CCNA
Cisco Certified Network Associate

INDEX

- **Router mode**
- **Line mode**
- **ROM mode**

- **Router Configuration Basic Commands**
  - **Various Show commands**
  - **Assigning IP address to serial interface**
  - **Assigning IP address to Ethernet Interface**
  - **Assigning Enable and Enable secret password**
  - **Assigning line, console and auxiliary passwords**
- **WAN TECHNOLOGIES**
    - **Types of WAN connectivity**
    - **Types of WAN Protocols**
    - **HDLC**
    - **PPP**
    - **PPP authentication protocols**
    - **PAP**
    - **CHAP**
- **Frame Relay Protocol**
  - **What is PVC and SVC**
  - **DLCI number**
  - **Encapsulation types**
  - **LMI standards**
  - **Inverse ARP**
- **Using TFTP Server**
    - **Configurations IOS backup**
    - **Configurations of IOS Restore**
    - **Configuration of IOS Repair**
- **Password Recovery**
    - **On fixed routers**
    - **On modular routers**
    - **Configuration of various IOS registers**
- **Routing Protocols**
  Basic of routing
  Types of routing
    - **Static routing**
    - **Default routing**
    - **Dynamic routing**
    - **What is IGP and EGP**
    - **Dynamic Routing Protocols**
    - **Distance Vector Protocol**
        - **RIP**
        - **IGPR**
    - **Link state Protocol**
        - **OSPF**
    - **Hybrid Protocol**

            - EIGRP

- **Access Lists**
- **Standard Access Lists**
    - **What is Wild card mask**
    - **Assigning Standand list on variours intefaces**
- **Extended Access Lists**
    - **Assigning Standand list on variours intefaces**
    - **Different protocols and port no**
- **NATTING**
  - **Dynamic NAT**
  - **Static NAT**
  - **PAT**
- **IPv6**
- **VPN**
  - ✓ **What is VPN**
  - ✓ **Types of VPN**
  - ✓ **Advantages of VPN**
  - ✓ **VPN protocols (L2 and L3)**

OSI Reference Model

Layer of OSI model

- **Application layer**
- **Presentation layer**
- **Session layer**
- **Transport layer**
- **Network layer**
- **Data link layer**
- **Physical layer**

Switching

- **Differences among HUB, Repeater , Bridge and Switch**
- **Broadcast and collision domain**
- **Function of a switch**
- **Types of switches**
    - **Manageable Switches**
    - **Unmanageable Switches**
- **Series of switches**
- **Configuration and modes of Switches**
- **Switch port modes**
    - **Access port**
    - **Trunk port**
- **Trunking Protocols**
    - **ISL**
    - **802.1q**

-
- **What is VLAN**

- **Types of VLAN**
  - **Static VLAN**
  - **Dynamic VLAN**
- **VTP (Vlan trunking Protocol)**
- **Modes of VTP**
  - **Server**
  - **Client**
  - **Transparent**
- **STP and Advance STP**
- **CDP**

