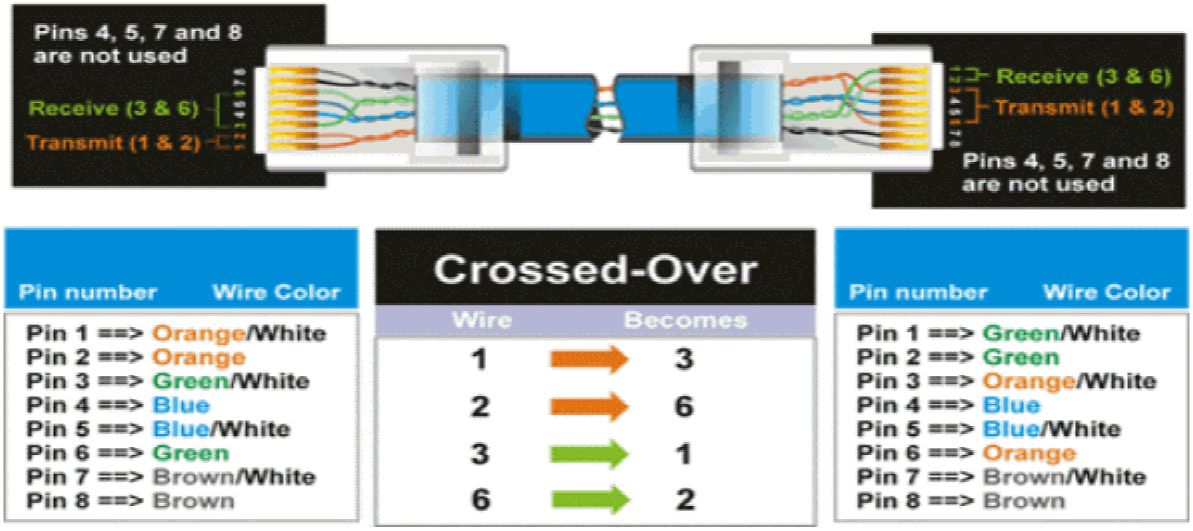
Straight-Through

Wire		Becomes
1	→	1
2	→	2
3	→	3
6	→	6

Pin number	Wire Color
Pin 1 ==>	Orange/White
Pin 2 ==>	Orange
Pin 3 ==>	Green/White
Pin 4 ==>	Blue
Pin 5 ==>	Blue/White
Pin 6 ==>	Green
Pin 7 ==>	Brown/White
Pin 8 ==>	Brown

Crossover Cable:

Sometimes you will use crossover cable, it's usually used to connect same type of devices. A crossover cable can be used to:
1) Connect 2 computers directly.
2) Connect a router's LAN port to a switch/hub's normal port. (normally used for expanding network)
3) Connect 2 switches/hubs by using normal port in both switches/hubs.



Pin number	Wire Color
Pin 1 ==>	Orange/White
Pin 2 ==>	Orange
Pin 3 ==>	Green/White
Pin 4 ==>	Blue
Pin 5 ==>	Blue/White
Pin 6 ==>	Green
Pin 7 ==>	Brown/White
Pin 8 ==>	Brown

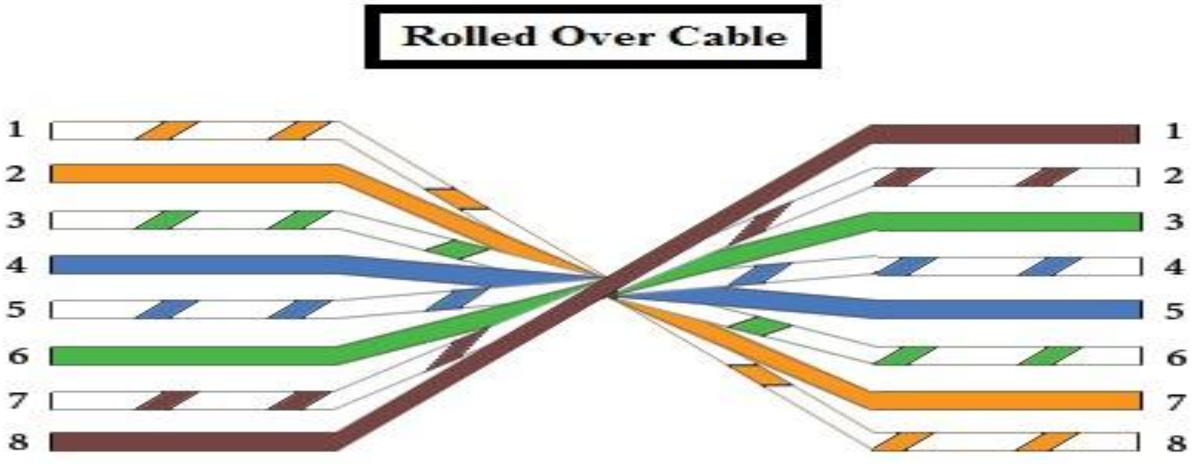
Crossed-Over

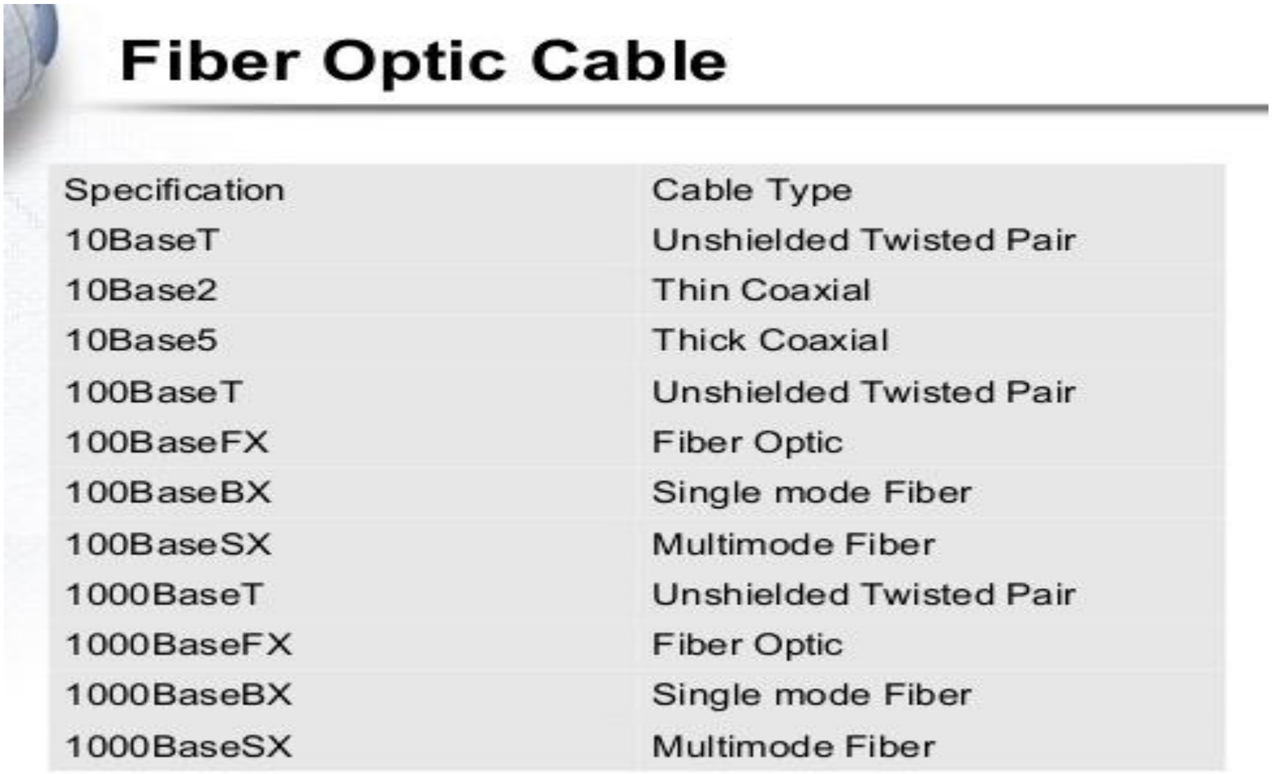
Wire		Becomes
1	→	3
2	→	6
3	→	1
6	→	2

Pin number	Wire Color
Pin 1 ==>	Green/White
Pin 2 ==>	Green
Pin 3 ==>	Orange/White
Pin 4 ==>	Blue
Pin 5 ==>	Blue/White
Pin 6 ==>	Orange
Pin 7 ==>	Brown/White
Pin 8 ==>	Brown

Rollover cable:

Rollover cable (also known as Cisco console cable or a Yostcable) is a type of null-modem cable that is often used to connect a computer terminal to a router's console port. Thiscable is typically flat (and has a light blue color) to help distinguish it from other types of network cabling.





Fiber Optic Cable

Specification	Cable Type
10BaseT	Unshielded Twisted Pair
10Base2	Thin Coaxial
10Base5	Thick Coaxial
100BaseT	Unshielded Twisted Pair
100BaseFX	Fiber Optic
100BaseBX	Single mode Fiber
100BaseSX	Multimode Fiber
1000BaseT	Unshielded Twisted Pair
1000BaseFX	Fiber Optic
1000BaseBX	Single mode Fiber
1000BaseSX	Multimode Fiber

OSI MODEL

The **Open Systems Interconnection model** (**OSI model**) is a conceptual model that characterizes and standardizes thecommunication functions of a telecommunication or computing system without regard to their underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols. The model partitions a communication system into abstraction layers. The original version of the model defined seven layers.

A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that comprise the contents of that path. Two instances at the same layer are visualized as connected by a *horizontal* connection in that layer.

The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The Open Systems Interconnect (OSI) model has seven layers. This article describes and explains them, beginning with the 'lowest' in the hierarchy (the physical) and proceeding to the 'highest' (the application). The layers are stacked this way:

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

Functions of Different Layers :

Layer 1: The Physical Layer :

It activates, maintain and deactivate the physical connection. Voltages and data rates needed for transmission is defined in the physical layer. It converts the digital bits into electrical signal.

Layer 2: Data Link Layer :

Data link layer synchronizes the information which is to be transmitted over the data. Error controlling is easily done. The encoded data are then passed to physical. Error detection bits are used by the data link on layer. It also corrects the errors. Outgoing messages are assembled into frames. Then the system waits for the acknowledgements to be received after the transmission. It is reliable to send message.

Layer 3: The Network Layer :

It routes the signal through different channels to the other end. It acts as a network controller. It decides by which route data should take. It divides the outgoing messages into packets and to assemble incoming packets into messages for higher levels.

Layer 4: Transport Layer :

It decides if data transmission should be on parallel path or single path. Functions such as multiplexing, segmenting or splitting on the data done by layer four that is transport layer. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

Layer 5: The Session Layer :

Session layer manages and synchronize the conversation between two different applications. Transfer of data from one destination to another session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

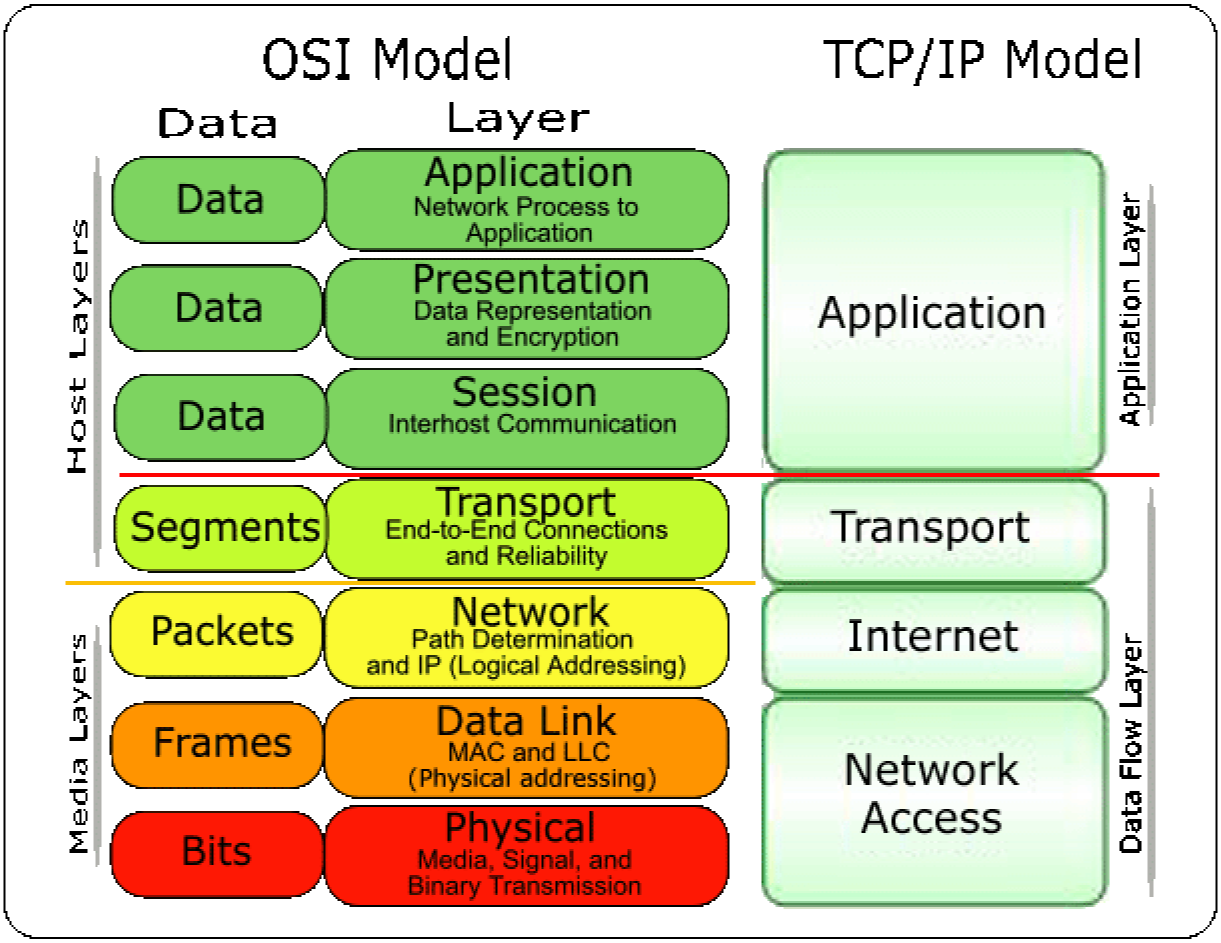
Layer 6: The presentation Layer :

Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data. Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role translator.

Layer 7: Application Layer :

It is the top layer. Manipulation of data (information) in various ways is done in this layer. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.

LAYER NAME	PROTOCOLS & SPECIFICATIONS	DEVICES
Application, Presentation, Session (Layers 5-7)	Telnet, HTTP, FTP, SMTP, POP3, VoIP, SNMP	Firewall, Intrusion Detection System
Transport Layer (Layer 4)	TCP, UDP	
Network Layer (Layer 3)	IP	ROUTER
Data Link Layer	Ethernet, HDLC, Frame Relay, PPP	SWITCHES, DSL Modem, Cable Modem
Physical Layer	Ethernet	HUBS



WHAT IS TCP AND UDP?

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)is a transportation protocol that is one of the core protocols of the Internet protocol suite. Both TCP and UDP work at transport layer TCP/IP model and both have very different usage.

Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
TCP is connection-oriented protocol. When a file or message send it will get delivered unless connections fails. If connection lost, the server will request the lost part. There is no corruption while transferring a message.	**UDP is connectionless protocol**. When you a send a data or message, you don't know if it'll get there, it could get lost on the way. There may be corruption while transferring a message.
TCP is a Reliable Protocol.	**UDP is an unreliable protocol.**
TCP sends acknowledgement.	**UDP does not send any acknowledgement.**
TCP header size is 20 bytes.	**UDP Header size is 8 bytes.**
The speed for TCP is slower than UDP.	**UDP is faster because there is no error-checking for packets.**
TCP is suited for applications that require high reliability, and transmission time is relatively less critical.	**UDP is suitable for applications that need fast, efficient transmission, such as games.**
TCP header size is 20 bytes	**UDP Header size is 8 bytes.**
TCP does Flow Control. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP does not have an option for flow control.

What is DNS?

The **Domain Name System** (**DNS**) is a hierarchical decentralized naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.

Most prominently, it translates more readily memorized domain names/website names to the numerical IP addresses needed for the purpose of locating and identifying computer services and devices with the underlying network protocols.

By providing a worldwide, distributed directory service, the Domain Name System is an essential component of the functionality of the Internet.

What is MAC Address?

A **media access control address** (**MAC address**), also called physical address, is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and WiFi. Logically, MAC addresses are used in the media access control protocol sub layer of the OSI reference model.

What is a node?

A network can consist of two or more computers directly connected by some physical medium such as coaxial cable or optical fiber. Such a physical medium is called as Links and the computer it connects is called as Nodes.

What is a gateway or Router?

A node that is connected to two or more networks is commonly called as router or Gateway. It generally forwards message from one network to another.

IP ADDRESSING

The success of TCP/IP as the network protocol of the Internet is largely because of its ability to connect together networks of different sizes and systems of different types. These networks are arbitrarily defined into three main classes (along with a few others) that have predefined sizes, each of which can be divided into smaller subnetworks by system administrators. A subnet mask is used to divide an IP address into two parts. One part identifies the host (computer), the other part identifies the network to which it belongs. To better understand how IP addresses and subnet masks work, look at an IP (Internet Protocol) address and see how it is organized.

- **Address -** The unique number ID assigned to one host or interface in a network.
- **Subnet -** A portion of a network that shares a particular subnet address.
- **Subnet mask -** A 32-bit combination used to describe which portion of an address refers to the subnet and which part refers to the host.
- **Interface -** A network connection.

Understand IP Addresses

An IP address is an address used in order to uniquely identify a device on an IP network. The address is made up of 32 binary bits, which can be divisible into a network portion and host portion with the help of a subnet mask. The 32 binary bits are broken into four octets (1 octet = 8 bits)

An IP address has two parts. The first part of an IP address is used as a network address, the last part as a host address. If you take the example 192.168.123.132 and divide it into these two parts you get the following:

192.168.123.132 - Network Address
0.0.0.132 - Host Address

Subnet mask :

The second item, which is required for TCP/IP to work, is the subnet mask. The subnet mask is used by the TCP/IP protocol to determine whether a host is on the local subnet or on a remote network.

In TCP/IP, the parts of the IP address that are used as the network and host addresses are not fixed, so the network and host addresses above cannot be determined unless you have more information. This information is supplied in another 32-bit number called a subnet mask.

A Subnet mask helps you know which portion of the address identifies the network and which portion of the address identifies the node. Class A, B, and C networks have default masks, also known as natural masks, as shown here:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

Network classes:

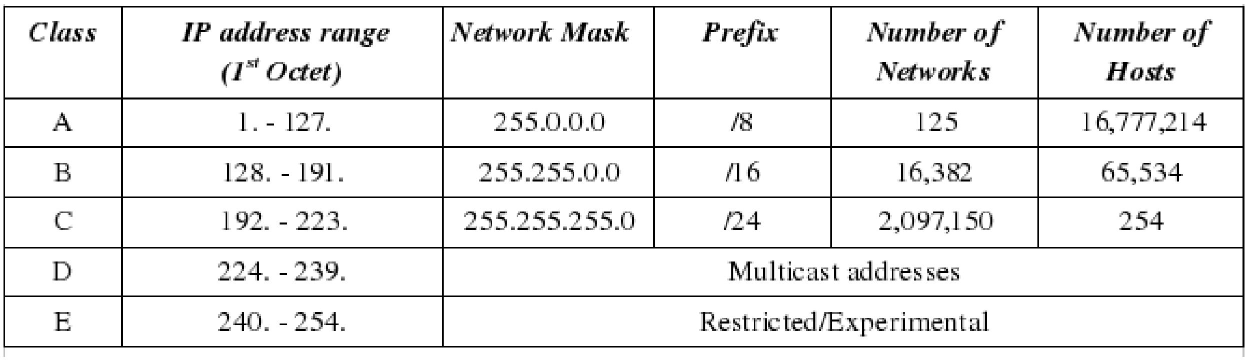
Internet addresses are allocated by the InterNIC, the organization that administers the Internet. These IP addresses are divided into classes. The most common of these are classes A, B, and C. Classes D and E exist, but are not generally used by end users. Each of the address classes has a different default subnet mask. You can identify the class of an IP address by looking at its first octet. Following are the ranges of Class A, B, and C Internet addresses, each with an example address:

- **Class A networks** use a default subnet mask of **255.0.0.0** and have **0-127** as their first octet. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.

- **Class B networks** use a default subnet mask of **255.255.0.0** and have **128-191** as their first octet. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.

- **Class C networks** use a default subnet mask of **255.255.255.0** and have **192-223** as their first octet. The address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.

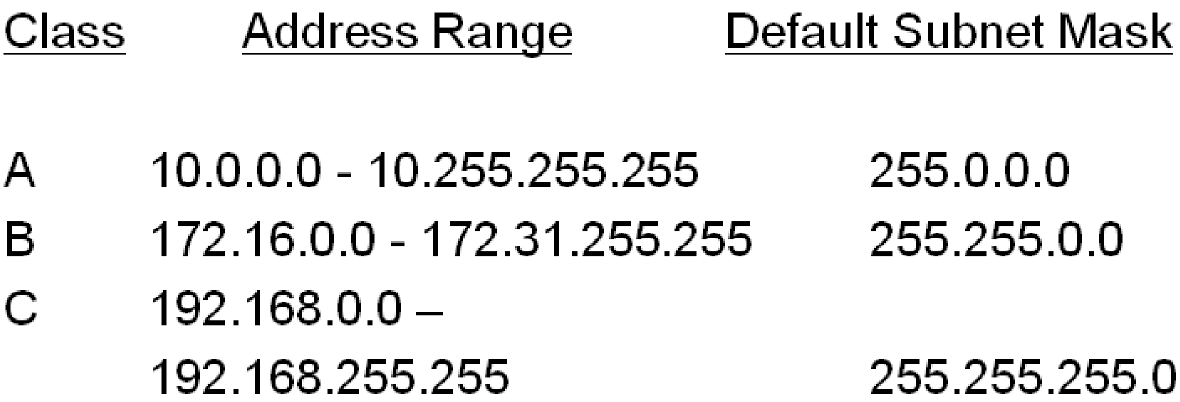
In some scenarios, the default subnet mask values do not fit the needs of the organization, because of the physical topology of the network, or because the numbers of networks (or hosts) do not fit within the default subnet mask restrictions. The next section explains how networks can be divided using subnet masks.



Class	*IP address range (1st Octet)*	*Network Mask*	*Prefix*	*Number of Networks*	*Number of Hosts*
A	1. - 127.	255.0.0.0	/8	125	16,777,214
B	128. - 191.	255.255.0.0	/16	16,382	65,534
C	192. - 223.	255.255.255.0	/24	2,097,150	254
D	224. - 239.	Multicast addresses			
E	240. - 254.	Restricted/Experimental			

*** 127 is used as loop back address for testing purposes.**

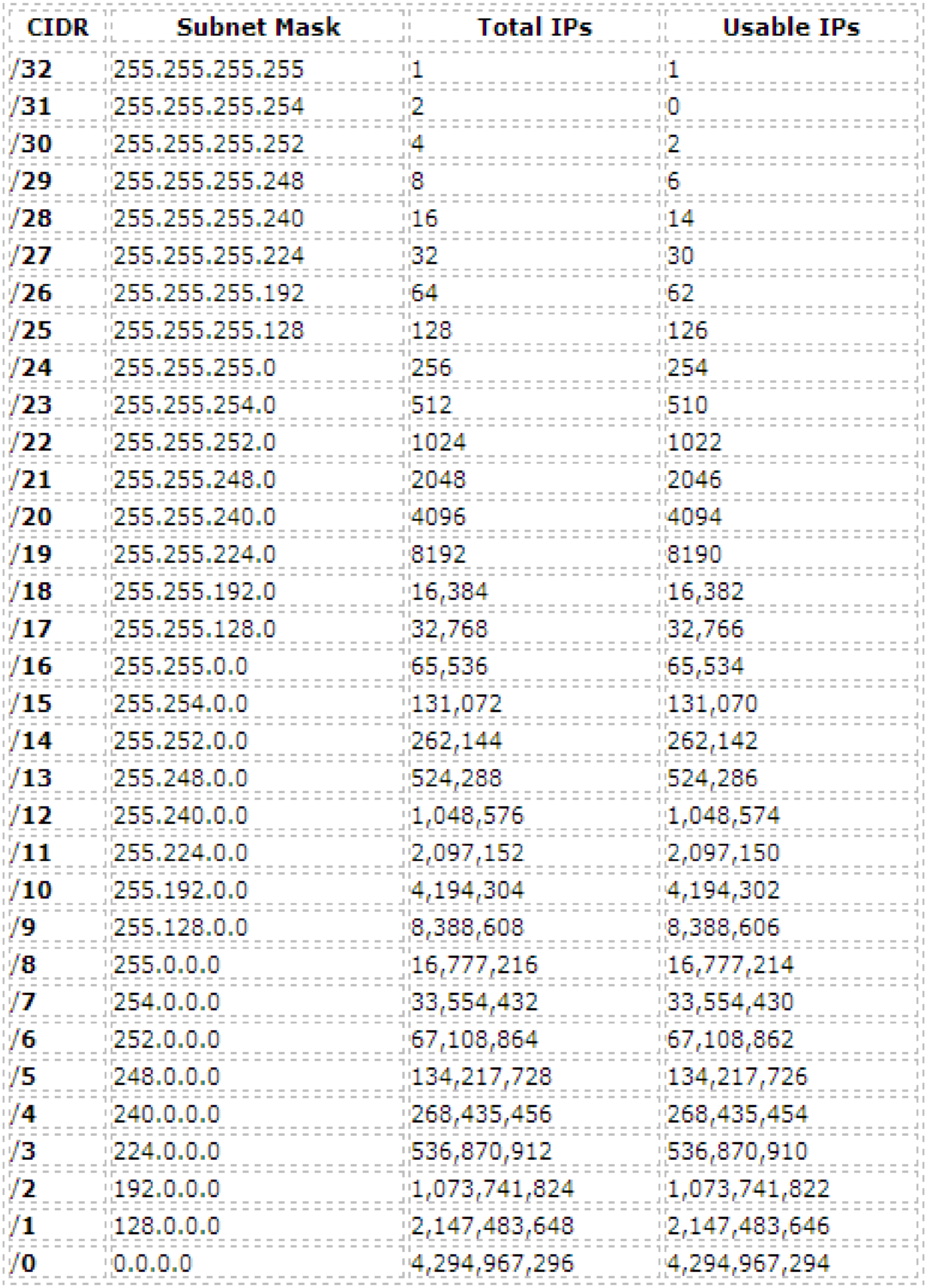
Private Address/Free:



Class	Address Range	Default Subnet Mask
A	10.0.0.0 - 10.255.255.255	255.0.0.0
B	172.16.0.0 - 172.31.255.255	255.255.0.0
C	192.168.0.0 – 192.168.255.255	255.255.255.0

SUBNET MASK’s:

/8	=	255.0.0.0
/9	=	255.128. 0.0
/10	=	255.192.0.0
/11	=	255.224.0.0
/12	=	255.240.0.0
/13	=	255.248.0.0
/14	=	255.252.0.0
/15	=	255.254.0.0
/16	=	255.255.0.0
/17	=	255.255.128.0
/18	=	255.255.192.0
/19	=	255.255.224. 0
/20	=	255.255.240. 0
/21	=	255.255.248. 0
/22	=	255.255.252. 0
/23	=	255.255.254. 0
/24	=	255.255.255. 0
/25	=	255.255.255.128
/26	=	255.255.255.192
/27	=	255.255.255.224
/28	=	255.255.255.240
/29	=	255.255.255.248
/30	=	255.255.255.252
/31	=	255.255.255.254
/32	=	255.255.255.255



CIDR	Subnet Mask	Total IPs	Usable IPs
/32	255.255.255.255	1	1
/31	255.255.255.254	2	0
/30	255.255.255.252	4	2
/29	255.255.255.248	8	6
/28	255.255.255.240	16	14
/27	255.255.255.224	32	30
/26	255.255.255.192	64	62
/25	255.255.255.128	128	126
/24	255.255.255.0	256	254
/23	255.255.254.0	512	510
/22	255.255.252.0	1024	1022
/21	255.255.248.0	2048	2046
/20	255.255.240.0	4096	4094
/19	255.255.224.0	8192	8190
/18	255.255.192.0	16,384	16,382
/17	255.255.128.0	32,768	32,766
/16	255.255.0.0	65,536	65,534
/15	255.254.0.0	131,072	131,070
/14	255.252.0.0	262,144	262,142
/13	255.248.0.0	524,288	524,286
/12	255.240.0.0	1,048,576	1,048,574
/11	255.224.0.0	2,097,152	2,097,150
/10	255.192.0.0	4,194,304	4,194,302
/9	255.128.0.0	8,388,608	8,388,606
/8	255.0.0.0	16,777,216	16,777,214
/7	254.0.0.0	33,554,432	33,554,430
/6	252.0.0.0	67,108,864	67,108,862
/5	248.0.0.0	134,217,728	134,217,726
/4	240.0.0.0	268,435,456	268,435,454
/3	224.0.0.0	536,870,912	536,870,910
/2	192.0.0.0	1,073,741,824	1,073,741,822
/1	128.0.0.0	2,147,483,648	2,147,483,646
/0	0.0.0.0	4,294,967,296	4,294,967,294

SUBNETTING

Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is unrealistic.

Each data link on a network must have a unique network ID, with every node on that link being a member of the same network. If you break a major network (Class A, B, or C) into smaller subnetworks, it allows you to create a network of interconnecting subnetworks. Each data link on this network would then have a unique network/subnetwork ID. Any device, or gateway, that connects *n* networks/subnetworks has *n* distinct IP addresses, one for each network / subnetwork that it interconnects.

EXAMPLE :

A system administrator who is allocated a block of IP addresses may be administering networks that are not organized in a way that easily fits these addresses. For example, you have a wide area network with 150 hosts on three networks (in different cities) that are connected by a TCP/IP router. Each of these three networks has 50 hosts. You are allocated the class C network 192.168.123.0. (For illustration, this address is actually from a range that is not allocated on the Internet.) This means that you can use the addresses 192.168.123.1 to 192.168.123.254 for your 150 hosts.

Two addresses that cannot be used in your example are 192.168.123.0 and 192.168.123.255 because binary addresses with a host portion of all ones and all zeros are invalid. The zero address is invalid because it is used to specify a network without specifying a host. The 255 address (in binary notation, a host address of all ones) is used to broadcast a message to every host on a network. **Just remember that the first and last address in any network or subnet cannot be assigned to any individual host.**

You should now be able to give IP addresses to 254 hosts. This works fine if all 150 computers are on a single network. However, your 150 computers are on three separate physical networks. Instead of requesting more address blocks for each network, you divide your network into subnets that enable you to use one block of addresses on multiple physical networks.

The advantages associated with Subnetting a network are summarized below:

- Through subnetting, you can reduce network traffic and thereby improve network performance. You only allow traffic that should move to another network (subnet) to pass through the router and to the other subnet.

- Subnettiing can be used to restrict broadcast traffic on the network.

- Subnetting facilitates simplified management.You can delegate control of subnets to other administrators.

- Troubleshooting network issues is also simpler when dealing with subnets than it• is in one large network.

Types of Subnetting:

# FLSM [Fixed Length Subnet Mask]
# VLSM [Variable Length Subnet Mask]

Variable-Length Subnet Masking (**VLSM**) amounts to "subnetting subnets," which means that **VLSM** allows **network** engineers to divide an IP address space into a hierarchy of subnets of different sizes, making it possible to create subnets with very different host counts without wasting large numbers of addresses.

Default gateways:

If a TCP/IP computer needs to communicate with a host on another network, it will usually communicate through a device called a router. In TCP/IP terms, a router that is specified on a host, which links the host's subnet to other networks, is called a default gateway. This section explains how TCP/IP determines whether or not to send packets to its default gateway to reach another computer or device on the network.

BASICS OF ROUTER CONFIGURATION

What is a Router?

Router is a device which connects to different networks with the help of routing and routing protocols. It also breaks up large layer 3 broadcast domain.

A Router is a networking device that forwards data packets between computer networks. Routers perform the "traffic directing" functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.

A router is connected to two or more data lines from different networks (as opposed to a network switch, which connects data lines from one single network). When a data packet comes in on one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its **Routing table** or routing policy, it directs the packet to the next network on its journey. This creates an overlay internetwork.

Router Memories

ROM : ROM **is read-only memory** available on a router's processor board. The initial bootstrap software that runs on a Cisco router is usually stored in ROM. ROM also maintains instructions for Power-on Self Test (POST) diagnostics. For ROM Software upgrades, the pluggable chips on the motherboard should be replaced.

RAM : RAM is a volatile data storage type of memory in which stored information is lost with power off. RAM stands for **random access memory** where the word random refers that stored data can be accessed in any order. RAM can be SRAM or DRAM. DRAM is used in more applications for the simplicity of its structure and lower cost.

RAM is used at run time for executable operating system code, and its subsystems, routing tables, caches, running configuration, packets, and so forth.

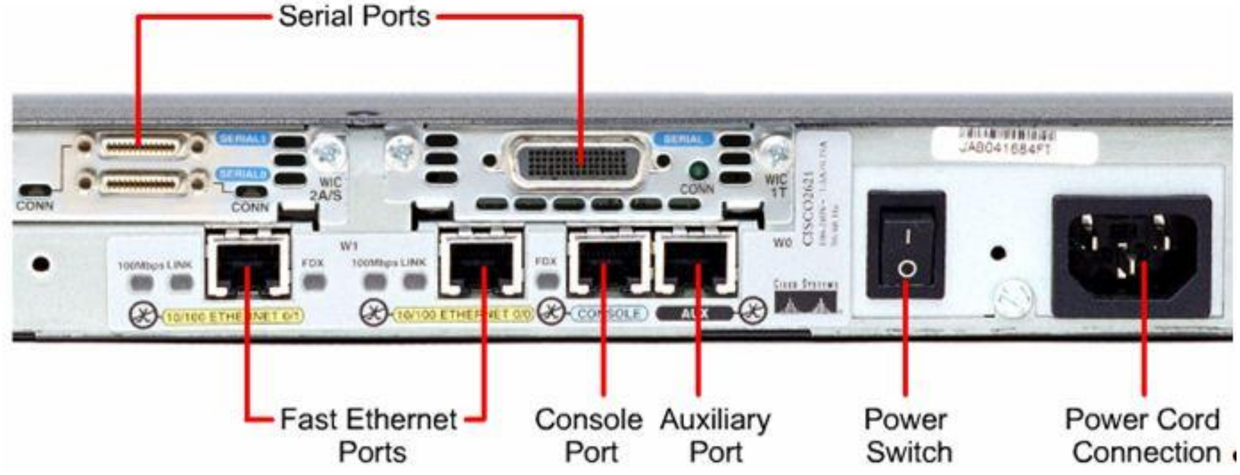
RAM Provides temporary memory for the router configuration file of the router while the router is powered on.

NVRAM : NVRAM stands for **non-volatile random access memory** and is used to describe any type of RAM that stored data is not lost by power turned off. NVRAM is used for writable permanent storage of the startup configuration in CISCO routers.

NVRAM is used to store the Startup Configuration File. This is the configuration file that IOS reads when the router boots up. It is extremely fast memory and retains its content when the router is restarted.

Flash : Flash memory is a non-volatile memory storage that doesn't lose the information by turning the power off. Flash memories exist in many forms in routers, internal flash, external flash card or even USB flash cards.

Flash is used for permanent storage of a full Cisco IOS software image in compressed form. In Juniper routers **Flash stores the JUNOS image and the configuration files.**



There is an AUX port which allows to configure the router remotely.

On CISCO Routers, there are 3 modes :

Exec Mode : Default Mode.

Enable Mode : Privileged Mode. #en

Configuration Mode : In this mode, we config the routers. Also known as global configuration mode. #configure terminal or #conf t.

To change the hostname, we have to be enter in configuration mode and enter the command.
#hostname R1

For assigning IP Address to R1, fa0/0
#int fa0/0
#ip add 10.0.0.1 255.0.0.0
#no shut
[no shut is used to permanently up the interface]
Similarly to all interfaces and routers.

Note : **To come back to privileged mode from config mode we have to just type #exit and we will be automatically thrown back to that mode.We can also use (Ctrl+z) to end up.**

# show running- config : Shows you the running configuration on that router.
# show startup-config : Shows you the NVRAM content.
#copy running-config startup-config : To save the config.
#wr : Is used to save the configuration as well.
#show ip interface brief: Shows all ip details.
#no ip domain lookup: For not getting stuck on any miss or corrupt entry or spelling mistake.

IP ROUTING

IP Routing is an umbrella term for the set of protocols that determine the path that data follows in order to travel across multiple networks from its source to its destination. Data is routed from its source to its destination through a series of routers, and across multiple networks. The IP Routing protocols enable routers to build up a forwarding table that correlates final destinations with next hop addresses.

IP Routing is done in 3 ways :

1. **Static Routing**
2. **Dynamic Routing**
3. **Default Routing**

1. Static Routing

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry.

Whenever you're doing static routing, just go to the router and define the unknown routes of the router.
For eg. if R1 has 2 unkown networks 30.0.0.0 & 40.0.0.0 then,
#ip route 30.0.0.0 255.0.0.0 20.0.0.2
#ip route 40.0.0.0 255.0.0.0 20.0.0.2

Here, 20.0.0.2 is the next hop ip address.. we calculate the next hop from the router from which we are pinging the other network. In this case the R1 router. To simplify it, imagine the other unknown network is some room 3 doors away. To reach there, we have to cross the door of the room we are in.. that means, the next hop is the door ie the next ip address.

Note : You can also assign serial interface like s0/0 for static routing.
#ip add 30.0.0.0 255.0.0.0 serial0/0

Static Routing is basically done on smaller networks. Manually assigning the routes is a hectic task when the network is big. Thus, dynamic routing is used by users to simplify the task.

2. Dynamic Routing :

- **Distance Vector : RIP , RIPv2, IGRP.**
- **Link State : OSPF & IS-IS.**
- **Hybrid : EIGRP.**

Distance Vector

- Metric is needed to calculate the best path towards the destination = minimum hop count.

- Periodic Update is done and sends complete Routing Table.

- Broadcast while updating and advertise.

- It has only one table that is routing table.

- Class full Protocol.

- Looping is possible : How to avoid looping :

    - Maximum Hop Count on rip is 15. IGRP is 256 but by default its 100.
    - **Split Horizon** - It will not allow the packet to be sent from the same interface.
    - **Route Poisoning** - Destination Router will send a fake update saying this is the max hop count to the source router.
    - **Holdown Timers** - Destination Router will wait for a defined timer.

RIP and RIPv2 :

RIP	RIPv2
RIP is the Routing Information Protocol.	RIPv2 is Routing Information Protocol version 2.
Metric is minimum hop count. (max hop count = 15)	Metric - Minimum Hop Count (max hop count = 15)
Sends Periodic Update and also sends complete table (30 secs).	Sends Periodic Update and Complete Table (30secs)
Broadcast while update and advertise.	**Multicast** while update and advertise with 224.0.0.9
It has only 1 table that is the routing table.	It has only 1 table ie routing table.
Classful protocol.	**Classless Protocol.**
Looping is possible.	Looping is possible.
Algorithm : Bellman Ford	Algorithm : Bellman Ford.
Administrative Distance : 120	Administrative Distance : 120
Hold Timer : 180 with elapse 60 secs.	Hold Timer : 180 with elapse 60 secs.
Flush Timer : 240 secs.	Flush Timer : 240 secs.
R1 (config) # router rip R1 (config) # network 10.0.0.0 R1 (config) # network 20.0.0.0 R1 (config) # network 70.0.0.0 R1 (config) # ^z # wr	R1 (config) # router rip R1 (config) # version 2 R1 (config) # no auto-summary R1 (config) # network 10.0.0.0 #^z #wr
NO AUTHENTICATION	**AUTHENTICATION**

NOTE : **In any routing protocol, if there is an equal metric for a particular destination, the routing protocol will do load balancing.**
It is packet based load balancing on CISCO Routers by default.

To remove RIP : **#no router rip**

IGRP (INTERIOR GATEWAY ROUTING PROTOCOL)

Interior Gateway Routing Protocol (**IGRP**) is a distance vector interior routing protocol (IGP) developed by Cisco. It is used by routers to exchange routing data within an autonomous system.

IGRP is a proprietary protocol. IGRP was created in part to overcome the limitations of RIP (maximum hop count of only 15, and a single routing metric) when used within large networks.

- Metric : Bandwidth + delay = Cost (composite metric)
- Periodic Update : 90 secs.
- Broadcast while update and advertise.
- It has only one table that is routing table.
- Classful Protocol (like RIP)
- Looping is possible.
- **CISCO Proprietary**. (Dual Algo or Diffusing Algo)
- Only on CISCO Router
- Administrative Distance = 100
- Hop max is 256 and by default its 100.

LINK STATE:

OSPF (OPEN SHORTEST PATH FIRST)

- Metric : Lowest Cost (Bandwidth)
- Incremental Update (periodic update every 30mins)
- Multicast while update and advertise**. Multicast address 224.0.0.5 & 224.0.0.6**
- It has 3 tables **:**
  NEIGHBOUR TABLE.
  TOPOLOGY TABLE.
  ROUTING TABLE.
- Classless Protocol.
- Loop free.
- Algorithm : Dijkstra (SPF)
- Administrative Distance : 110.
- **It has an area concept.**

NOTE :

- **Interior Gateway Protocols (IGP) are RIP, RIPv2, IGRP, OSPF, EIGRP and IS-IS.**
- **Exterior Gateway Protocols are BGP.**

AS = Autonomus System.

It is a system comprising of various routers under specific routing protocols.

ASBR = Autonomous System Border Router.
It is the router which connects 2 Autonomous System of same or different routing protocols running within them.

LINK STATE DATASTRUCTURES :

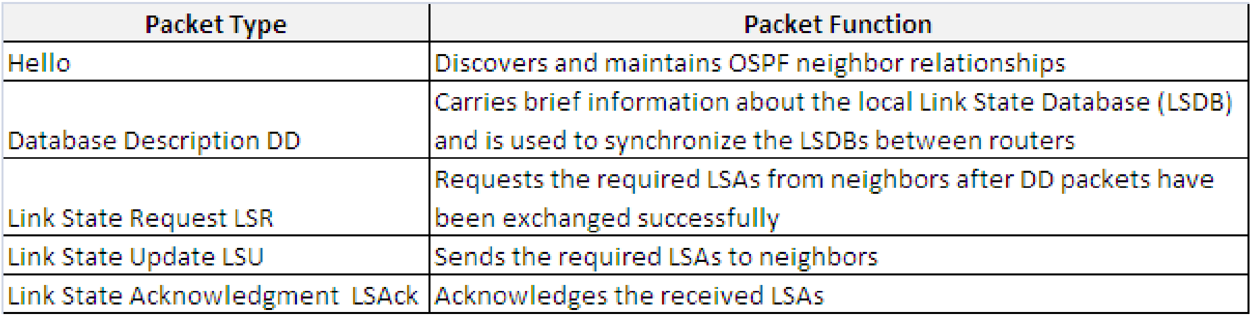
NEIGHBOUR TABLE: Also known as the adjacency database. List of recognised neighbors are in it.