Basic Network Devices

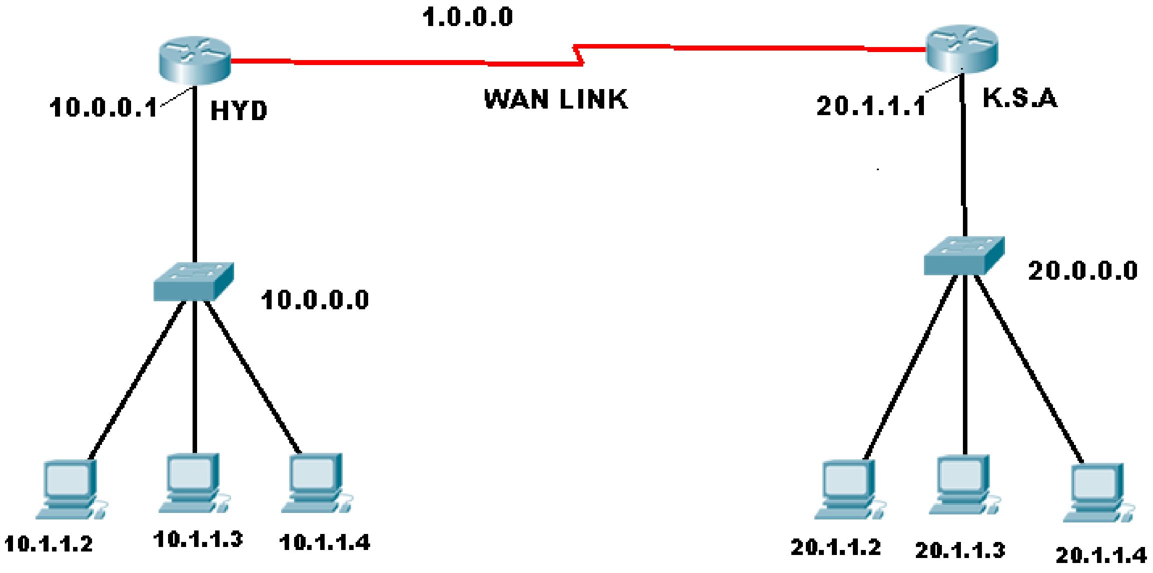
Router

- ✓ It is an internetworking device used to connect two or more different networks
- ✓ It works on layer 3 i.e. network layer
- ✓ Routers divide larger network into logically designed network

It does two basic things

- ❖ Select the best path from the routing table
- ❖ Forward the packet on that path.

Example (Router makes it possible to connect two different networks)



HYD and K.S.A are two routers connecting two different sites via WAN (Wide Area Network)

- ✓ HYD LAN is in **10.0.0.0** network
- ✓ K.S.A LAN is in **20.0.0.0** network
- ✓ WAN Link is in **1.0.0.0** network

Note: - Every Interface of the Router Must Have Different Network Address Else Communication Will Not Happen

Hub

- ✓ It's a layer one device (Physical Layer)
- ✓ It's not an intelligent device
- ✓ Every time when it receive the frame it does broadcast
- ✓ It uses CSMA/CD
- ✓ It works on shared bandwidth
- ✓ It does half duplex transmission

- ✓ It has one broadcast domain
- ✓ It has one collision domain

Switch

- ✓ It a layer 2 device (Data Link Layer)
- ✓ It is an intelligent device
- ✓ Works on MAC (media access control) addresses
- ✓ It maintains CAM (content addressable memory: A switch's CAM table contains network information such as MAC addresses available on physical switch ports and associated VLAN parameters.) table
- ✓ It has one broadcast domain
- ✓ Each port is consider as one collision domain
- ✓ Number of port is equal to number of collision domain
- ✓ It works on full duplex
- ✓ It uses hardware called ASIC (Application Specific Integrated Circuit) which makes switch much faster.

Note:-Bridges and Switches both are layer 2 works on MAC address but bridges are software base switching and Switches are hardware switching base (I.e. ASIC) Hardware base switching is faster than software base switching.

What is TCP/IP?

TCP/IP is a standard language like English used by computers and network devices for communication

TCP/IP is a universal standard and can make communication possible among all operation system.

The **Internet Protocol Suite** (commonly known as **Transmission Control Protocol and Internet Protocol**) is the set of communications protocols used for the Internet and other similar networks.

TCP/IP for communication use **IP Address**

What is IP ADDRESS?
An Internet Protocol (IP) address is a numerical identification and logical address that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication.
IP Address is divided into two portions
1) Network portion
2) Host portion
It has two versions
1) IPv4 (32 bits)
2) IPv6 (128 bits)
What is Subnet mask?

It’s an address used to identify the network and host portion of the IP address

What is Default gateway?
It’s the Entry and Exit point of the network.
1. It’s the LAN/Ethernet IP address of a router.
2. IP address and the default gateway should be in the same network.
3. The default gateway is used only to communicate with other/foreign.

What is subnetting?
Logically dividing one network into smaller networks is called as subnetting or VLSM. One subnet can be subnetted for multiple times for efficient use.

Subnetting (VLSM variable length subnet mask) is used for proper implementation of IP addresses which allows more than one subnet mask for a given network according to the individual needs.

What is Supernetting or CIDR?

Classless Inter-Domain Routing (**CIDR**) merges or combine network addresses of same class into one single address to reduce the size of the routing table.

It is done on core router to reduce the size of routing table.

It is implemented by ISP (internet service providers).