TOPOLOGY TABLE : Referred to as LSDB. Routers and Links in the area or Network.
All routers within the area have an identical LSDB.

ROUTING TABLE : Commonly named a forwarding database. Lists the best paths to destinations.

OSPF PACKETS:

- Hello
- Database Description- DD
- Link State Request- LSR
- Link State Update- LSU
- Link State Acknowledgement- LSAck



Packet Type	Packet Function
Hello	Discovers and maintains OSPF neighbor relationships
Database Description DD	Carries brief information about the local Link State Database (LSDB) and is used to synchronize the LSDBs between routers
Link State Request LSR	Requests the required LSAs from neighbors after DD packets have been exchanged successfully
Link State Update LSU	Sends the required LSAs to neighbors
Link State Acknowledgment LSAck	Acknowledges the received LSAs

NEIGHBOURSHIP:

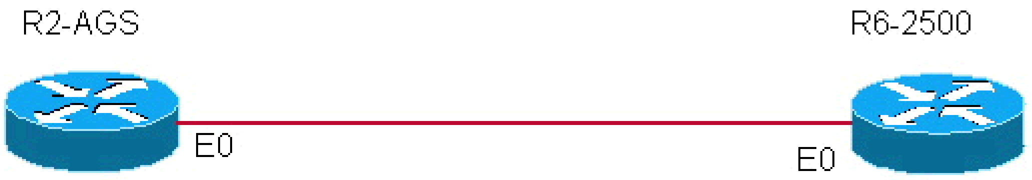
HELLO:

- **Router ID***
- Hello/Dead Intervals
- known Neighbors
- **Area ID***
- Router Priority
- DR IP address
- BDR IP address
- **Authentication Password***
- **Stub Area Flag***

***** **Entry must match on neighboring routers.**

Establishing Bidirectional Communication:

A:172.16.5.1/24 **B:172.16.5.2/24**



[DOWN STATE]

I'm router ID 172.16.5.1 and i see no one.

In this state the state is down and no neighbor ship is set.

[INIT STATE]

ROUTER B
Neighbor List
172.16.5.1/24 interface E0/0

I'm router ID 172.16.5.2 and I see 172.16.5.1.

In this state the router B sends the hello and adds router A in the neighbor list.

Router A
Neighbor list
172.16.5.2/24 interface E0/0

[TWO WAY STATE]

This state designates that bi-directional communication has been established between two routers. Bi-directional means that each router has seen the other's hello packet

[EXSTART STATE]

Router A : I will start exchange because I have ID 172.16.5.1

Router B: No, I will start because I have higher ID

[EXCHANGE STATE]

Router B : Here is the summary of my link state database

Router A : Here is my summary of link state database.

[LOADING STATE]

Router A : I need the complete entry for network 172.16.5.3/24

Router B : Here is the entry for network 172.16.5.3/24

Router A : Thanks for the information

[FULL STATE]

OSPF Neighbor StatesThe following is a brief summary of the states OSPF may pass through before becoming adjacent to (neighbors with) another router:

• **Down States :** No active neighbor detected.
• **Init States :** Hello packet received.
• **Two-way States:** Router see's its own router ID in a received hello packet.
• **ExStart States :** Master/slave roles determined.
• **Exchange States :** DBDs (summary of LSDB) sent.
• **Loading States :** Exchange of LSRs and LSUs, to populate LSDBs.
• **Full States :** Neighbors fully adjacent.

WHAT IS THE PURPOSE OF DR & BDR?

Based on the network type, OSPF router can elect one router to be a **Designated Router (DR)** and one router to be a **Backup Designated Router (BDR)**. For example, on multi-access broadcast networks (such as LANs) routers defaults to elect a DR and BDR. DR and BDR serve as the central point for exchanging OSPF routing information. Each non-DR or non-BDR router will exchange routing information only with the DR and BDR, instead of exchanging updates with every router on the network segment. DR will then distribute topology information to every other router inside the same area. This greatly reduces OSPF traffic.

Every router on a network segment establish a full neighbor relationship with the DR and BDR. Non-DR and non-BDR routers establish a two way neighbor relationship between themselves.

- In any multicast network, DR & BDR are elected
- DR & BDR are elected with higher priority, with default priority being 1.
- If the Priority is same, the higher router ID is chosen to elect the DR & BDR.
- DR election is non-preemptive.
- Non-DR routers are known as DR others.
- DR other routers for full state neighbourship only with DR & BDR.
- If priority is 0, no election for that router.
- DR other router forms neighbourship at the 2 way state to DR other routers.
- DR other routers update to DR and BDR with multicast address of 224.0.0.6
- DR updates other routers with 224.0.0.5

OSPF over NBMA (Non-broadcast multiple access) Topology modes of operation.

1. RFC complaint modes are as follows :
    - Non Broadcast (NBMA)
    - Point to Multipoint
2. Additional modes from CISCO are :
    - Broadcast
    - Point to Point

OSPF MODE	HELLO TIMER	RFC/CISCO
NBMA	30 seconds	RFC
Broadcast	10 seconds	CISCO
Point to Multipoint	30 seconds	RFC
Non-Broadcast	30 seconds	CISCO
Point to Point	10 seconds	CISCO

Wild Card Bits/ Inverse Mask :

0 - Care , 1- Ignore

A **wildcard mask** is a mask of bits that indicates which parts of an IP address are available for examination. In the Cisco IOS, they are used in several places, for example:

- To indicate the size of a network or subnet for some routing protocols, such as OSPF.
- To indicate what IP addresses should be permitted or denied in access control lists (ACLs).

At a simplistic level a wildcard mask can be thought of as an inverted subnet mask. For example, a subnet mask of 255.255.255.0 (binary equivalent = 11111111.11111111.11111111.00000000) inverts to a wildcard mask of 0.0.0.255.

A wild card mask is a matching rule The rule for a wildcard mask is:

- 0 means that the equivalent bit must match
- 1 means that the equivalent bit does not matter

For Example:

```
255.255.255.255   - Broadcast Address
255.255.255.0     - Subnet Mask

0   .0   .0   .255   - Wild Card Bits
```

* If you give subnet mask to router, then the router being on the IOS will convert subnet mask to wild card before sending it to the OSPF

OSPF Router Configuration :

```
R1 # conf t
R1 (config) # router ospf 10
R1 (config) # network  10.0.0.0   0.255.255.255  area 1
R1 (config) # network  20.0.0.0  0.255.255.255   area 0
R1 (config) # ^z
# wr
```

Specify networks and areas on R2,R3 and other routers respectively.

#show ip ospf database : shows the database on that router.

WHAT ARE LSA's ?

The **link-state advertisement** (LSA) is a basic communication means of the OSPF routing protocol for the Internet Protocol (IP). It communicates the router's local routing topology to all other local routers in the same OSPF area. OSPF is designed for scalability, so some LSAs are not flooded out on all interfaces, but only on those that belong to the appropriate area. In this way detailed information can be kept localized, while summary information is flooded to the rest of the network.

The LSA types defined in OSPF are as follows:

- **LSA 1** - Router LSA - The router announces its presence and lists the links to other routers or networks in the same area, together with the metrics to them. Type 1 LSAs are flooded across their own area only. The link-state ID of the type 1 LSA or LSA 1 is the originating router ID. Eg. **Area 0 will have LSA 1 on the routers in that area.**

- **LSA 2** - The Network LSA or LSA 2 is created for each multi-access network. Remember the OSPF network types? The broadcast and non-broadcast network types require a DR/BDR. If this is the case you will see these network LSAs being generated by the DR. In this LSA we will find all the routers that are connected to the multi-access network, the DR and of course the prefix and subnet mask.

- **LSA 3 -** This LSA will flood into all the other areas of our OSPF network. This way all the routers in other areas will know about the prefixes from other areas**. The router will provide information regarding OSPF Inter Area (OIA) via LSA 3.**

- **LSA 4 -** When ABR receives this router LSA it will create a **LSA 4** and flood it into specific area. This LSA will also be flooded in all other areas and is required so all OSPF routers know where to find the ASBR.
LSA 4 basically is generated by the ABR (Area Border Router) to provide information regarding the ASBR (Autonomous System Border Router).

- **LSA 5 -** External routes generated by the ASBR will be sent via LSA 5. It has 2 types : **External type 1 (E1) (actual cost) and External type 2 (E2) (cost 20 by default).**

- **LSA 6 -** Used in a now obsolete multicast version of Multicast Open Shortest Path First (MOSPF). **Most routers no longer support MOSPF.** this LSA may be reassigned in the future.

HYBRID:

EIGRP [Enhanced Interior Gateway Routing Protocol]

- Metric **:** Bandwidth + Delay (+MTU+Reliability+load)
- Incremental Update.
- Multicast while update and advertise**.**
  Multicast address 224.0.0.10
- It has three tables:
  1. Neighbor table.
  2. Topology table. Best path (successor) & second best path (feasible successor)
  3. Routing table.
- Classless Protocol.
- Loop free.
- CISCO Proprietary (dual algo or diffusing algo)(May 2014) Partially Open Source.
- Administrative Distance: 90.
- Max Hop 256 and by default its is 100.
- It supports unequal cost path load balancing.

Composite Matrix:

***K1 = Bandwidth, K2 = Reliability, *K3 = Delay**
K4 = Load, K5 = MTU. (*By default)

EIGRP Features:

- Advanced Distance Vector Protocol = By rumour.
- Rapid Convergence.
- 100% Loop free Classless Routing.
- Easy Configuration.
- Incremental Update.
- Load across equal and unequal cost pathways.
- Flexible Network Design.
- Multicast/Unicast instead of Broadcast.
- Support for VLSM and Discontiguous subnets.
- Manual Summarization at any point in internetwork.
- Support for multiple network layer protocols. - IP, IPX, SPX, APPLETEK.
    - ❖ **Routed Protocol:** IP, IPX, SPX, APPLETEK .
    - ❖ **Routing Protocols:** RIP, RIPv2, OSPF, IGRP, EIGRP, BGP, IS-IS.

Metric Calculation:

Delay: Delay is the sum of all the delays in 10's of microsecond x 256.

Bandwidth : 10,000,000 / lowest bandwidth on the link x 256.

Metric = Bandwidth + Delay.

Storage = 1 MB = 1024 KB (Mega Byte) (Kilo Byte)

Transfer = 1Mbps = Megabits per sec = 1000 Kbps.

T1 = 1.544 Mbps, E1 = 2.048 Mbps.

EIGRP Packets:

- **Hello** : Establish Neighbor Relationships.
- **Update** : Send Routing Updates.
- **Query** : Ask neighbors about routing info.
- **Reply** : Respond to query about routing info.
- **ACK** : Acknowledge a reliable packet.

EIGRP Hello Packets :

- Two routers becomes neighbors when they see the hello packet of the other router. Hello Address = 224.0.0.10
- EIGRP does not form neighbors if K values are mismatched.
- EIGRP does not form neighbors if AS numbers are mismatched.
- T1 or less than T1 line = 60 seconds hello x 3 times =180 seconds hold timer.
- More than T1 line = 5 seconds hello x 3 times = 15 seconds hold timer.

EIGRP Retransmission Policy:

- Router keeps a neighbor list and a retransmission list for every neighbor.
- Each reliable packet (update, query, reply) is transmitted when the packet is not acknowledged.
- A neighbor relationship is reset when the retry limit (16) for reliable packets is reached.
- Retransmission occurs each time the RTO is reached.

EIGRP SUMMARY:

1. **EIGRP has Five packets :**
   - **Update, Query, Reply packets require acknowledgement.**
   - **Hello and ACK do not require acknowledgement.**

2. **EIGRP hello packets are used to build EIGRP adjacencies.**

3. **By default, hellos are sent in the following intervals.**
   - **Every 60 secs on T1 or slower multipoint interfaces.**
   - **Every 5 secs on all others.**

4. **The router resets neighbor relationship when it reaches the retry limit (16) or when hold time expires.**

5. **Neighbor routers are slow to respond to multicasts receive unacknowledged packets again as unicast packets.**

DIFFUSING UPDATE ALGORITHM

A **diffusing update algorithm** (DUAL or DUAL finite state machine) is a convergence algorithm that dictates a routing protocol used by Cisco's proprietary Enhanced Interior Gateway Routing Protocol (EIGRP) to prevent routing loops via a continuous route computation.

EIGRP is responsible for the routing within an autonomous system and DUAL responds to changes in the routing topology and dynamically adjusts the routing tables of the router automatically.

DUAL uses EIGRP’s composite metric in the form of the Feasible Distance and Advertised Distance to make its route selections.

- The **Feasible Distance (FD)** is the total distance (metric) from the router to its destination.

- The **Advertised Distance (AD)** is the distance (metric) advertised by a neighbor router to its destination.

- The **Feasibility Condition (FC)** is fulfilled when the feasible successor's A.D is less than the successor's F.D.

- **Variance** is used when the successor's FD is greater than the feasible successor's AD.

For E.g. if

	FD	AD
R2	11	6
R4	14	9

then, variance = 2 (multiplier) = 11x2 = 22

11------------14-----------------22.

70% 30%

The packets will be sent in this manner. (The % is just for example).

Configuration EIGRP:

```
R1 # conf t
R1 (config) # router eigrp 10
R1 (config) # no auto-summary
R1 (config) # network  10.0.0.0
R1 (config) # network 20.0.0.0
R1 (config) # ^z
# wr
```

Show Commands :

```
#show ip eigrp neighbors
#show ip eigrp topology
```

EIGRP DUAL Overview:

- – It tracks all routes advertised by neighbors
- – Selects loop free path using successor and remembers any feasible successors.
- – If the successor is lost, it uses feasible successor.
- – If there is no feasible successor, it queries the neighbors and recompute a new successor.

- DUAL is a finite state formula that uses discovery process to calculate loop free routes.
- EIGRP labels best pathway to a given network as the successor.
- If AD of a non-successor route is less than the FD of the best route, that route is labeled as the Feasible successor and can be used immediately if the pathway via successor is unavailable.

OSPF	EIGRP
Open Standard	Partially Open Standard.
Link State Routing Protocol.	Advanced Distance Vector Protocol.
Slow Convergence as it has to manually get the path again by recalculating.	Fast Convergence as it has the 2nd best path.
It works under hierarchy.	It is a flexible design.
Flood Queries are minimal due to area concept.	Flood Queries are more due to more flexible design.
OSPF supports 1 routed protocol ie IP.	EIGRP supports multi routed protocols like IP,IPX,SPX,etc.
OSPF supports only equal load balancing.	EIGRP supports both equal and unequal load balancing.
OSPF use multicast address 224.0.0.5 goes for all ospf routers and 224.0.0.6 goes for all DR and BDR	Eigrp use multicast address 224.0.0.10
Administrative Distance is 110.	Administrative Distance is 90.

Classful Routing Protocol	**Classless Routing Protocol**
RIP, IGRP	RIPv2, EIGRP,OSPF, IS-IS, BGPv4
Does not send subnet mask in route advertisement.	Sends subnet mask in route advertisement.
It has only classful addressing.	It supports all kinds of addressing like FLSM, VLSM.
It supports auto-summarization only.	It supports auto and manual summarization.
Does not support discontiguous networks.	Supports both contiguous and discontiguous network.
/8 , /16 , /24	Supports all.

Recursive Lookup

- Recursive lookup refers to routes for which the second routing lookup is required in order to resolve the exit path for traffic going to this destination. Mostly, this generally refers to routes that define only the next hop address (that's a non directly connected subnet) without a specified exit interface.
- It is done to check the outgoing routes.

-The bottom line is that a next-hop doesn't need to be directly connected; the next-hop is just an IP address part of a specific network. Therefore, the router must be able to reach this network – either through a directly connected interface, or through a recursive lookup. Should the next-hop not be reachable, the route is declared invalid!
- If R1 is the router, it would check the route for network first and then for the hop again.

- **Here we got a very simple routing table:**

```
172.16.0.0/24 is subnetted, 2 subnets
C 172.16.1.0 [1/0] via 172.16.2.2
C 172.16.2.0 is directly connected, Serial0/0/0
S 192.168.2.0/24 [1/0]  via 172.16.2.2
S 192.168.3.0/24 [1/0]  via 172.16.2.2
```

Now, when a packet arrives with destination IP let's say 192.168.2.69, router will find out that a suitable route for such packet is static route 192.168.2.0/24 with the next hop IP address 172.16.2.2

This next hop IP address 172.16.2.2 is then found as directly connected through exit interface Serial0/0/0.

As stated in Cisco curriculum:

Every route that references only a next-hop IP address and does not reference an exit interface must have the next-hop IP address resolved using another route in the routing table that has an exit interface.

So this process is called recursive lookup - when a route table entry references to another IP address and not to a directly connected exit interface. Therefore another lookup has to be made. There can be more lookups, until the route with exit interface specified is found - so that's why it's called recursive.

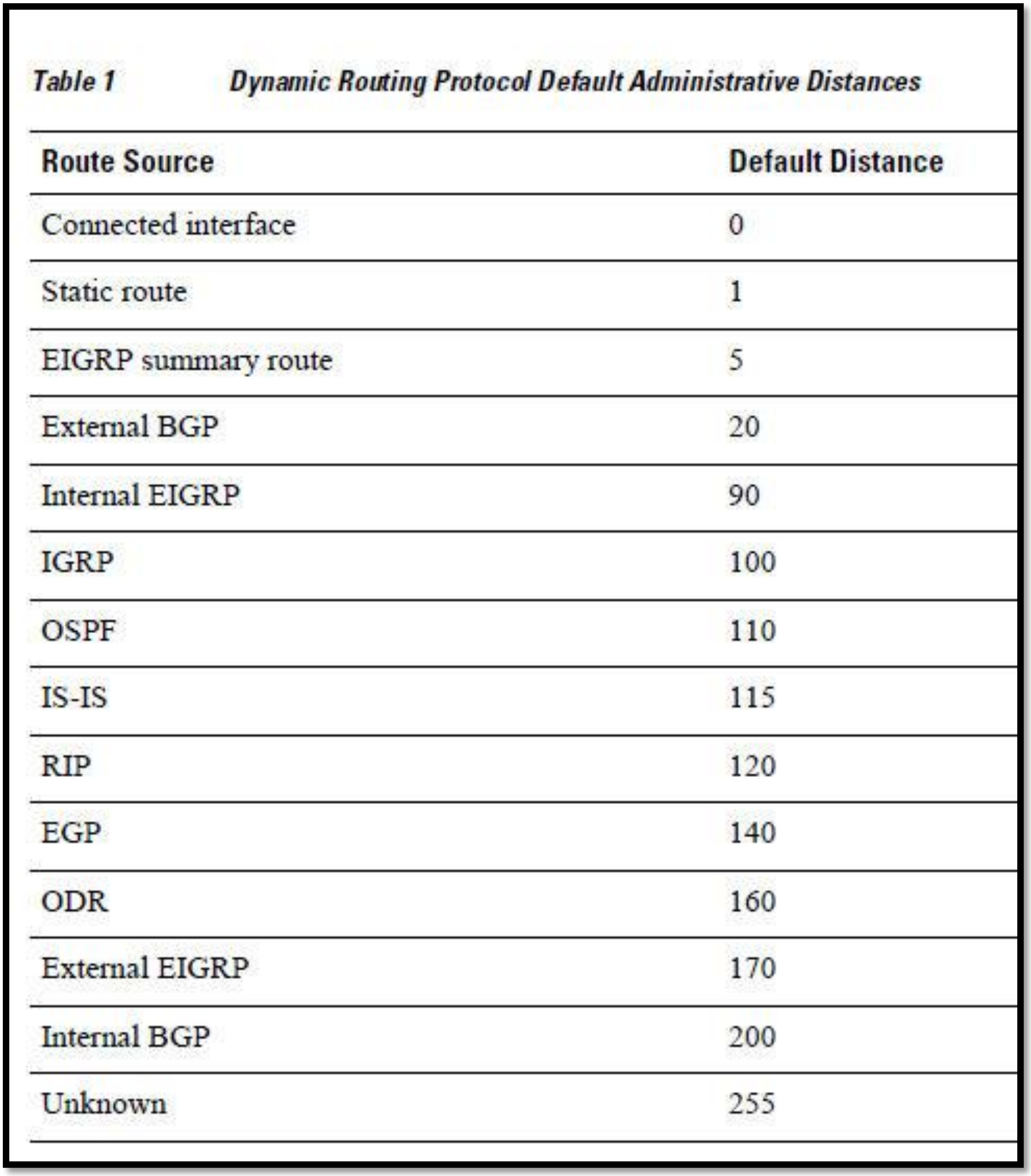


Table 1 *Dynamic Routing Protocol Default Administrative Distances*

Route Source	Default Distance
Connected interface	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
ODR	160
External EIGRP	170
Internal BGP	200
Unknown	255

Administrative Distance:

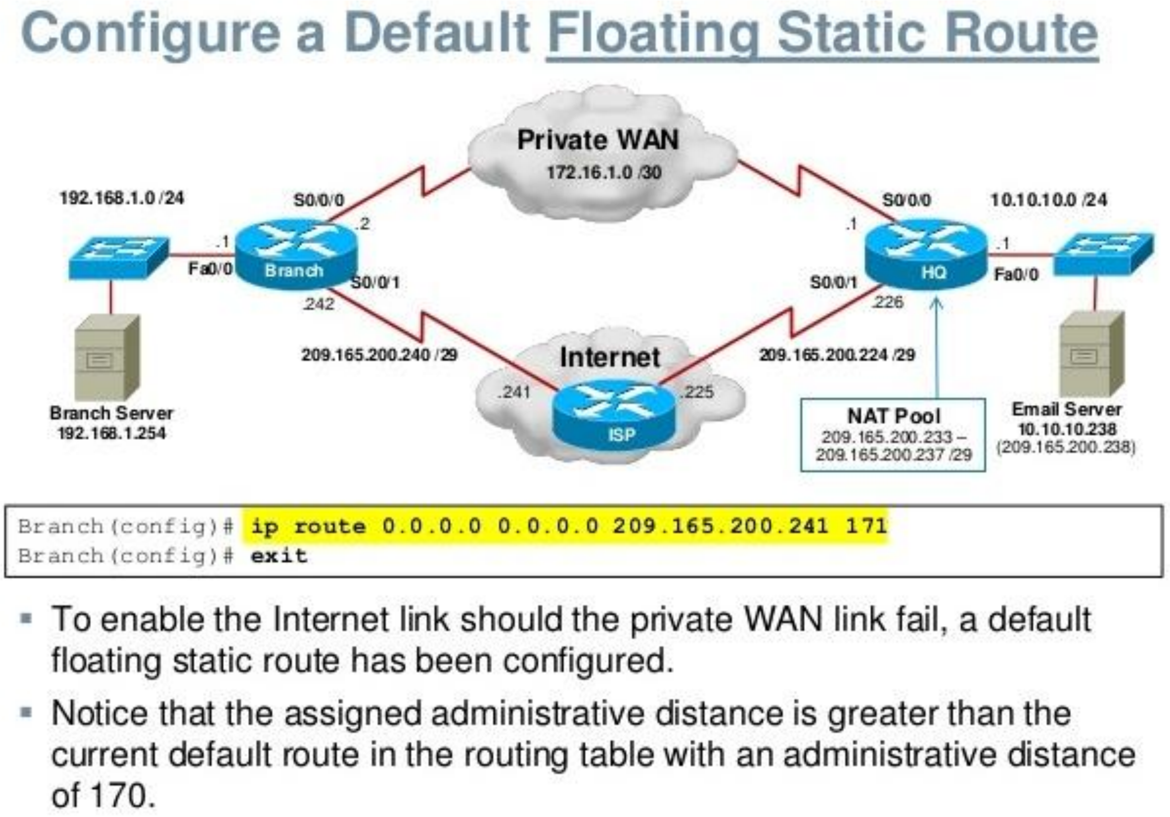
Administrative distance is the feature that routers use in order to select the best path when there are two or more different routes to the same destination from two different routing protocols.

Administrative distance defines the reliability of a routing protocol.

Floating Static Routes:

A Floating Static Route is a static route which an Administrative Distance is higher than that of the routing protocol is currently in use.

In this way the Floating Static Route will only appear in the routing table if the Dynamically learned route is Lost.



Configure a Default Floating Static Route

```
Branch(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.241 171
Branch(config)# exit
```

- To enable the Internet link should the private WAN link fail, a default floating static route has been configured.
- Notice that the assigned administrative distance is greater than the current default route in the routing table with an administrative distance of 170.

Contiguous Network:

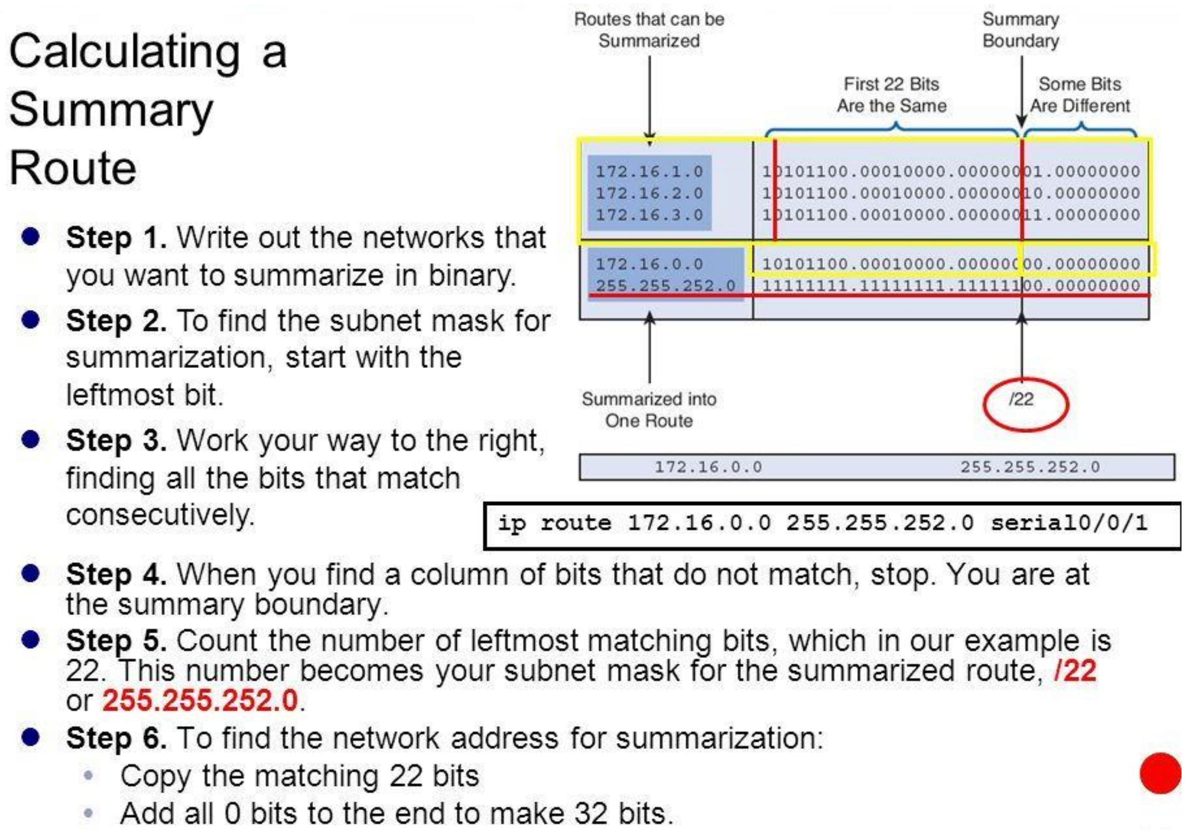
A network is contiguous if you can get from every part of that network to every other part of that network without going outside of the network.

Discontiguous Network:

A network is Discontiguous if going from one part of the network to some other part of the network you must go through some different network.

Route Summarization (route aggregation):

Route summarization, also called route aggregation, is a method of minimizing the number of routing tables in an IP (Internet Protocol) network. It works by consolidating selected multiple routes into a single route advertisement.



Calculating a Summary Route

Routes that can be Summarized
Summary Boundary
First 22 Bits Are the Same
Some Bits Are Different
Summarized into One Route
/22

```
172.16.1.0     10101100.00010000.00000001.00000000
172.16.2.0     10101100.00010000.00000010.00000000
172.16.3.0     10101100.00010000.00000011.00000000

172.16.0.0     10101100.00010000.00000000.00000000
255.255.252.0  11111111.11111111.11111100.00000000

172.16.0.0                 255.255.252.0
```

```
ip route 172.16.0.0 255.255.252.0 serial0/0/1
```

- **Step 1.** Write out the networks that you want to summarize in binary.
- **Step 2.** To find the subnet mask for summarization, start with the leftmost bit.
- **Step 3.** Work your way to the right, finding all the bits that match consecutively.
- **Step 4.** When you find a column of bits that do not match, stop. You are at the summary boundary.
- **Step 5.** Count the number of leftmost matching bits, which in our example is 22. This number becomes your subnet mask for the summarized route, **/22** or **255.255.252.0**.
- **Step 6.** To find the network address for summarization:
  - Copy the matching 22 bits
  - Add all 0 bits to the end to make 32 bits.

SWITCHING

1.Virtual LAN (VLAN).
2.Trunking.
3.VLAN trunking Protocol (V.T.P).
4.Inter- VLAN’s.
5.Spanning Tree Protocol (S.T.P).
6.Etherchannel.
7.First Hop Redundancy Protocol (F.H.R.P).
8.Layer 2 Security.

Virtual LAN (VLAN).

We create VLAN's to break up large Layer 3 Broad cast Domain.

1. By-default VLAN's Database is Stored in Flash –Memory, With File name VLAN.dat
2. By-default VLAN1 is created , and all the ports are in VLAN1.
3. VLAN,s Range

1 to 1001	-	Normal Range
1002 to 1005	-	Reserved VLAN,s (not useable)
1006 to 4096	-	Extended VLAN's

Command to create a VLAN's.

```
# en
#conf  t
#show vlan ( to view vlan database)
#name Sales ( give what ever you want)
#exit
```

How to Assign a port in VLAN.

```
#int fa 0/5 (interface number which you want to assign into a vlan)
#switchport mode access
#switchport access vlan 2 ( 2 is the Vlan number)
```

```
#int fa 0/11 (interface number which you want to assign into a vlan)
#switchport mode access
#switchport access vlan 3 ( 3 is the Vlan number)
```

Old way to create a VLAN,s

Directly on enable mode.

```
#vlan database.
#vlan 4 name IT
#exit
```

How to Assign multiple port’s in VLAN.

```
#int range fa0/1-10, fa0/16, fa0/19
#switchport mode access
#switchport access vlan 2 ( 2 is the Vlan number)
```

Trunking.

Trunks are used to inter-connect Switches to form network.

There are two types of switchports.

1. Access Mode - Single VLAN traffic

A access port is typically for a switch to host connection and this port is assigned to only one VLAN.

This can be done with the following commands :

```
# interface fastethernet [interface number]
# switchport mode access
# switchport access vlan [vlan number]
```

2. Trunk Mode -Multiple VLAN traffic

A trunk is typically a link between two switches or a switch and a router. This allows multiple VLAN's to traverse the interface/link. This can be configured in a few different ways but will achieve the same result.

```
# interface fasterthernet [interface number]
# switchport mode Trunk
```

Now, there are 2 types of Trunk Mode.

I- Dynamic. (By default)
II- Static.

Dynamic Trunking .

Dynamic Desirable : The 'dynamic desirable' will configure the port to try and become a trunk link by sending a request to the other end of the wire requesting to become a trunk port.

Dynamic Auto : The 'dynamic auto' will configure the port to accept incoming negotiation and will accept becoming either a trunk or an access port.

No negotiate : Prevents the interface from generating DTP frames.

Dynamic Desirable	**(trunk will form)**	Dynamic Desirable
Dynamic Desirable	**(trunk will form)**	Dynamic Auto
Dynamic Desirable	**(trunk will form)**	Static Trunk
Dynamic Auto	**(trunk will not form)**	Dynamic Auto
Dynamic Auto	**(trunk will form)**	Static Trunnk

For viewing Switchport Mode :

```
#Show int [interface number] switchport
```

Few Useful commands :

#switchport mode access – This command puts the interface (access port) into permanent nontrunking mode. The interface will generate DTP frames, negotiating with the neighboring interface to convert the link into a nontrunk link. The interface becomes a nontrunk interface even if the neighboring interface does not agree to the change.

#switchport mode dynamic desirable – This command makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode. This is the default mode for all Ethernet interfaces. If the neighboring interface is set to the access or non-negotiate mode, the link will become a non-trunking link.

#switchport mode dynamic auto – This command makes the interface willing to convert the link to a trunk link if the neighboring interface is set to trunk or desirable mode. Otherwise, the link will become a non-trunking link.

#switchport mode trunk – This command puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighboring interface does not agree to the change.

#switchport nonegotiate – Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is access or trunk. You must manually configure the neighboring interface as a trunk interface to establish a trunk link, otherwise the link will be a non-trunking link.

Trunk Encapsulation.

- Dot1q or 802.1q (I.E.E.E Standard)
- Open Standard
- Native Lan (By default 1)
- Simplier header

The default encapsulation method is **Inter Switch link (ISL)** which is **CISCO Proprietry**. You can change from the default with the **switchport trunk encapsulation** command. For COS switches or integrated IOS switches, the default encapsulation is **negotiate**. This method signals between the trunked ports to choose an encapsulation method.

(ISL is preferred over 802.1Q.) The **negotiate** option is valid for **auto** or **desirable** trunking modes only. If you choose "**on**" as the mode or if you want to force a particular method or if the other side of the trunk cannot negotiate the trunking type, you must choose the option **ISL** or **dot1Q** to specify the encapsulation method.

NOTE : Not all switches allow you to negotiate a trunk encapsulation setting. The 2900XL and 3500XL trunks default to **ISL** and you must use the**switchport trunk encapsulation** command to change the encapsulation type. The 2950 and some 4000 switches support only 802.1Q trunking and provide no options for changing the trunk type.

For Configuration Static Trunk encapsulation :

```
#interface [ interface number]
#switchport trunk encapsulation dot1q
#switchport mode trunk
```

On another switch :

```
#interface [ interface number]
#switchport mode trunk
```

Here are some Cisco IOS switchport configurations translated into English:

switchport mode trunk says: “Always trunk on this end, and I will send DTP to attempt to negotiate a trunk on the other end.”

switchport nonegotiate says: “Do not send or respond to DTP from this end. Disable all DTP on this port.” (Best used on user access ports, when trunking to non-Cisco switches, when trunking to a router[1], or if you are paranoid about fast convergence.

switchport mode dynamic desirable says: “Ask the other end to trunk using DTP and trunk if the negotiation succeeds. If DTP negotiation fails then become an access port.”

switchport mode dynamic auto says: “If the other end asks me to be a trunk with DTP, then become a trunk, but I wont initiate any negotitation from this end. If no one asks me to become a trunk then I will become an access port.”

switchport mode access says: “Never trunk on this end, and I will send out DTP to help my link partner reach the same conclusion.”

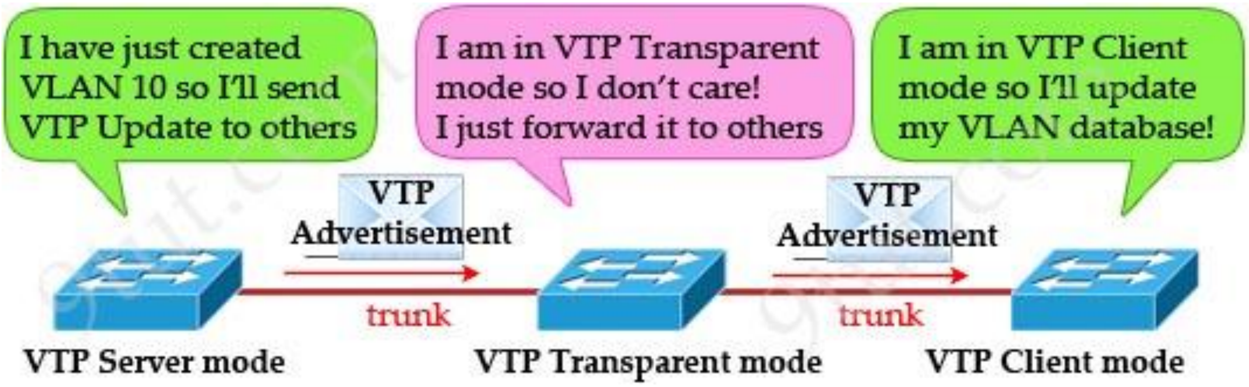
switchport trunk encapsulation says: “Do not negotiate the trunk protocol with DTP. Only use the trunk protocol specified in this command (isl or dot1q).

VLAN trunking Protocol (V.T.P)

VLAN Trunk Protocol (VTP) reduces administration in a switched network. When you configure a new VLAN on one 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 series products.

There are 3 Modes in V.T.P:


I have just created VLAN 10 so I'll send VTP Update to others
I am in VTP Transparent mode so I don't care! I just forward it to others
I am in VTP Client mode so I'll update my VLAN database!
VTP Advertisement
VTP Advertisement
trunk
trunk
VTP Server mode
VTP Transparent mode
VTP Client mode

1. **Server Mode :**

   By-default all the switches are in server mode. We can Create , Delete, or Modify vlan's.

   Vlan database of VTP server is forwarded to it's Trunk port.

2. **Client Mode :**

   If we Change a switch into client mode we cannot Create , Delete, or Modify vlan's.

   It just to get the vlan information (vlan database from server) so it's copy it to own vlan database & forward to it's Trunk port.

3. **Transparent Mode :**
   If we change a switch into VTP transparent mode it will not keep trhe vlan information (vlan database) sent by the VTP server, but just forward it to its trunk ports.

   NOTE : VTP transparent mode can have it's own VLAN database which means we can Create, Delete, Modify Vlan's but it will not be Propagated to other switches on Domain.

NOTE: For Configuration V.T.P All switches have the same the VTP domain name and same VTP password.

Below commands will Propagate all vlan database from switch 1 to switch 2.

Switch 1:

```
#vtp mode server
#vtp domain india (set whatever you want)
#vtp password 123 (set whatever you want)
```

Switch 2:

```
#vtp mode client
#vtp domain india
#vtp password 123
```

Now we can assign a port's in switch 2 vlan's.

Inter-VLAN's.

InterVLAN is a method to enable communication between two different VLANs connected in a network device like network switch or a router.

- You need a Router, Layer 3 switch or any other layer 3 devices to enable it.
- The VLANs must be in different network.
- Between the layer 2 and layer 3 device the link should be in trunking state.

Normally it required layer 3 switch or router.it is essential in the big networks and big companies. In big network we can see lot of vlan if you want to communicate different vlans we are using
Example
Vlan : Sales
Vlan : Marketing
If you want to communicate the sales vlan to marketing vlan in network you have to configure the intervlan routing.

For Example : The router is connected to the switch using a single interface. The switchport connecting to the router is configured as a trunk link. The single interface on the router is then configured with multiple IP addresses that correspond to the VLANs on the switch. This interface accepts traffic from all the VLANs and determines the destination network based on the source and destination IP in the packets. It then forwards the data to the switch with the correct VLAN information.

In this type of inter-VLAN routing, the interface connecting the router to the switch is usually a trunk link. The router accepts traffic that is tagged from the VLANs on the switch through the trunk link. On the router, the physical interface is divided into smaller interfaces called subinterfaces. When the router receives the tagged traffic, it forwards the traffic out to the subinterface that has the destination IP address.

sub interfaces aren’t real interfaces but they use the LAN physical interfaces on the router to forward data to various VLANs. Each sub interface is configured with an IP address and assigned a VLAN based on the design.

Now inter-VLAN routing can be configured on the router, when configuring router, we use sub interfaces.

(Older way router-on-a-stick or Using router if we don’t have Layer 3 Switch.)

On Router:

Each subinterface is created using the interface *interface_number.Subinterface_number* in the global configuration mode..

R1(config)#interface <interface_number.Subinterface_number>

NOTE: the between the interface ID and the sub interface ID is a must. The sub interface ID is a logical number but ideally it should describe the VLAN ID.

To create a sub interface which will be used to route for VLAN 2, we will use the command shown below.

R1(config)#interface fastethernet 0/0.2

This will take us into the subinterface configuration mode which is denoted by the prompt shown below.

R1(config-subif)#

In the sub interface mode, we can link the VLAN ID to this interface as well as assign it an ip address and a subnet mask.To link the sub interface with the specific VLAN, we use the command “**encapsulation dot1q <VLAN_Number>**” this will specify that this interface will get traffic from the specified VLAN. In our example, the command needed to link VLAN 2 to this subinterface

R1(config-subif)#encapsulation dot1q 2

In this mode, we can also assign the sub interface with the ip address and subnet mask which will be used for VLAN 2. The default gateway on the PC’s will be used as the interface address as shown below.