Private Ip

- 0.0.0.0/8 (10.0.0.0 to 10.255.255.255)
- 172.16.0.0/12 (172.16.0.0 to172.31.255.255)
- 192.168.0.0/16 (192.168.0.0 to192.168.255.255)
- 169.254.0.0/16 (169.254.0.0 to169.254.255.255)*

*Note that169.254.0.0/16 is a block of private IP addresses used for random self IP assignment where DHCP servers are not available.

IP Addressing

IP Addressing Rules

- It is a 32 bit dotted decimal number with 4 octets, each octet of 8 bits.
- It is divided into two portions, Network and host portion
- IP addresses must be unique in a network
- 32 bits divided into 4 octets
- Each octet has a decimal value range of 0 to 255.
- The network portion can not be all 0’s nor all 1’s
- The first octet can not be 127 (network), this is reserved for loopback
- The host portion can not be all 0’s – this defines the network address
- The host portion can not be all 1’s – this defines a broadcast in that particular network
- The IP address 255.255.255.255 defines a general broadcast
- Although IP addresses are stored as binary numbers, they are usually displayed in human-readable notations, such as 208.77.188.166 (for IPv4)
- The original designers of TCP/IP defined an IP address as a 32-bit number and this system, now named Internet Protocol Version 4 (IPv4), is still in use today.

Useful Statistics

Class	**1st octet range decimal**	**1st octet structure binary**	**Total Number of networks**	**Maximum Number of hosts/network**	**Address Structure**	**Default Subnet Mask**
A	1 – 127	0xxxxxxx	2^7-2 126	2^{24}-2 16,777,214	N.H.H.H	255.0.0.0
B	128 – 191	10xxxxxx	2^{14} 16,384	2^{16}-2 65,534	N.N.H.H	255.255.0.0
C	192 – 223	110xxxxx	2^{21} 2,097,152	2^8-2 254	N.N.N.H	255.255.255.0
D	224 – 239	1110xxxx	Reserved for multicasting			
E	240 - 255	1111xxxx	Reserved for experimental and future use			

- N = Network portion and H = Host portion

Variable-Length Subnet Mask

Definition

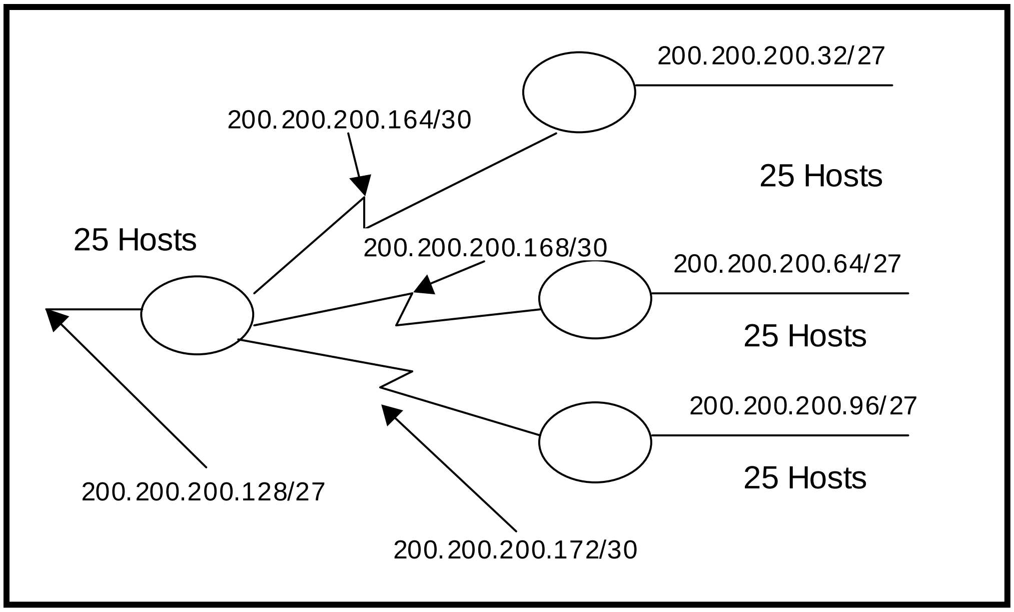
Variable-Length Subnet Mask (VLSM):

- VLSM is used for proper implementation of IP addresses which allows more than one subnet mask for a given network according to the individual needs
- Logically dividing one network into smaller networks is called as subnetting or VLSM.
- One subnet can be subnetted for multiple times for efficient use.
- Requires Classless Routing Protocols.

Advantages

Efficient Use of IP addresses: Without VLSMs, networks would have to use the same subnet mask throughout the network. But all your networks don't have the same number of hosts.

Example of a VLSMs Networks



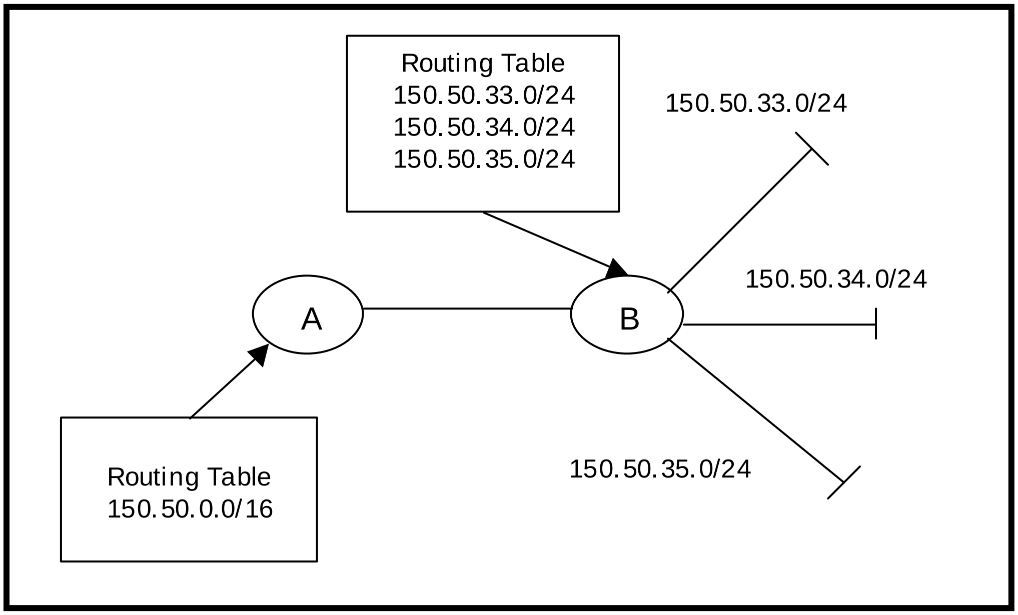
Route Summarization (CIDR)

Definition

Route Summarization: reduces the number of routes that a router must maintain because it represents a series of network numbers in a single summary address.

Advantages

- Reduces the size of Routing Tables
- Isolates Topology changes from other routes in a Large Network



Router Basics

What is a Router?
It is an internetworking device used to connect two or more different networks
It works on layer 3 i.e. network layer.

It does two basic things:-

1. Select the best path from the routing table.
2. Forward the packet on that path.

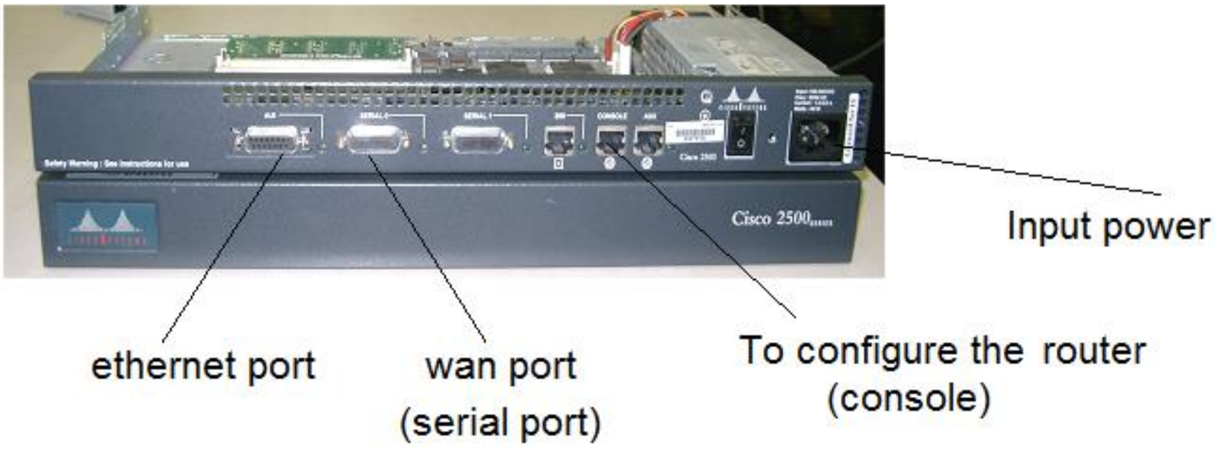
Router types

1. Fixed router (Non Upgradable cannot add and remove the Ethernet or serial interfaces)
2. Modular router (Upgradable can add and remove interfaces as per the requirement)