R1(config-subif)#ip address 10.0.0.1 255.0.0.0

When all the subinterfaces have been assigned to their respective VLANs, we need to activate the LAN interfaces that they are connected to by issuing the no shutdown command.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#no shutdown
```

On Switch :

```
sw1(config)#interface fastethernet 0/1
sw1(config-if)#switchport trunk encapsulation dot1q
sw1(config-if)#switchport mode trunk
```

This will activate the interface and allow for inter-VLAN routing.

In our scenario, the above commands needed to configure inter-VLAN routing using router-on-a-stick are shown below.

Router1 :

```
R1(config)#interface fastethernet 0/0.2
R1(config-subif)#encapsulation dot1q 2
R1(config-subif)#ip address 10.0.0.1 255.0.0.0
#
R1(config)#interface fastethernet 0/0.3
R1(config-subif)#encapsulation dot1q 2
R1(config-subif)#ip address 20.0.0.1 255.0.0.0
#
R1(config)#interface fastethernet 0/0
R1(config-if)no shutdown
```

Switch1 :

```
sw1(config)#interface fastethernet 0/1
sw1(config-if)#switchport trunk encapsulation dot1q
sw1(config-if)#switchport mode trunk
```

Configuration of inter-VLAN’s with Multi-Layer, L3 Switch.

On Switch:

```
#interface vlan 2
#ip add 10.0.0.1 225.0.0.0
#no shutdown
```

```
#interface vlan 3
#ip add 20.0.0.1 255.0.0.0
#no shutdown
```

NOTE: By-default routing on switches in disabled for enabling routing on switches command is:

```
#ip routing
```

Spanning Tree Protocol (S.T.P)

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network.

- To avoid bridging loops.
- Elect a Root Bridge, with the help of Bridge Id. Lowest bridge ID become root bridge.

Root Bridge: The Root bridge (switch) is a special bridge at the top of the Spanning Tree (inverted tree). The branches (Ethernet connections) are then branched out from the root switch, connecting to other switches in the Local Area Network.

Bridge ID:

Every switch has an identity when they are part of a network. This identity is called the **Bridge ID** or **BID**. It is divided into two parts. The first part is **Bridge Priority** field (which can be configured) while the second part is **MAC address** of the switch.

Priority	**System ID**
Range 0 - 65,535	MAC Address
Default-32,768	

Spanning Tree Ports:

Root Ports: is elected on the Non Root Bridge trying to go towards the root Bridge.

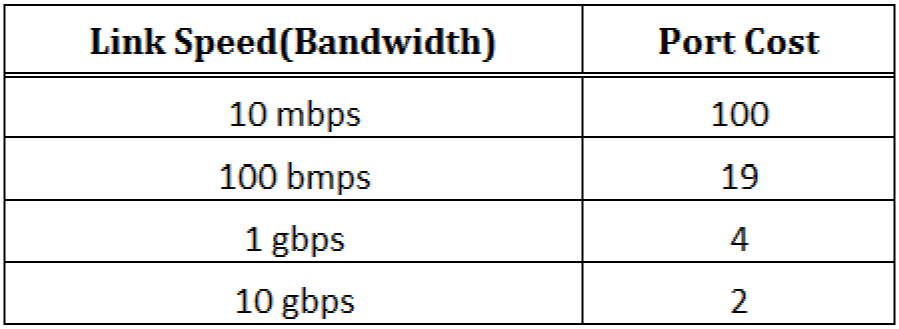
1- Lowest Spanning Tree cost towards the root bridge.
2- Lowest Bridge ID of the Uplink Non-Root Bridge Switch.
3- Lowest port Priority of the up-link switch (By-default 128).
4- Lowest Hardware ID (physical port of the switch)

Designated Port: Is elected opposite root port & Block port which means Root Bridge is trying to come towards the non- root bridges.

1- Lowest Spanningt tree Cost.
2- Lowest Bridge ID.

Blocking Port : is to block extra Links, to avoid looping, it calculated coming from root bridge towards the non root bridge.

1- Highest spanning tree cost.
2- Highest Bridge ID of the Non-Root Bridge.



Link Speed(Bandwidth)	Port Cost
10 mbps	100
100 bmps	19
1 gbps	4
10 gbps	2

Spanning-tree States:

Ports on switch running STP go through the five different states. During STP convergence, switches will move their root and designated ports through the various states: blocking, listening, learning, and forwarding, whereas any other ports will remain in a blocked state.

1- Blocking state
2- Listening state
3- Learning state
4- Forwarding state

Convergence is a state where all ports on switch have transitioned to either forwarding or blocking modes. During the STP converging, all user data frames would be dropped. No user data frame will be forwarded until convergence is complete. Usually convergence takes place in 30 seconds (15 seconds of listing state + 15 seconds of learning state).

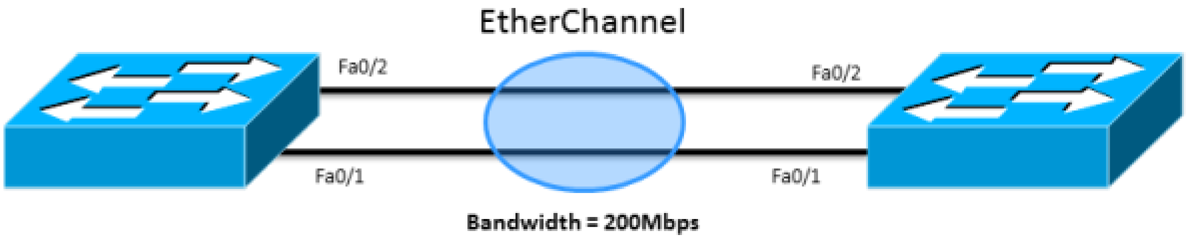
For fast convergence & only for connect a PC not for switch we can use the below mentioned command :

#interface fa[interface number]
#spanning-tree port fast.

If we connect Switch on that port for which we have given the command of Port-fast chances are that this port is go in the loop.

Etherchannel.

EtherChannel is a port link aggregation technology or port-channel architecture used primarily on Cisco switches. It allows grouping of several physical Ethernet links to create one logical Ethernet link for the purpose of providing fault-tolerance and high-speed links between switches, routers and servers.



We need to create port channel with the help of negotiating protocols of EtherChannel.

There are two protocols used for negotiating EtherChannel and Link Aggregation.

1- Port Aggregation Protocol (PAgP) - Cisco Proprietary protocol

Port Aggregation Protocol (PAgP) has two Channel modes and they are "Desirable" and "Auto".

Auto Mode: Auto mode in Port Aggregation Protocol (PAgP) does not initiate the negotiation, but responds to Port Aggregation Protocol (PAgP) packets initiated by other end

Desirable mode: Desirable mode in Port Aggregation Protocol (PAgP) initiates the negotiation and tries to form EtherChannel with other end.

2- Link Aggregation Control Protocol (LACP) – IEEE- Open Standard

Link Aggregation Control Protocol (LACP) has two Channel modes and they are "Active" and "Passive"

Active Mode: Active Mode in Link Aggregation Control Protocol (LACP) initiates the negotiation and tries to form EtherChannel with other end.

Passive Mode: Passive Mode in Link Aggregation Control Protocol (LACP) does not initiate the negotiation, but responds to Link Aggregation Control Protocol (LACP) packets initiated by other end.

3- EtherChannel "on" mode

EtherChannel "on" mode makes the interface into an EtherChannel without any negotiation protocols like PAgP or LACP. When using a EtherChannel "on" mode, EtherChannel will be created only when another interface group in EtherChannel "on" mode.

Switch interfaces exchange PAgP packets only with partner interfaces configured in the auto or desirable modes. Switch interfaces exchangeLACP packets only with partner interfaces configured in the active or passive modes.

Interfaces configured in the "on" Channel mode do not exchange Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP).

For Configuration EtherChannel Command we use :

On Switch 1:

```
#intrerface range fa[first interface number-second interface number]
#channel-protocl pagp
#channel-group 1 mode desirable
```

On Switch 2:

```
#intrerface range fa[first interface number-second interface number]
#channel-protocl pagp
#channel-group 1 mode desirable
```

For Channel Group listing Command we use:

```
#Show etherchannel
```

For Port & EtherChannel Details Command we use:

```
#show ethrchannel summary
```

First Hop Redundancy Protocol (F.H.R.P)

A **first hop redundancy protocol (FHRP)** is a computer networking protocol which is designed to protect the Default Gateway used on a Subnetwork by allowing two or more routers to provide backup for that address; in the event of failure of an active router, the backup router will take over the address, usually within a few seconds. In practice, such protocols can also be used to protect other services operating on a single IP address, not just routers.

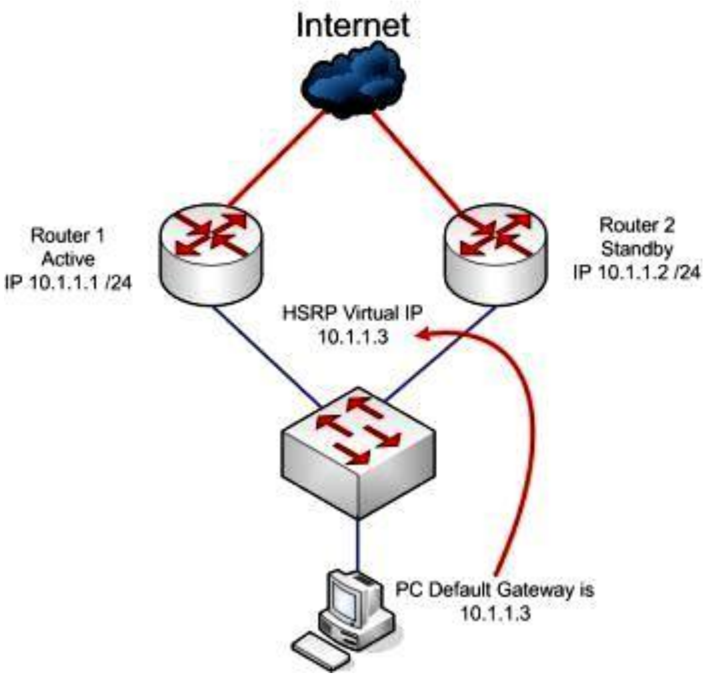
- **Hot Standby Router Protocol (HSRP)**
- **Virtual Router Redundancy Protocol (VRRP)**
- **Gateway Load Balancing Protocol (GLBP)**

Hot Standby Router Protocol (HSRP)

In computer networking, the **Hot Standby Routing Protocol** (**HSRP**) is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway.

1- Cisco proprietry
2- Standby Group
3- Active/Standby
4- Virtual IP / Virtual MAC address
5- Highest priority become active(By-default it is 100)
6- Non-PremDe by default (preempt is disabled)
7- Hello sends on each 3 seconds and hold on timer is 10 Sec.
8- It can be track other interfaces. If the tracking interface goes down it will decrease the priority with the given valu.(by value is 10)
9- By- default no load Balancing Supported

For Example:



Router 1:

```
#router ospf 10
#network 20.0.0.0 0.255.255.255 area 0
#redistribute connected subnets
```

Router 2:

```
#router ospf 10
#network 30.0.0.0 0.255.255.255 area 0
#redistribute connected subnets
```

Router 3 Suppose as Internet:

```
#network ospf 10
#network 3.3.3.3 255.255.255.255 area 0
#network 20.0.0.0 0.255.255.255 area 0
#network 30.0.0.0 0.255.255.255 area 0
```

For Enabling H.S.R.P: (On each router):

```
#interface fa0/0
#standby 1 ip 10.1.1.3
```

For Changes made in priority and enabling Preempt:

```
#int f 0/0
#standby 1 priority 101
#standby 1 preempt
```

For Track other Interfaces in H.S.R.P:

```
#standby 1 track s0/0
```

Virtual Router Redundancy Protocol (VRRP)

The Virtual Router Redundancy Protocol (**VRRP**) is a computer networking protocol that provides for automatic assignment of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP sub-network.

1- Open standard
2- V.R.R.P Group
3- Master/ Backup
4- Priority by default 100,Higher priority become MASTER
5- Preempt is enabled by default
6- Hello timer is 1 Sec. and Hold on Timer is 3 Sec.
7- It can track other Interfaces same as H.S.R.P(Config. Is little different)
8- By default no load balancing

Gateway Load Balancing Protocol (GLBP)

Gateway Load Balancing Protocol (**GLBP**) is a Cisco proprietary protocol that attempts to overcome the limitations of existing redundant router protocols by adding basic load balancing functionality. In addition to being able to set priorities on different gateway routers, **GLBP** allows a weighting parameter to be set.

1- Cisco Proprietry
2- G.L.B.P Group
3- Active Virtual Gateway (AVG) & Active Virtual Forward (AVF)
4- Priority is by-default 100,Higher Priority become Active Virtual Gateway
5- Preempt is disabled by default
6- Hello Timer is 3 Sec. & Hold on Timer 10 sec.
7- It can also track other Interface same as H.S.R.P
8- By-Default it can do load balancing.

Types of Load Balancing:

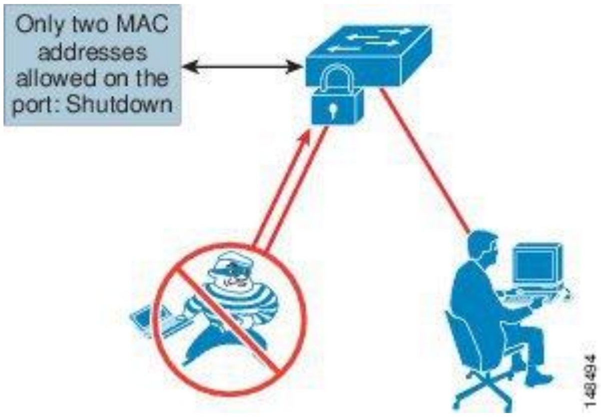
Round Robin: With Round Robin each MAC address is used sequentially in ARP replies for the virtual IP address. Round Robin load balancing is suitable for any number of end hosts.

Weighted: This is the ability GLBP to place a weight on each device when calculating the amount of load sharing that will occur through MAC assignment.

Host Dependent: The MAC address of a host is used to determine which MAC address the host is directed towards. This ensures that a host will be guaranteed to use the same virtual MAC address

Layer 2 Security (Port Security).

Without security protections in place, unauthorized devices could access your network through open and unprotected switch interfaces. The Port Security feature is used to restrict traffic on a switch interface (also called a"switchport") by identifying and limiting traffic allowed to enter that port based on source Ethernet MAC addresses.



1- Limit the Number of MAC address on a particular port (MAX is 1)

2- We can also Binding a MAC address also with the following methods :

- Static: MAC addresses added manually into the switch configuration, and
- Sticky: MAC addresses learned during switch operation and added automatically into the switch configuration.

3- Security Violations :

If a violation should occur, the switch will respond according to one of three modes:

- Shutdown : It will Shutdown the port & sends it to error-disable state & also sends log.
- Protect : It will not Shutdown the port but will not allow the traffic. Does not sends log.
- Restrict : It will not Shutdown the port but will not allow the traffic & sends log.

.

Configuration Commands for port Security:

```
Switch(config)#interface interface[interface number]
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1[1 is learned MAC entry]
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#end
```

Few Useful Commands :

We can view the default port security configuration with:

1- Switch(config)#show port security

2- Switch(config)#show port security interface[interface number]

3- Switch(config)#sh interface [interface number]

ACCESS CONTROL LIST (ACL)

Cisco provides basic traffic filtering capabilities with access control lists (also referred to as access lists). Access lists can be configured for all routed network protocols (IP, AppleTalk, and so on) to filter the packets of those protocols as the packets pass through a router.

You can configure access lists at your router to control access to a network: access lists can prevent certain traffic from entering or exiting a network.

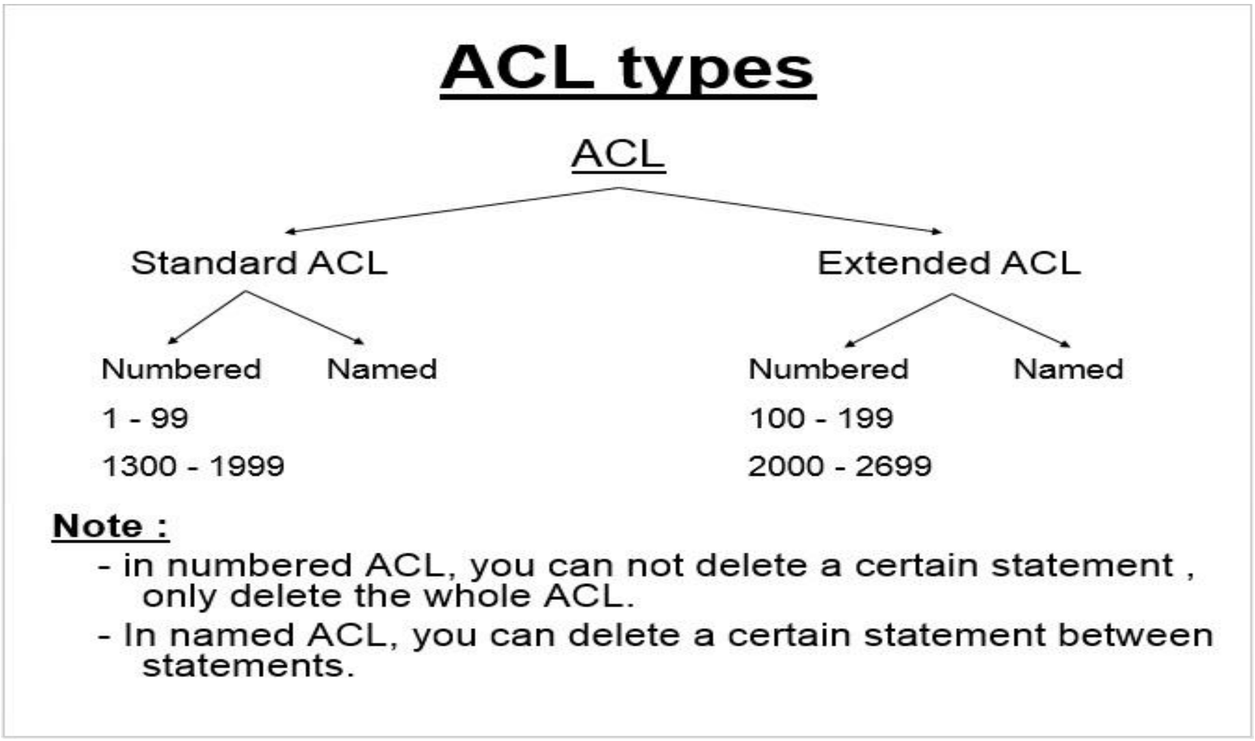
ACLs are basically a set of commands, grouped together by a number or name that is used to filter traffic entering or leaving an interface.

There are two types of Access Control Lists:

1. Standard Access Control list.
2. Extended Access Control List.

We can configure both the Access Control List with two ways:

1. Numbered ACL.
2. Named ACL.



ACL types

Note :

- in numbered ACL, you can not delete a certain statement , only delete the whole ACL.
- In named ACL, you can delete a certain statement between statements.

1. Standard Access Control List:

A standard IP ACL is simple; it filters based on source address only. You can filter a source network or a source host, but you cannot filter based on the destination of a packet, the particular protocol being used such as the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP), or on the port number. You can permit or deny only source traffic.

- If we configured Numbered Access list the range is 1 to 99 of standard ACL.
- On standard access list you cannot define destination IP Address, Port or Services & Protocols.
- You must configured Standard ACL Closest to the destination.

2. Extended Access Control List:

An extended ACL gives you much more power than just a standard ACL. Extended IP ACLs check both the source and destination packet addresses. They can also check for specific protocols, port numbers, and other parameters, which allow administrators more flexibility and control.

- If we configured Numbered Access list the range is 100 to 199 of Extended ACL.
- On Extended access list you can define destination IP Address, Port or Services & Protocols.
- You must configure Extended ACL Closest to the source.

When activating an ACL on an interface, you must specify in which direction the traffic should be filtered:

- **Inbound (as the traffic comes into an interface)**
- **Outbound (before the traffic exits an interface)**

Inbound ACLs:

Incoming packets are processed before they are routed to an outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups if the packet will be discarded after it is denied by the filtering tests. If the packet is permitted by the tests, it is processed for routing.

Outbound ACLs:

Incoming packets are routed to the outbound interface and then processed through the outbound ACL.

Universal fact about Access control list:

- ACLs come in two varieties: **Numbered and named**
- Each of these references to ACLs supports two types of filtering: **standard and extended.**
- Standard IP ACLs can filter only on the **source IP address** inside a packet.
- Whereas an extended IP ACLs can filter on the **source and destination IP addresses** in the packet.
- There are two actions an ACL can take: **permit or deny.**
- Statements are processed top-down.
- Once a match is found, no further statements are processed—therefore, order is important.
- If no match is found, the imaginary **implicit deny statement at the end of the ACL** drops the packet.
- An ACL should have at least one permit statement; otherwise, all traffic will be dropped because of the hidden implicit deny statement at the end of every ACL.

No matter what type of ACL you use, though, you can have only one ACL per protocol, per interface, per direction. For example, you can have one IP ACL inbound on an interface and another IP ACL outbound on an interface, but you cannot have two inbound IP ACLs on the same interface.

Configuration Guidelines

- Order of statements is important: put the most restrictive statements at the top of the list and the least restrictive at the bottom.
- ACL statements are **processed top-down until a match is found,** and then no more statements in the list are processed.
- If no match is found in the ACL, the packet is dropped (implicit deny).
- Each ACL needs either a unique number or a unique name.
- The router cannot filter traffic that it, itself, originates.
- You can have only one IP ACL applied to an interface in each direction (inbound and outbound)—you can't have two or more inbound or outbound ACLs applied to the same interface. (Actually, you can have one ACL for each protocol, like IP and IPX, applied to an interface in each direction.)
- Applying an empty ACL to an interface permits all traffic by default: in order for an ACL to have an implicit deny statement, you need at least one actual permit or deny statement.
- Remember the numbers you can use for IP ACLs.Standard ACLs can use numbers ranging **1–99 and 1300–1999,** and extended ACLs can use **100–199 and 2000–2699.**
- Wildcard mask is not a subnet mask. Like an IP address or a subnet mask, a wildcard mask is composed of 32 bits when doing the conversion; subtract each byte in the subnet mask from 255.

Creating a Named Standard Access List to Filter on Source Address

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list standard** name
4. **deny** {source [source-wildcard] | **any**
5. **permit** {source [source-wildcard] | **any**
6. Repeat some combination of Steps 4 through 7 until you have specified the sources on which you want to base your access list.
7. **end**
8. **show ip access-list**

DETAILED STEPS:

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**ip access-list standard** name **Example:** Device(config)# ip access-list standard R&D	Defines a standard IP access list using a name and enters standard named access list configuration mode.

Step 4	**deny** {source [source-wildcard] | **any** **Example:** Device(config-std-nacl)# deny 172.16.0.0 0.0.255.255 log	(Optional) Denies the specified source based on a source address and wildcard mask. If the source-wildcard is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. Optionally use the keyword **any** as a substitute for the source source-wildcard to specify the source and source wildcard of 0.0.0.0 255.255.255.255. In this example, all hosts on network 172.16.0.0 are denied passing the access list.
Step 5	**permit** {source [source-wildcard] | **any** **Example:** Device(config-std-nacl)# permit 172.18.5.22 0.0.0.0	Permits the specified source based on a source address and wildcard mask. Every access list needs at least one**permit** statement; it need not be the first entry. If the source-wildcard is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. Optionally use the keyword **any** as a substitute for the source source-wildcard to specify the source and source wildcard of 0.0.0.0 255.255.255.255. In this example, host 172.18.5.22 is allowed to pass the access list.
Step 6	Repeat some combination of Steps 4 through 7 until you have specified the sources on which you want to base your access list.	Remember that all sources not specifically permitted are denied by an implicit **deny** statement at the end of the access list.

Step 7	**end** **Example:** Device(config-std-nacl)# end	Exits standard named access list configuration mode and enters privileged EXEC mode.
Step 8	**show ip access-list** **Example:** Device# show ip access-list	(Optional) Displays the contents of all current IP access lists.

Creating a Numbered Standard Access List to Filter on Source Address:

SUMMARY STEPS:

1. **enable**
2. **configure terminal**
3. **access-list** access-list-number permit {source [source-wildcard] **| any**
4. **access-list** access-list-number **deny** {source [source-wildcard] **| any**
5. Repeat some combination of Steps 3 through 6 until you have specified the sources on which you want to base your access list.
6. **end**
7. **show ip access-list**

DETAILED STEPS:

	Command or Action	**Purpose**
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**access-list** access-list-number permit {source [source-wildcard] | **any** **Example:** Device(config)# access-list 1 permit 172.16.5.22 0.0.0.0	Permits the specified source based on a source address and wildcard mask. Every access list needs at least one permit statement; it need not be the first entry. Standard IP access lists are numbered 1 to 99 or 1300 to 1999. If the source-wildcard is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. Optionally use the keyword any as a substitute for the source source-

		wildcard to specify the source and source wildcard of 0.0.0.0 255.255.255.255. In this example, host 172.16.5.22 is allowed to pass the access list.
Step 4	**access-list** access-list-number **deny** {source [source-wildcard] | **any** **Example:** Device(config)# access-list 1 deny 172.16.7.34 0.0.0.0	Denies the specified source based on a source address and wildcard mask. If the source-wildcard is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. Optionally use the abbreviation **any** as a substitute for the source source-wildcard to specify the source and source wildcard of 0.0.0.0 255.255.255.255. In this example, host 172.16.7.34 is denied passing the access list.
Step 5	Repeat some combination of Steps 3 through 6 until you have specified the sources on which you want to base your access list.	Remember that all sources not specifically permitted are denied by an implicit **deny** statement at the end of the access list.
Step 6	**end** **Example:** Device(config)# end	Exits global configuration mode and enters privileged EXEC mode.
Step 7	**show ip access-list** **Example:** Device# show ip access-list	(Optional) Displays the contents of all current IP access lists.

Creating a Named Extended Access List:

Create a named extended access list if you want to filter the source and destination address or filter a combination of addresses and other IP fields.

SUMMARY STEPS:

1. **enable**
2. **configure terminal**
3. **ip access-list extended** name
4. **deny** protocol source [source-wildcard] destination [destination-wildcard]
5. **permit** protocol source [source-wildcard] destination [destination-wildcard]
6. Repeat some combination of Steps 4 through 7 until you have specified the fields and values on which you want to base your access list.
7. **end**
8. **show ip access-list**

DETAILED STEPS:

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**ip access-list extended** name **Example:** Device(config)# ip access-list extended nacl	Defines an extended IP access list using a name and enters extended named access list configuration mode.

Step 4	**deny** protocol source [source-wildcard] destination [destination-wildcard] **Example:** Device(config-ext-nacl)# deny ip 172.18.0.0 0.0.255.255 host 172.16.40.10	(Optional) Denies any packet that matches all of the conditions specified in the statement. If the source-wildcard or destination-wildcard is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source or destination address, respectively. Optionally use the keyword **any** as a substitute for the source source-wildcard or destination destination-wildcardto specify the address and wildcard of 0.0.0.0 255.255.255.255. Optionally use the keyword **host** source to indicate a source and source wildcard of source0.0.0.0 or the abbreviation **host** destination to indicate a destination and destination wildcard of destination0.0.0.0. In this example, packets from all sources are denied access to the destination network 172.18.0.0.
Step 5	**permit** protocol source [source-wildcard] destination [destination-wildcard] **Example:** Device(config-ext-nacl)# permit tcp any any	Permits any packet that matches all of the conditions specified in the statement. Every access list needs at least one permit statement. If the source-wildcard or destination-wildcard is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source or destination address, respectively. Optionally use the keyword **any** as a substitute for the source source-wildcard or destination destination-wildcardto specify the address and wildcard of 0.0.0.0 255.255.255.255.

		In this example, TCP packets are allowed from any source to any destination. Use the **log-input** keyword to include input interface, source MAC address, or virtual circuit in the logging output.
Step 6	Repeat some combination of Steps 4 through 7 until you have specified the fields and values on which you want to base your access list.	Remember that all sources not specifically permitted are denied by an implicit **deny**statement at the end of the access list.
Step 7	**end** **Example:** Device(config-ext-nacl)# end	Exits standard named access list configuration mode and enters privileged EXEC mode.
Step 8	**show ip access-list** **Example:** Device# show ip access-list	(Optional) Displays the contents of all current IP access lists.

Creating a Numbered Extended Access List:

Create a numbered extended access list if you want to filter on source and destination address, or a combination of addresses and other IP fields, and you prefer not to use a name. Extended IP access lists are numbered 100 to 199 or 2000 to 2699.

SUMMARY STEPS:

1. **enable**
2. **configure terminal**
3. **access-list** access-list-number **permit** protocol {source [source-wildcard] **|** **any**} {destination [destination-wildcard] **|** **any**
4. **access-list** access-list-number **deny** protocol {source [source-wildcard] **|** **any**} {destination [destination-wildcard] **|** **any**
5. Repeat some combination of Steps 3 through 6 until you have specified the fields and values on which you want to base your access list.
6. **end**
7. **show ip access-list**

DETAILED STEPS:

	Command or Action	**Purpose**
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**access-list** access-list-number **permit** protocol {source [source-wildcard] **|** **any**} {destination [destination-wildcard] **|** **any**} **Example:** Device(config)# access-list 107 permit tcp any 172.69.0.0 0.0.255.255 eq telnet	Permits any packet that matches all of the conditions specified in the statement. Every access list needs at least one **permit**statement; it need not be the first entry. Extended IP access lists are numbered 100 to 199 or 2000 to 2699.

		If the source-wildcard or destination-wildcard is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source or destination address, respectively. Optionally use the keyword **any** as a substitute for the source source-wildcard or destination destination-wildcard to specify the address and wildcard of 0.0.0.0 255.255.255.255. TCP and other protocols have additional syntax available. See the **access-list** command in the command reference for complete syntax.
Step 4	**access-list** access-list-number **deny** protocol {source [source-wildcard] | **any**} {destination [destination-wildcard] | **any**} [**precedence** precedence] [**tos** tos] [**established**] [**log** | **log-input**] [**time-range** time-range-name] [**fragments**] **Example:** Device(config)# access-list 107 deny tcp any any	Denies any packet that matches all of the conditions specified in the statement. If the source-wildcard or destination-wildcard is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source or destination address, respectively. Optionally use the keyword **any** as a substitute for the source source-wildcardor destinationdestination-wildcard to specify the address and wildcard of 0.0.0.0 255.255.255.255.

Step 5	Repeat some combination of Steps 3 through 6 until you have specified the fields and values on which you want to base your access list.	Remember that all sources not specifically permitted are denied by an implicit **deny** statement at the end of the access list.
Step 6	**end** **Example:** Device(config)# end	Exits global configuration mode and enters privileged EXEC mode.
Step 7	**show ip access-list** **Example:** Device# show ip access-list	(Optional) Displays the contents of all current IP access lists.

IOS MANAGEMENT

For **<u>Backup and Restore router Configuration we need TFTP/FTP Server</u>**.

This is a step−by−step approach to copy a configuration from a router to a TFTP server, and back to another router. Before you proceed with this method, make sure you have a TFTP server on the network to which you have IP connectivity.

1. At the Router > prompt, issue the enable command, and provide the required password when prompted.

   The prompt changes to Router #, which indicates that the router is now in privileged mode.

2. Copy the running configuration file to the TFTP server:

   ```
   #copy running−config tftp:
   #Address or name of remote host []? 10.0.0.10
   #Destination filename []? mumbai
   #1030 bytes copied in 2.489 secs (395 bytes/sec)
   ```

3. Copy the configuration file from the TFTP server to a new router in privileged (enable) mode which has a basic configuration

   ```
   #copy tftp: running−config
   #Address or name of remote host []? 10.0.0.10
   #Source filename []?mumbai
   !
   #Accessing tftp://10.0.0.10/ mumbai...
   # Loading mumbai from 64.104.207.171 (via FastEthernet0/0): !
   #[OK − 1030 bytes]

   #1030 bytes copied in 9.612 secs (107 bytes/sec)
   ```

<u>NOTE:</u> Then lastly we need to manually up all the port’s /Interfaces because all interfaces are in shutdown mode.

<u>For Erasing the Start-up configuration:</u>

```
#erase start-up config          -         Will erase all the start-up config.
```

For **<u>Backup and Restore router Inter-networking Operating System - IOS we need TFTP/FTP Server</u>**.

This is a step–by–step approach to copy Inter-networking Operating System - IOS from a router to a TFTP server, and back to another router. Before you proceed with this method, make sure you have a TFTP server on the network to which you have IP connectivity.

1. At the Router > prompt, issue the enable command, and provide the required password when prompted.

   The prompt changes to Router #, which indicates that the router is now in privileged mode.

   Type command

   #show flash (Because IOS stored in FLASH) then copy **.bin** file.

2. Copy IOS .bin file to the TFTP server:

```
#copy flash tftp:
# Source filename?c2600-imz.122-28.bin (Copied flash.bin file)
# Address or name of remote host []? 10.0.0.10
#Destination filename []?c2600-imz.122-28.bin
```

For Erase/Delete Inter-networking Operating System - IOS:

```
#delete flash: c2600-imz.122-28.bin
#delete filename[ c2600-imz.122-28.bin]
#delete flash: [ c2600-imz.122-28.bin]?
```

Now if we reload the router, router IOS image will be deleted & we are in ROMMON mode. ROMMON (ROM Monitor) mode in that mode Variables are used.

```
>FE=0
>IP_ADDRESS=10.0.0.1
>IP_SUBNET_MASK=255.0.0.0
>DEFAULT_GATEWAY=10.0.0.10
>TFTP_SERVER=10.0.0.10
>TFTP_FILE= c2600-imz.122-28.bin
>tftpdnld
```

Note: Due to Spanning-tree convergence on switch our **tftpdnld** process is terminated.
So in that case we need to go to -----

```
#interface fastethernet0/1
#spanning-tree portfast
```

Once we have enable spanning-tree portfast bck to the router and copied .bin IOS is copying now

```
>reset
```

To de-compress the IOS Image once router is in started in enable mode type

```
#conf t
#boot system flash c2600-imz.122-28.bin
#end
#wr
```

Passwords

There are FIVE types of Passwords.
Line Passwords— are configured on router lines. Examples of lines are:

1. **Console Line Passwords** – The console is the main serial administrative port on a router. This is where you configure the router when it is new and has no network configuration.

Configuration:

```
#line console 0 (to set the password)
#password 123
#login (enable authentication)
```

For removal of Console Line Password:

```
#line console 0
#no password (for removal of password)
#no login
```

2. **Aux Line Passwords** – The aux line is an auxiliary port. Like the console, it is a physical port on every router. You can think of it as a backup console port. Besides being a backup console port, the aux port is periodically used for administrative console dial up access to the router.

Configuration:

```
#line aux 0 (to set the password)
#password 123
#login (enable authentication)
```

For removal of Aux Line Password:

```
#line aux 0
#no password (for removal of password)
#no login
```

3. **VTY Lines Passwords** – Virtual Terminal Password lines are “virtual tty” lines and are used when you connect to the router via telnet or ssh. These are not physical lines on the router but virtual “inbound network lines”.

- It is used for the telnet password.
- By default login keyword is on the VTY & there are 0-4 sessions are there for telnet.
- On VTY if you set **no login** then it will be directly logged you in without any passwords.

Configuration:

```
#line vty 0 4 (to set the password)
#password 123
#login (enable authentication)
```

For Telnet access you need to set 2 Types of passwords.

1. VTY password
2. Enable secret password

For removal of VTY Line Password:

```
#line vty 0 4
#no password (for removal of password)
#end
```

Privileged mode Password / Enable Mode:

Another basic router security requirement is that you configure a password used to enter privileged mode (enable mode).

Configuration:

```
#conf t
#enable password 123
```

For removal of VTY Line Password:

```
#conf t
#no enable password (for removal of password)
#end
```

Enable Secret Password:

The enable secret command does encrypt the password.

Configuration:

```
#conf t
#enable secret cisco (cisco is password)
```

For removal of VTY Line Password:

```
#conf t
#no enable secret (for removal of password)
#end
```

NOTE: If you set Enable mode password as well Enable secret password it will only take the secret password.

Multiple Username & Passwords:

You can configure usernames and associated passwords on a Cisco router. This is a more advanced level of security than line passwords. Once configured on the lines, the line password is then ignored.

If multiple engineers are using 1 Router, we can create multiple username and passwords with their rights.

Configuration:

```
#conf t
#username cisco password ccna
#username network password ccnp
```

We can configure as many as username and passwords which we required.
Once you create the username, you need to tell each line to use the local username/password database, on the router. To do this, go back to each line and type login local.

```
#line console 0
#login local
#exit
#line aux 0
#login local
#line vty 0 4
#login local
```

For removal of **Username & Passwords:**

```
#conf t
#no username cisco password ccna
#end
```

Encryption password:

For encrypt all cleared visible password on level 7.