CISCO Router models/series

- 1700
- 1800
- 2500
- 2600
- 2800
- 3200
- 3600
- 3700
- 3800
- 4000
- 7200
- 10000
- 12000

External Components of Cisco Router



Serial interface

It is used for WAN connection
From serial interface usally V.35 cable is connected to the modem

Ethernet interface or AUI (Attach Unit Interface)

Used for LAN connection
Connection from switch is connected to Ethernet port
IP address on this interface is considered as default gateway for LAN users.
It can be Ethernet, fast Ethernet or giga Ethernet
In old router it was named as AUI, in the new routers we have RJ-45 Ethernet port

Console port

It is administration port for router
It is used for initial configuration of the router.
It is also used for password recovery
Rollover cable/Console cable is used to connect the router console port to the system COM port for initial configuration

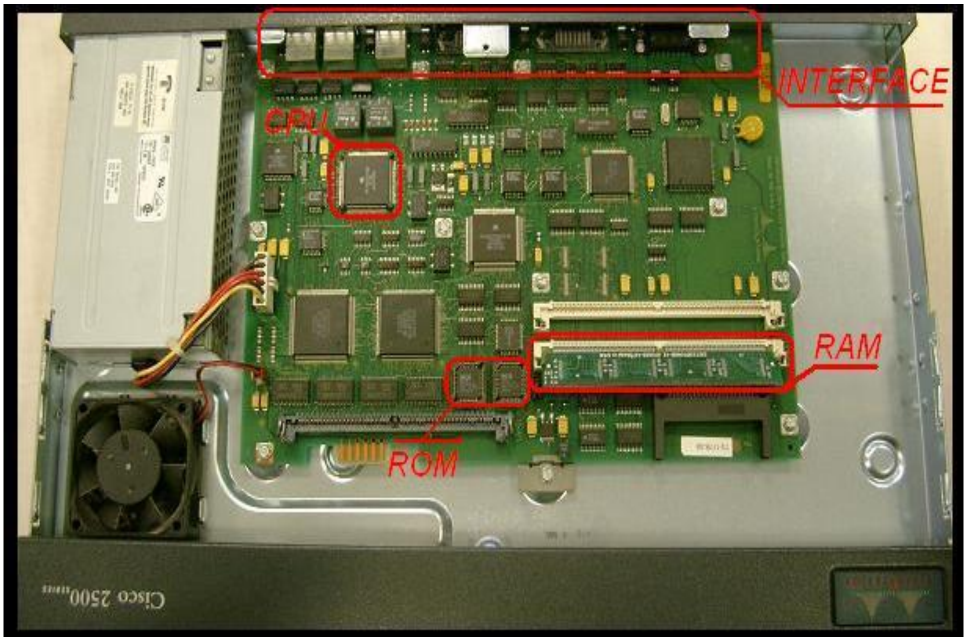
Auxiliary Port

It is also used for remote administration using PSTN line & modem

Power supply

It also has small SMPS which is used to give the constant DC power to the router.

Internal Components of Router



- **RAM**
  Contains dynamic / running configuration
- **NVRAM**
  Contains backup of configuration (startup configuration)
- **Flash**
  Contains copy of Cisco IOS (Internet Operating System)
- **ROM**
  Contains a subset of IOS (mini IOS)
  Contains bootable IOS image

Router Start-up Sequence

1. The router performs a POST. The POST tests the hardware to verify that all components of the device are operational and present. For example, the POST checks for the different interfaces on the router. The POST is stored in and run from ROM (read-only memory).

2. The bootstrap looks for and loads the Cisco IOS software. The bootstrap is a program in ROM that is used to execute programs. The bootstrap program is responsible for finding where each IOS program is located and then loading the file. By default, the IOS software is loaded from flash memory in all Cisco routers.

3. The IOS software looks for a valid configuration file stored in NVRAM. This file is called startup-config and is only there if an administrator copies the running-config file into NVRAM.