```
#conf t
#service password encryption
```

Note: All level 7 passwords are easy to cracked with on-line software's.
http://www.ifm.net.nz/cookbooks/passwordcracker.html

Password Recovery Procedure for the Cisco

Step-by-Step Procedure

Perform these steps in order to recover your password:

1. Either switch off or shut down the router.
2. Switch on the router for entering in ROMMON mode. Press Ctrl + Break OR Ctrl + C for entering in rommon mode.
3. Once the router is on rommon mode
4. Type **confreg 0x2142** at the rommon 1> prompt in order to boot from Flash.

This step bypasses the startup configuration where the passwords are stored.

5. Type **reset** at the rommon 2> prompt.

The router reboots, but ignores the saved configuration.

6. Type **no** after each setup question, or press **Ctrl-C** in order to skip the initial setup procedure.
7. Type **enable** at the Router> prompt.

You are in enable mode and should see the Router# prompt.

8. Type **configure memory** or **copy startup-config running-config** in order to copy the nonvolatile RAM (NVRAM) into memory.

⚠ **Warning:** Do **not** enter **copy running-config startup-config** or **write**. These commands erase your startup configuration.

9. Issue the **show running-config** command.

The **show running-config** command shows the configuration of the router. In this configuration, the **shutdown** command appears under all interfaces, which indicates all interfaces are currently shut down. In addition, the passwords (enable password, enable secret, vty , and console passwords) are in either an encrypted or unencrypted format. You can reuse unencrypted passwords. You must change encrypted passwords to a new password.

10. Type **configure terminal**.

The hostname(config)# prompt appears.

11. Type **enable secret <**password**>** in order to change the **enable secret** password. For example:

    ```
    hostname(config)#enable secret cisco
    ```

12. Type **config-register** <configuration_register_setting> .
    Where <configuration_register_setting> is either the value you recorded in step 2 or 0x2102 . For example:

    ```
    hostname(config)#config-register 0x2102
    ```

13. Press **Ctrl-z** or **end** in order to leave the configuration mode.

The hostname# prompt appears.

14. Type **write memory** or **copy running-config startup-config** in order to commit the changes.

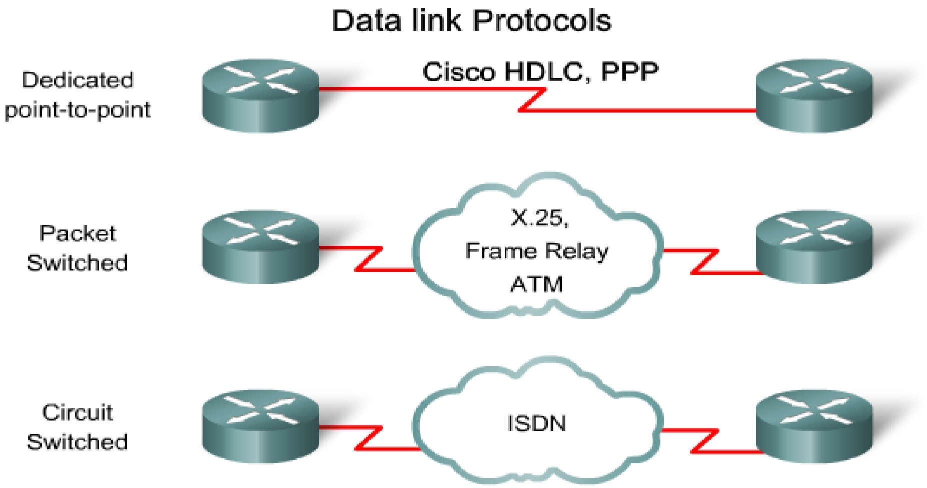
What Is a WAN?

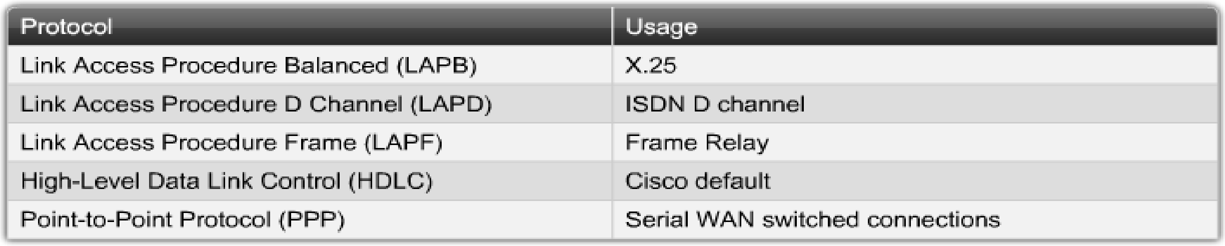
A WAN is a data communications network that covers a relatively broad geographic area and often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

WAN [Wide Area Network]: A computer **network** that spans a relatively large geographical area. Typically, a **WAN** consists of two or more local-area **networks** (LANs). Computers connected to a **wide-area network** are often connected through public **networks**, such as the telephone system. They can also be connected through leased lines or satellites.

There are three types of WAN network technologies:

1. Dedicated - Point-to-Point Links, Lease-line
2. Circuit Switching – ISDN,PSDN
3. Packet Switching – Frame Relay, ATM, X.25

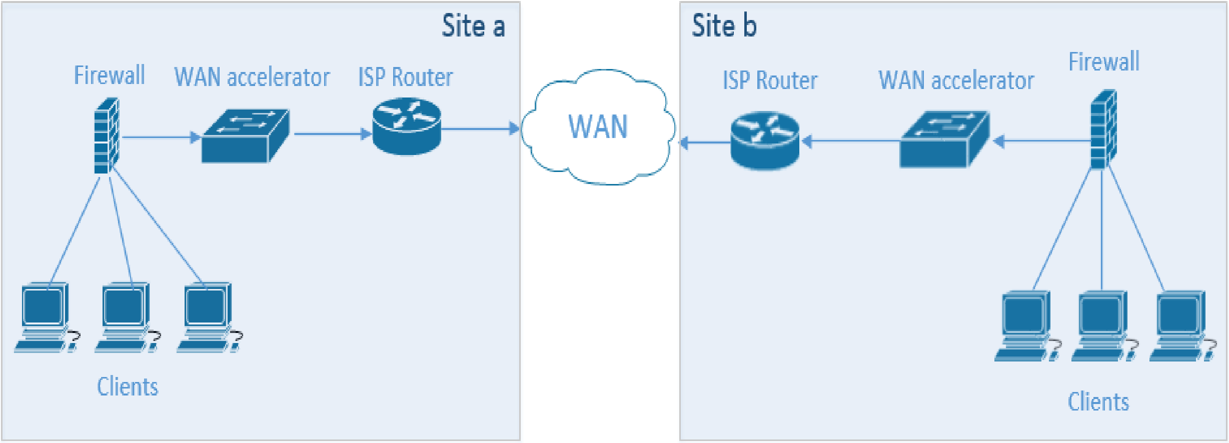




Protocol	Usage
Link Access Procedure Balanced (LAPB)	X.25
Link Access Procedure D Channel (LAPD)	ISDN D channel
Link Access Procedure Frame (LAPF)	Frame Relay
High-Level Data Link Control (HDLC)	Cisco default
Point-to-Point Protocol (PPP)	Serial WAN switched connections

1. Dedicated - Point-to-Point Links, Lease-line

A *point-to-point link* provides a single, pre-established WAN communications path from the customer premises through a carrier network, such as a telephone company, to a remote network. A point-to-point link is also known as a leased line because its established path is permanent and fixed for each remote network reached through the carrier facilities. The carrier company reserves point-to-point links for the private use of the customer.

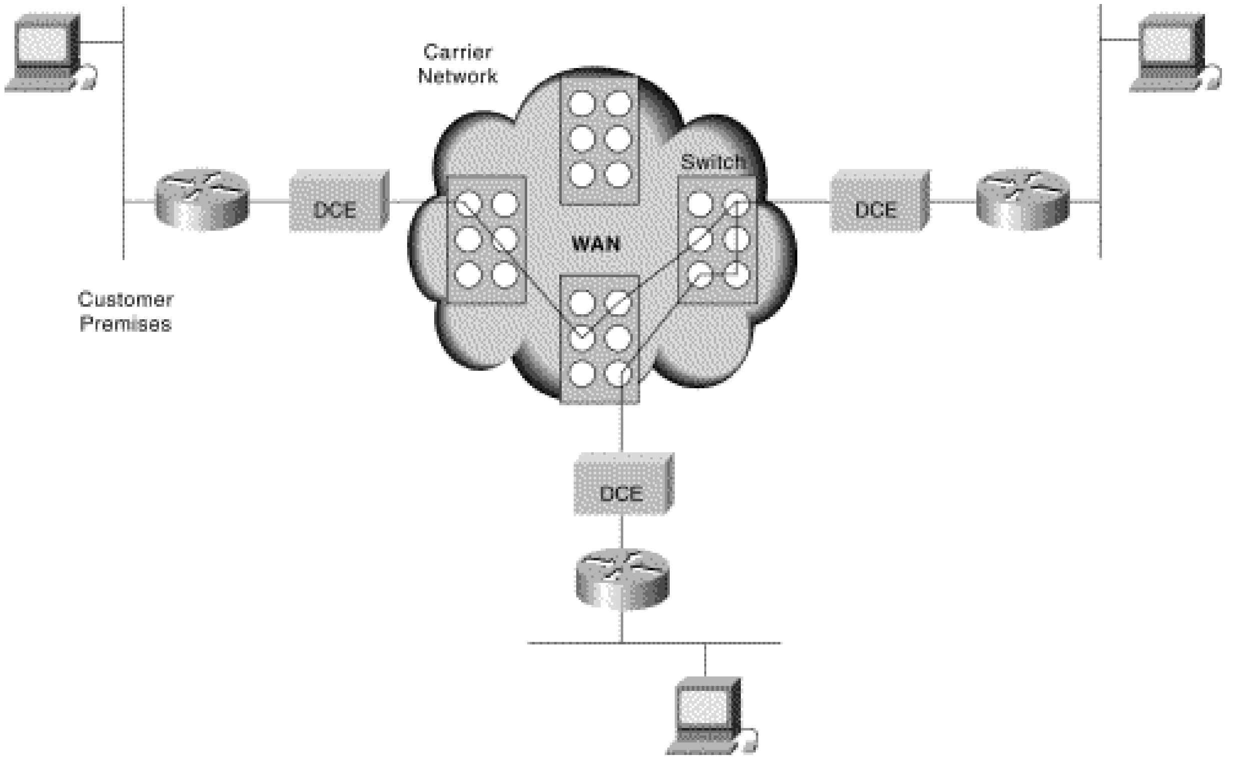


Characteristic of Dedicated –Point to Point Links, Leased Line

1. 24 X 7 Access
2. Dedicated Bandwidth because no one is sharing that links with us.
3. Secure as we are only using that link.
4. Very Expansive.

2. Circuit Switching – ISDN,PSDN

Circuit switching is a WAN switching method in which a dedicated physical circuit is established, maintained, and terminated through a carrier network for each communication session. Circuit switching accommodates two types of transmissions: datagram transmissions and **d**ata-stream transmissions. Used extensively in telephone company networks, circuit switching operates much like a normal telephone call. Integrated Services Digital Network (ISDN) is an example of a circuit-switched WAN technology

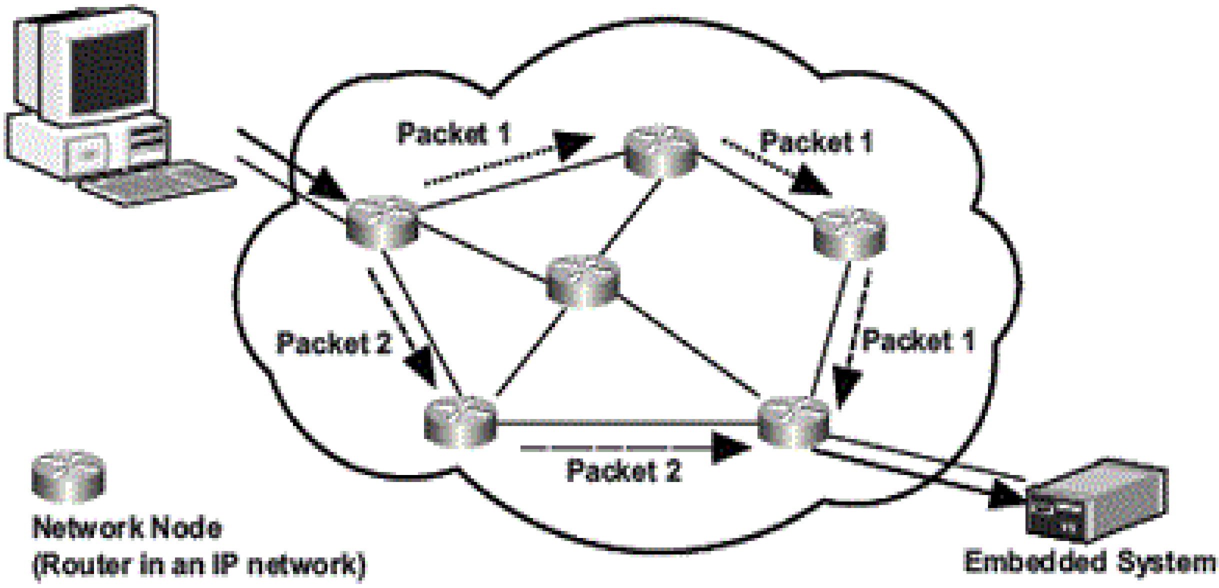


Characteristic of Circuit Switching – ISDN,PSDN

1. Dial On Demand
2. Shared Bandwidth because there are multiple users who uses the same link.
3. Not so secure as there are multiple users who uses that link.
4. Very Cheap.

3. Packet Switching – Frame Relay, ATM, X.25

Packet switching is a WAN switching method in which network devices share a single point-to-point link to transport packets from a source to a destination across a carrier network. Statistical multiplexing is used to enable devices to share these circuits. Asynchronous Transfer Mode (ATM), Frame Relay, Switched Multimegabit Data Service (SMDS), and X.25 are examples of packet-switched WAN technologies.



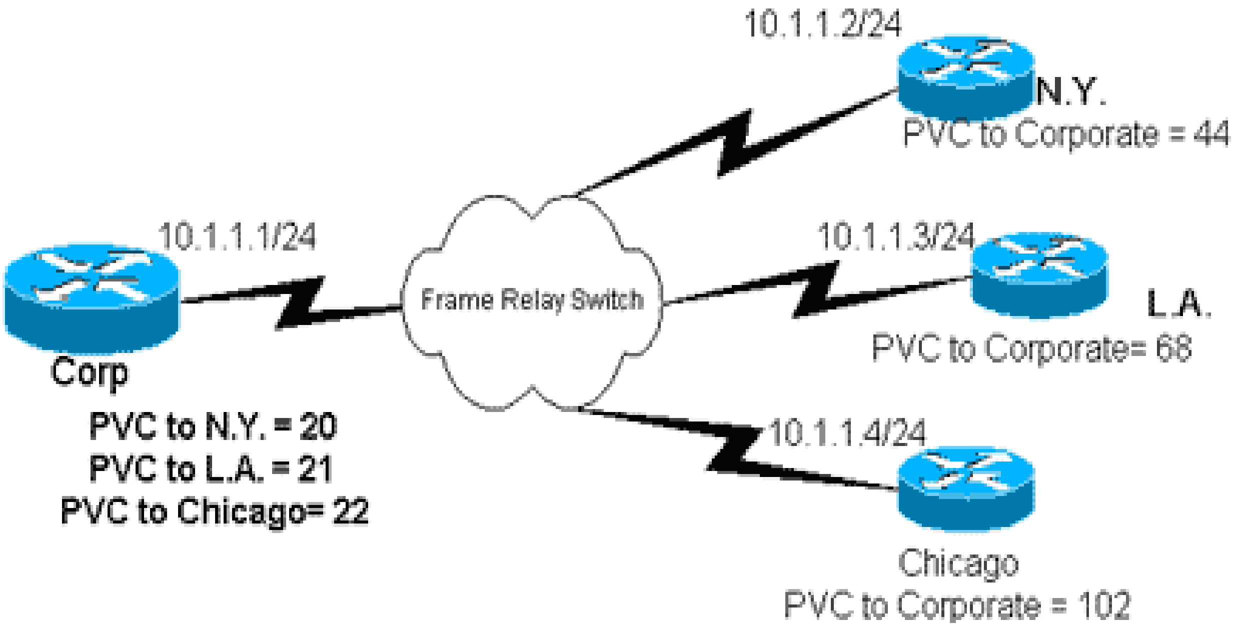
Characteristic of Packet Switching – Frame Relay, ATM, X.25

1. Access 24 X 7
2. Shared Bandwidth because there are multiple users who uses the same link.
3. Not so secure as there are multiple users who uses that link.
4. COST EFFECTIVE.

Frame Relay:

Frame Relay is a standardized wide area network technology that specifies the physical and logical link layers of digital telecommunications channels using a packet switching methodology.

Frame Relay is a scalable WAN solution that is often used as an alternative to leased lines when leased lines prove to be cost unaffordable. With Frame Relay, you can have a single serial interface on a router connecting into multiple remote sites through virtual circuits.



Frame relay is also known as Non-Broadcast Multi-access (NBMA) network.

1. It works on layer 2 , with DLCI (Data link Control Identifier)
2. Router Works on Layer 3(IP Add ress)
3. Mapping layer 2 (DLCI) TO layer 3 (IP Address)

There are 2 ways of Mapping.

1. Dynamic (inverse A.R.P) – by default
2. Static Mapping

Virtual Circuits (VCs)

A VC is a logical connection between two devices; therefore, many of these VCs can exist on the same physical connection. The advantage that VCs have over leased lines is that they can provide full connectivity at a much lower price. VCs are also full-duplex: you can simultaneously send and receive on the same VC.
There are two types of VCs: permanent VCs (PVCs) and switched or semi permanent VCs (SVCs).

PVC is similar to a leased line: it is configured up front by the carrier and remains up as long as there is a physical circuit path from the source to the destination.

SVC are similar to telephone circuit-switched connections: whenever you need to send data to a connection, an SVC is dynamically built and then torn down once your data has been sent.

The three possible states that your PVC can be in are

- **Active**— Active is good. Active means that everything is up and operational.
- **Inactive**— Inactive is bad. Inactive means that you are connected to your Frame Relay provider, but there is a problem with the far-end connection. The problem is most likely between the far-end router and its connection to the Frame Relay provider. You should contact your provider to troubleshoot the issue.
- **Deleted**— Deleted is also bad. Deleted means that there is a problem between your router and the Frame Relay provider's equipment. You should contact your provider to troubleshoot this issue.

DLCI: data-link connection identifiers

Each VC has a unique local address, called a DLCI. Circuits are identified by data-link connection identifiers (DLCI). DLCIs are assigned by your provider and are used between your router and the Frame Relay provider. In other words, DLCIs are locally significant. This means that as a VC traverses various segments in a WAN, the DLCI numbers can be different for each segment. DLCIs are locally significant. The carrier’s switches take care of mapping DLCI numbers for a VC between DTEs and DCEs.

Nonbroadcast Multi-access:

Nonbroadcast multi-access (NBMA) is a term used to describe WAN networks that use VCs for connectivity Frame Relay is a nonbroadcast multi-access (NBMA) medium, which means that broadcast traffic is not allowed to traverse Frame Relay traffic.

Split Horizon Issues:

The main problem of NBMA environments arises when the network is partially meshed for a subnet. This can create problems with routing protocols that support split horizon.

Solutions to Split Horizon Problems:

Given the preceding problem with routing protocols that use split horizon, there are solutions that you can use to overcome this issue:

1. Use static routes instead of dynamic routing protocols. This is not a scalable solution.
2. Disable split horizon with the no ip split-horizon command. This could create a loop, If you are not careful
3. Have a fully meshed topology where every router has PVC to every other router. This can get expensive.
4. Use sub interfaces. This is your best option.

Sub interfaces:

A sub interface is a subset of an existing physical interface. As far as the router is concerned, the sub interface is a separate interface. By creating sub interfaces, each circuit can be on its own subnet. There are two types of sub interfaces:

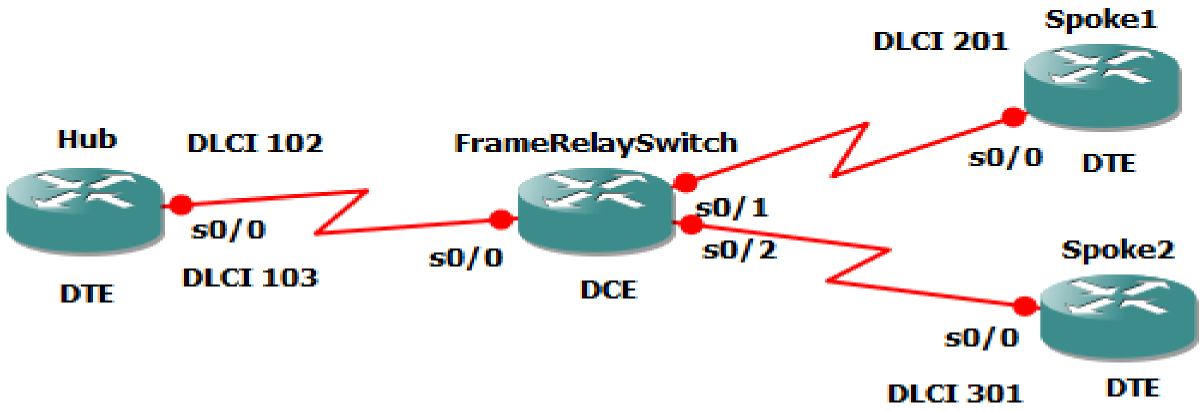
1. Point-to-point— this maps a single IP subnet to a single sub interface and DLCI.
2. Multipoint— this maps a single IP subnet to multiple DLCIs on a sub interface.

Inverse-Arp:

Frame Relay needs a mechanism to map Layer 3 addresses withLayer 2 Frame Relay DLCIs. This can be done through a static map command (shown later in the configuration section) or through inverse-arp. Just like Ethernet ARP, inverse-arp is used to map a Layer 3 address to a Layer 2 address. However, Ethernet ARP maps an IP address to a MAC address and inverse-arp works to map an IP address (or other protocol) to a DLCI.

Configuring a Cisco Router as a Frame Relay Switch:

Cisco routers can be configured as dedicated Frame Relay switches that act as DCE devices. On a Cisco router configured as a Frame Relay switch



For example in above scenario we have Three Branches.

1. Mumbai as Hub
2. Delhi as Spoke1
3. Bangalore as Spoke2

Note: Route is always configured on Provider edge
Mapping is always configured on Customer edge

On Frame Relay Switch:

```
#hostname FrameRelaySwitch
!
#Frame-relay switching
!
#interface Serial0/0
#no ip address
#encapsulation frame-relay
#frame-relay route 102  interface Serial0/1 201
#frame-relay lmi-type cisco
#frame-relay intf-type dce
#clockrate 64000
#no shutdown
!
#interface Serial0/1
#no ip address
#encapsulation frame-relay
#frame-relay route 201  interface Serial0/0 102
#frame-relay lmi-type cisco
#frame-relay intf-type dce
#clockrate 64000
#no shutdown
```

On HUB (Mumbai):

```
#interface Serial0/0
#ip address 20.0.0.1 255.255.255.248
#encapsulation frame-relay
#no shutdown
```

On Spoke1 (Delhi):

```
#interface Serial0/0
#ip address 20.0.0.2 255.255.255.248
#encapsulation frame-relay
#no shutdown
```

For Verifying Frame Relay Status:

```
#Show frame-relay pvc
#show frame-relay map
```

Now if we add Bangalore in Frame Relay network we need to make some new configuration in Frame-Relay Switch.

On Frame Relay Switch:

```
#interface Serial0/2
#no ip address
#encapsulation frame-relay
#frame-relay route 301  interface Serial0/0 103
#frame-relay lmi-type cisco
#frame-relay intf-type dce
#clockrate 64000
#no shutdown
```

On Spoke2   (Bangalore):

```
#interface Serial0/0
#ip address 20.0.0.3 255.255.255.248
#encapsulation frame-relay
#no shutdown
```

To resolve Hub and spoke Issue we need to configure **STATIC MAPPING**.

Hub (Mumbai):

```
#interface Serial0/0
#no frame-relay inverse arp
#frame-relay map ip 20.0.0.2 102 broadcast
#frame-relay map ip 20.0.0.3 103 broadcast
```

Spoke1 (Delhi):

```
#interface Serial0/0
#no frame-relay inverse arp
#frame-relay map ip 20.0.0.1 201 broadcast
#frame-relay map ip 20.0.0.3 201 broadcast
```

Spoke2 (Bangalore):

```
#interface Serial0/0
#no frame-relay inverse arp
#frame-relay map ip 20.0.0.1 301 broadcast
#frame-relay map ip 20.0.0.2 301 broadcast
```

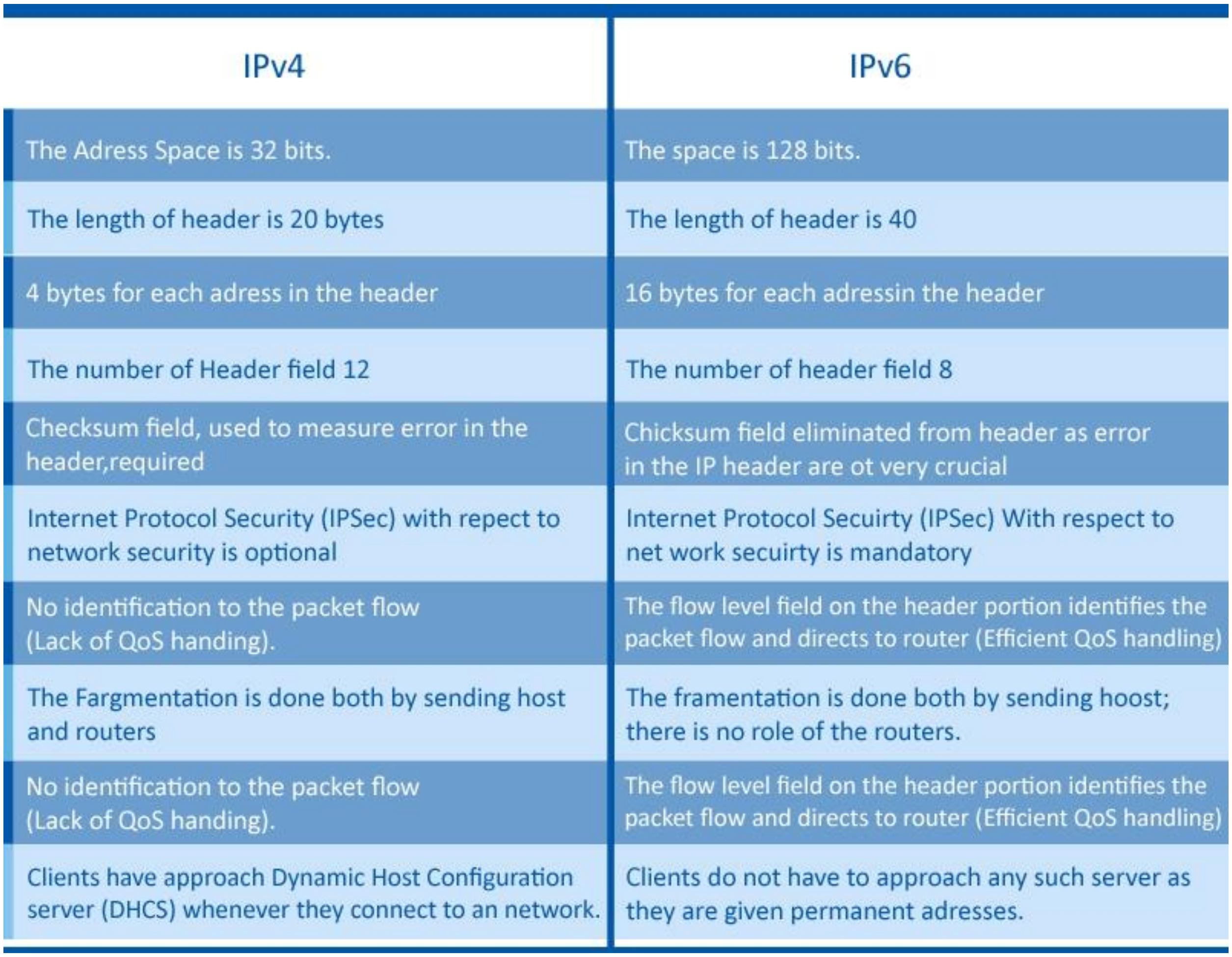
IPv6 (Internet Protocol Version 6)

IPv6 (Internet Protocol version 6) is a set of specifications from the Internet Engineering Task Force (IETF) that's essentially an upgrade of IP version 4 (IPv4). The basics of IPv6 are similar to those of IPv4- devices can use IPv6 as source and destination addresses to pass packets over a network, and tools like ping work for network testing as they do in IPv4, with some slight variations.

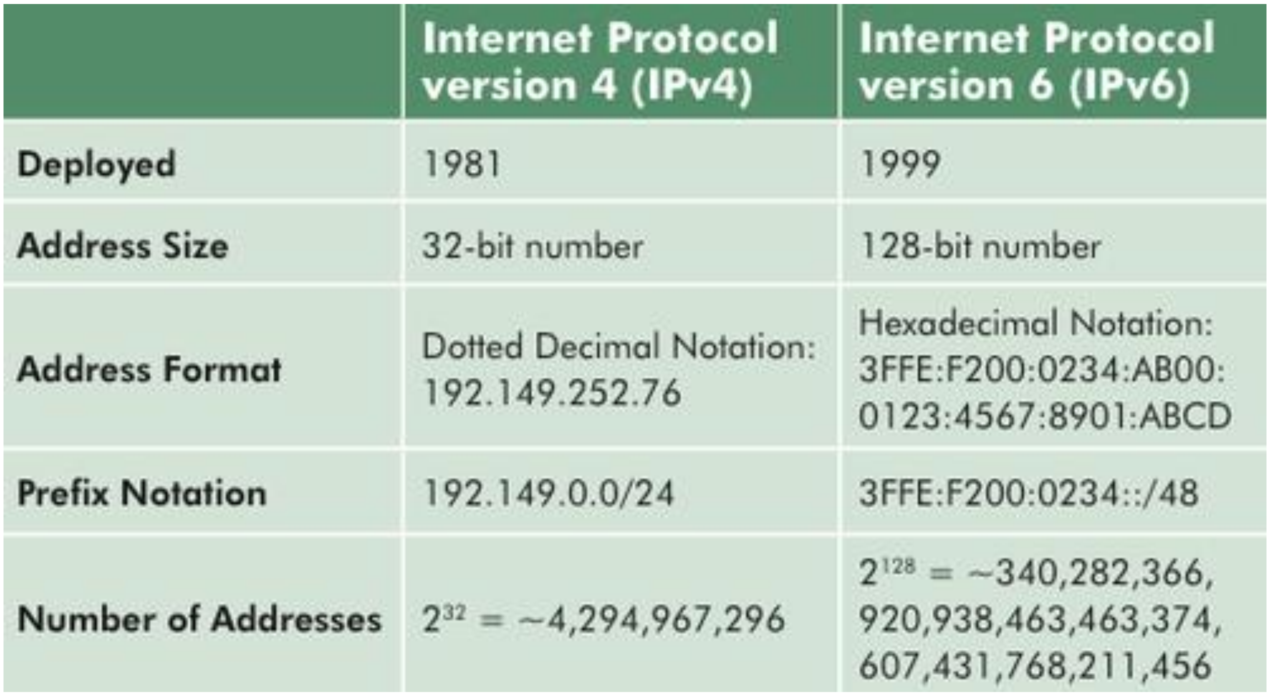
The most obvious improvement in IPv6 over IPv4 is that IP addresses are lengthened from 32 bits to 128 bits. This extension anticipates considerable future growth of the Internet and provides relief for what was perceived as an impending shortage of network addresses. IPv6 also supports auto-configuration to help correct most of the shortcomings in version 4, and it has integrated security and mobility features.

IPv6 features include:

- Supports source and destination addresses that are 128 bits (16 bytes) long.
- Requires IPSec support.
- Uses Flow Label field to identify packet flow for QoS handling by router.
- Allows the host to send fragments packets but not routers.
- Doesn't include a checksum in the header.
- Uses a link-local scope all-nodes multicast address.
- Does not require manual configuration or DHCP.
- Uses host address (AAAA) resource records in DNS to map host names to IPv6 addresses.
- Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.
- Supports a 1280-byte packet size (without fragmentation).
- Moves optional data to IPv6 extension headers.
- Uses Multicast Neighbor Solicitation messages to resolve IP addresses to link-layer addresses.
- Uses Multicast Listener Discovery (MLD) messages to manage membership in local subnet groups.

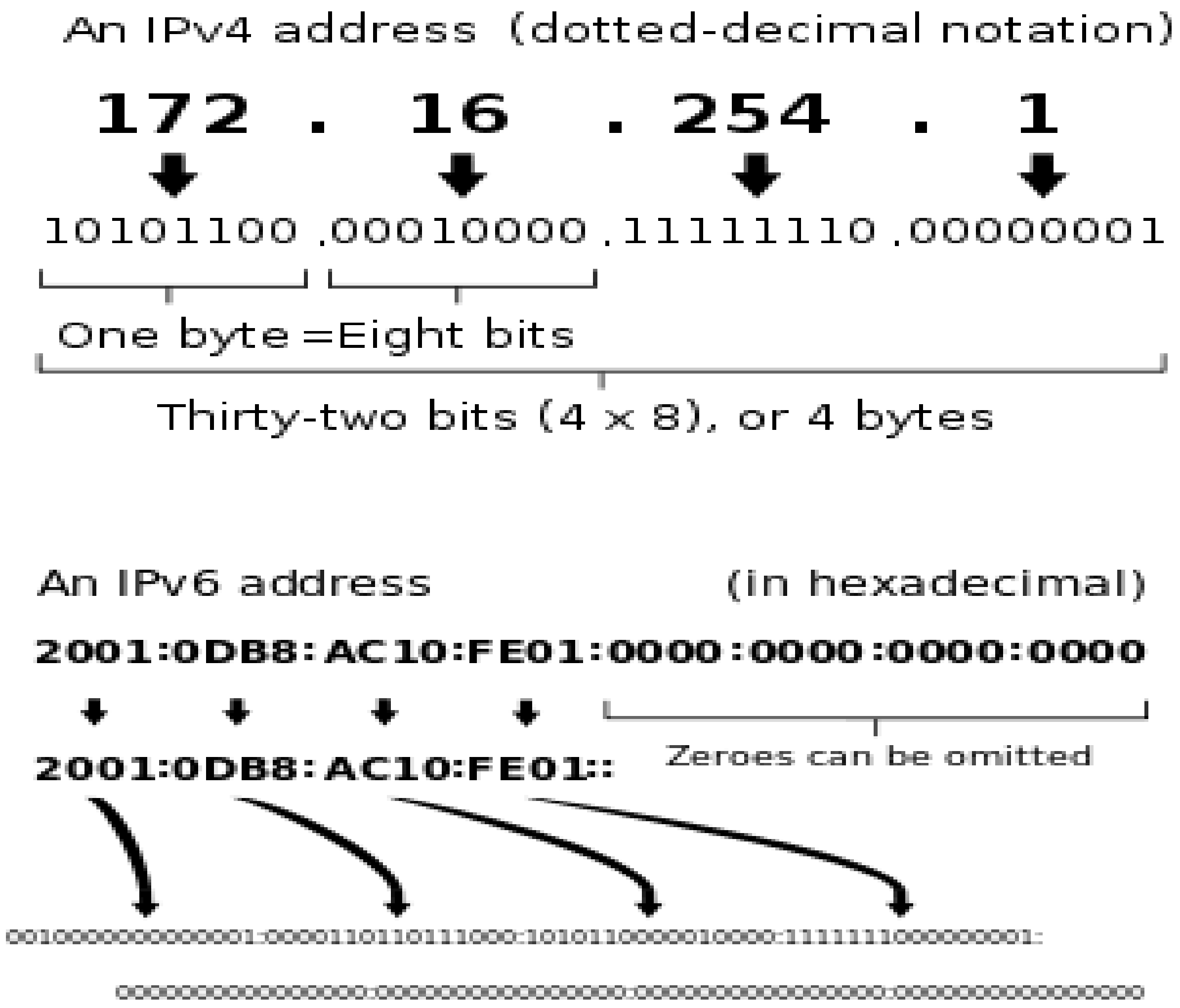


IPv4	IPv6
The Adress Space is 32 bits.	The space is 128 bits.
The length of header is 20 bytes	The length of header is 40
4 bytes for each adress in the header	16 bytes for each adressin the header
The number of Header field 12	The number of header field 8
Checksum field, used to measure error in the header,required	Chicksum field eliminated from header as error in the IP header are ot very crucial
Internet Protocol Security (IPSec) with repect to network security is optional	Internet Protocol Secuirty (IPSec) With respect to net work secuirty is mandatory
No identification to the packet flow (Lack of QoS handing).	The flow level field on the header portion identifies the packet flow and directs to router (Efficient QoS handling)
The Fargmentation is done both by sending host and routers	The framentation is done both by sending hoost; there is no role of the routers.
No identification to the packet flow (Lack of QoS handing).	The flow level field on the header portion identifies the packet flow and directs to router (Efficient QoS handling)
Clients have approach Dynamic Host Configuration server (DHCS) whenever they connect to an network.	Clients do not have to approach any such server as they are given permanent adresses.



	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	2^{32} = ~4,294,967,296	2^{128} = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456

Examples of IPv4 & IPv6:



Important Questions

1: What is the primary purpose of a LAN?
A: The primary purpose of a local-area network is to allow resource sharing. The resources may be devices, applications, or information. Examples of shared resources are files, databases, e-mail, modems, and printers.

2: What is a protocol?
A: A protocol is an agreed-upon set of rules. In data communications, the rules usually govern a procedure or a format.

3: Why is a MAC address not a true address?
A: An address specifies a location. A MAC address is not a true address because it is permanently associated with the interface of a specific device and moves whenever the device moves. A MAC identifies the device, not the location of the device.

4: What is a packet? What is the primary similarity between a frame and a packet? What is the primary difference between a frame and a packet?
A: A packet is the means by which data is transported from one network to another. The similarity between a frame and a packet is that they both encapsulate data and provide an addressing scheme for delivering the data. The difference between a frame and a packet is that the frame delivers data between two devices sharing a common data link, whereas a packet delivers data across a logical pathway, or route, spanning multiple data links.

5: What is ARP?
A: ARP, or Address Resolution Protocol, is a function that maps the IP addresses of interfaces on a data link to their corresponding MAC identifiers.

6: What is the essential difference between TCP and UDP?
A: TCP, or Transmission Control Protocol, provides a connection-oriented service over the Connectionless internet layer. UDP, or User Datagram Service, provides a connectionless service.

7: What is a floating static route?
A: A floating static route is an alternative route to a destination. The administrative distance is set high enough that the floating static route is used only if a more-preferred route becomes unavailable.

8: What information must be stored in the route table?
A: At a minimum, each entry of the routing table must include a destination address and the address of a next-hop router or an indication that the destination address is directly connected.

9: Why do routing protocols use metrics?
A: A route metric, also called a route cost or a route distance, is used to determine the best path to a destination. *Best* is defined by the type of metric used.

10: What is a distance vector routing protocol?
A: A distance vector protocol is a routing protocol in which each router calculates routes based on the routes of its neighbors and then passes its routes to other neighbors.

11: What are Hold down timers, and how do they work?
A: Hold down timers help prevent routing loops. If a route is declared unreachable or if the metric increases beyond a certain threshold, a router will not accept any other information about that route until the hold down timer expires. This approach prevents the router from accepting possibly bad routing information while the internetwork is reconverging.

12: What are the differences between distance vector and link state routing protocols?
A: A distance vector router sends its entire route table, but it only sends the table to directly connected neighbors. A link state router sends only information about its directly connected links, but it floods the information throughout the internetworking area. Distance vector protocols usually use a variant of the Bellman-Ford algorithm to calculate routes, and link state protocols usually use a variant of the Dijkstra algorithm to calculate routes.

13: What is the purpose of a topological database?
A: A topological database holds the link state information originated by all routers in the link state routing domain.

14: What is an autonomous system?
A: Depending on the usage, an autonomous system can be defined as an internetwork under a common administrative domain or a single routing domain.

15: What is the difference between an IGP and an EGP?
A: An Interior Gateway Protocol is a routing protocol that routes within an autonomous system. An Exterior Gateway Protocol is a routing protocol that routes between autonomous systems.

16: What is the feasibility condition?
A: The feasibility condition is the rule by which feasible successors are chosen for a destination. The feasibility condition is satisfied if a neighbor's advertised distance to a destination is lower than the receiving router's feasible distance to the destination. In other words, a router's neighbor meets the feasibility condition if the neighbor is metrically closer to the destination than the router. Another way to describe this is that the neighbor is "downstream" relative to the destination.

17: What is a Router ID? How is a Router ID determined?
A: A Router ID is an address by which an OSPF router identifies itself. It is either the numerically highest IP address of all the router's loopback interfaces, or if no loopback interfaces are configured, it is the numerically highest IP address of all the router's LAN interfaces.

18: What is the significance of area 0?
A: Area 0 is the backbone area. All other areas must send their inter-area traffic through the backbone.

19: What is the difference between OSPF network entries and OSPF router entries?
A: OSPF network entries are entries in the route table, describing IP destinations. OSPF router entries are entries in a separate route table that record only routes to ABRs and ASBRs.

20: What is the purpose of an administrative distance?
A: In contrast to metrics, which are used to determine the best path among multiple routes to the same destination discovered by the same routing protocol, administrative distances are used to determine the best path among multiple routes to the same destination discovered by different routing protocols.

21: How can administrative distances cause problems when redistributing?
A: A route to a destination within a routing domain with a higher administrative distance can be redistributed into a routing domain with a lower administrative distance. If that route is redistributed back into the higher-distance domain, packets might be misrouted into the lower-distance domain.

22: What is MTU?

A: MTU stands for Maximum Transmission Unit. It refers to the maximum packet size that can be sent out onto the data line without the need to fragment it.

23: What is subnetting?

A: Subnetting is the process of creating smaller networks from a big parent network. Being a part of a network, each subnet is assigned some additional parameters or identifier to indicate its subnet number.

24: What is Bandwidth?

A: Bandwidth refers to the transmission capacity of a medium. It is a measure of how much volume a transmission channel can handle, and is measured in Kbps.

25: What is Route Poisoning?

A: Route Poisoning is the process of inserting a table entry of 16 to a route, making it unreachable. This technique is used in order to prevent problems caused by inconsistent updates on a route.

26: Mention what is the size of IP address?

A: Size of IP address is 32 bit for IPv4 and 128 bit for IPv6.

27: Mention what is the difference between dynamic IP and static IP addressing?

A: Dynamically IP addresses are provided by DHCP server and static IP address are given manually.

28: In how many ways you can access router?

A: You can access it in three ways:

- Telnet (IP)
- AUX (Telephone)
- Console (Cable)

29: **What are broadcast domains?**

A: A broadcast domain defines a group of devices that receive each others' broadcast messages. As with collisions, the more broadcasts that occur on the network, the slower your network will be. This is because every device that receives a broadcast must process it to see if the broadcast is intended for it.

30: What is the difference between a routing protocol and a routed protocol?

A: Routing protocols determine how to route traffic to the best location of a routed protocol. Examples of routing protocols are RIP, EIGRP, OSFP, and BGP. Examples of routed protocols are IP and IPX.

31:Where would you use cross and straight cable?

A: A straight-through cable is used for DTE-to-DCE connections.

- 1. A hub to a router, PC, or file server.
- 2.A switch to a router, PC, or file server.

Crossover cables should by used when you connect a DTE to another DTE or a DCE to another DCE.

- 1. A hub to another hub
- 2. A switch to another switch
- 3. A hub to a switch
- 4. A PC, router, or file server to another PC, router, or file server

32: What is Network Latency?

A: Network latency refers to the performance of one device when it communicates with another. Network latency is affected by bandwidth speeds, network card performance, cabling and congestion. High latency can also mean users won’t be able to properly communication with applications, which will “time out” if latency is too high.

33: What is attenuation?

A: The degeneration of a signal over distance on a network cable is called attenuation.

34: What is cladding?
A: A layer of a glass surrounding the center fiber of glass inside a fiber-optic cable.

35: Describe the difference between unicast, multicast, and broadcast traffic?
A: Unicast traffic flows from a single source to a single destination MAC address. Multicast traffic flows from a single source MAC address to many destinations and uses a functional MAC address. Broadcast traffic is from a single source to all devices on the Ethernet segment. This is specified by a destination MAC address of all ones.

36: What is a stub area?
A: A stub area is an area that does not accept routing updates from outside its autonomous system.

37: Which layer of OSI model I responsible for reliable connections?

A: The transport layer is responsible for reliable connection.

38: What is the main difference between acknowledgement and handshaking?

A: Acknowledgement is just a message which convey the sender that receiver received the data successfully. Handshaking is used to convey the properties of the connection that is being established.

39: When does the congestion occur?

A: Network congestion is occurred due to accessing of same bandwidth by many users at the same time and there is no alternative to network segmentation.

40: What is routing?

A: Routing is process of finding the shortest path for communicating from source to destination. This process is accomplished by the routers on network.

41: What is window in networking terms?

A: A window is sets of segment that is allowed to be sent from source to destination before the acknowledgement is sent back to it.

42: What is VLAN?

A: Virtual LAN or VLAN is a logical groupor segment network connected to administratively defined ports on a switch, they Broadcast control, Flexibility and security.

43: What is sub-Netting? Why it is used?

A: It is used to break the larger network into smaller sub-networks, used in IP Networks. Basically used for minimizing the network traffic, optimizing the performance, and managing the network.

44: What is communication and how it is differ to transmission?

A: Communication means exchanging of data between source and destination. Whereas, transmission refers to only transferring of data from source to receiver.

45: Two interface of the router is configured with IP addresses 192.168.1.1; subnet mask 255.255.255.0 and IP address 192.168.2.1, subnet mask 255.255.255.0. Would the routing table of the router contain any information? Provide explanations

A: The router would have to perform AND operation with IP address and subnet mask when the interface has configured. This is ultimately yield a network address and after it configured to interface, two entries will available in the routing tables which are 192.168.1.0 and 192.168.2.0 which are network address of 192.168.1.1 and 192.168.2.1 respectively.

46: Does bridge divide a network into smaller segments?

A: No, it not, it only filters the large networks without changing their size.

47: What is the role of LLC sub layer?

A: Logical Link Control sub layer provides the controlled or optional services to the Network layer with start and stop codes. It also does the error correction.

48: What is RAID in CCNA?

A: A method to standardize and categorize fault tolerance disk systems. Some servers use the three RAID: RAID Level 0 (stripping), RAID Level 1 (mirroring) and RADI Level 5 (stripping and parity).

49: List the two types of transmission technology?

A: Point-to-point and broadcast transmission technologies are available in the CCNA.

50: What is point-to-point transmission protocol?

A: It is an industry standard in which the exchange of multiport datagrams is done use of protocol that is providing point-to-point link.

51: What are the possible ways of data exchange?

A: There are only three types of possible ways to exchange data i.e. Simplex, Half-duplex and full-duplex.

52: What is the difference between Baseband and Broadband?

A: If the transmission is on baseband, the entire of the cable is consumed by the single signal. Whereas, in in broadband transmission, signals are sent on multiple frequencies, allowing multiple signals to be sent simultaneously.

53: What is difference between TCP and UDP?

A: TCP is connection oriented Protocol whereas UDP is connectionless protocol. In TCP protocol reliable transmission is done. UDP is less reliable then TCP.

54: Difference between public IP and private IP?

A: Public IP should be unique address that is assigned to a company. Private address can be used by anyone on private network because it is not recognized by the internet.

55: What is latency?

A: Latency is the time duration that is measured from the point of time which a device receives a data frame to the time it sends out again towards another network segment.

56: What is frame relay?

A: Frame Relay is a WAN protocol that delivers connection-oriented communication by implementing and retaining virtual circuits. It has a high performance rating and operates at the Data Link and Physical Layers.

57: Explain difference between Router, Switch and Hub?

Hub: A hub is typically the least expensive, least intelligent, and least complicated of the three. Its job is very simple – anything that comes in one port is sent out to the others. Hub has single collision domain and single broadcast domain

Switch: Switch is a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. Switches have multiple collision domains and have a single broadcast domain

58: Explain broadcast and collision domain?

A: A broadcast domain is a logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer.

A collision domain is a section of a network where data packets can collide with one another when being sent on a shared medium or through repeaters

59: What is the range of class A address?

A: Class A Range from 1.0.0.1 to 126.255.255.254 and Supports 16 million hosts on each of 127 networks.

60: What is the range of class B address?

A: Class B range from 128.1.0.1 to 191.255.255.254 and Supports 65,000 hosts on each of 16,000 networks.

61: What is the range of class C address?

A: Class C range is from 192.0.1.1 to 223.255.254.254 and Supports 254 hosts on each of 2 million networks.

62: What is a peer-peer process?

A: A peer-to-peer (P2P) network is a type of decentralized and distributed network architecture in which individual nodes in the network (called "peers") act as both suppliers and consumers of resources. There will be no centralized system we usually seen like Client server model. Simply in p2p, network devices act as both client and server

63: What is Round Trip Time?

A: Round-trip time (RTT), also called round-trip delay, is the time required for a packet to travel from a specific source to a specific destination and back again.Source is the computer sending the packet and the destination is a remote computer or system that receives the packet and retransmits it. A user can determine the RTT to and from an IP address by pinging that address.

64: What is DHCP scope?

A: A Dynamic Host Configuration Protocol (DHCP) scope is the consecutive range of possible IP addresses that the DHCP server can lease to clients on a subnet.

65: What is Checksum?

A: A simple error-detection scheme in which each transmitted message is accompanied by a numerical value based on the number of set bits in the message. The receiving station then applies the same formula to the message and checks to make sure the accompanying numerical value is the same. If not, the receiver can assume that the message has been garbled.

Thank You