4. If a startup-config file is in NVRAM, the router will load and run this file. The router is now operational. If a startup-config file is not in NVRAM, the router will start the setup-mode configuration upon bootup.

1.

Routers can be configured from:-

1. Console terminal
2. Auxiliary port – externally, via modems
3. Virtual terminals (Telnet) – after installation

Router Modes

❖ **User EXEC mode** (look, but don't change)

Automatically enter this mode when router is turned on

You can perform basic tasks, such as connect to remote devices, and perform basic tests

Prompt: Router>

❖ **Privileged EXEC mode**

High-level testing commands

Set operating parameters

Command to enter: Router>enable

Prompt: Router#

- **Global configuration mode**

  Commands apply to features that affect the system as a whole
  Enter from privileged EXEC mode with command:
  Router#config t

  Prompt: Router (config) #

- **Interface mode**

  Configure interface, such as Ethernet, serial
  Enter from global configuration mode with command:

  Router (config)#int e 0/0 Or Router (config)#int s 0/0

  Prompt: Router (config-if) #

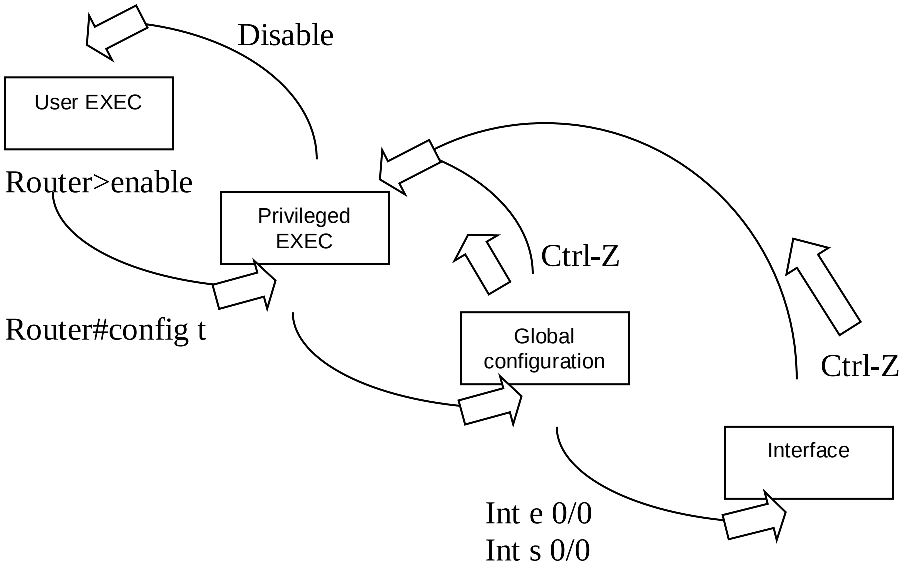
- **Setup mode**

  Helps new user to create a configuration for the first time, via a series of questions
  Prompted at bootup or enter **setup** at router# prompt

- **Rommon mode**

  Provides router with a small subset of IOS and helps router boot if IOS not found in Flash

Prompt: Rommon 1>



Router Configuration Commands

❖ Editing commands

Ctrl-A	beginning of line
Ctrl-E	end of line
Ctrl-F	forward one character
Ctrl-B	back one character
Esc-F	forward one word
Esc-B	back one word

❖ Command History

Router #show history

- Enabled by default
- 10 commands recorded in history buffer by default
- Use history size command to change to a maximum of 256
- Ctrl-P or Up arrow shows most recent
- Show history command at privileged EXEC mode shows if enabled and history size
- Tab keys completes entries of known keywords

1. Setting Router Name

Router (config) #hostname (*desired_name*)

2. Welcome Banner

Displayed when router is accessed
Displayed prior to prompting for a password

Syntax : Router(config)#**banner motd** #*message*#

3. Saving Configurations Changes

To save running (active) configuration to startup configuration for availability at next bootup

Router#copy running-config startup-config

4. To delete startup configuration

Router#erase starup-config

Router Status Commands

- **Show version**
  Shows IOS configuration
  Image file name and location
  How long router is up and active
- **Show startup-config**
  Shows image size
  Shows backup configuration file
- **Show running-config**
  Shows current, active configuration
- **Show interfaces**
  Shows statistics/parameters for all configured interfaces
- **Show flash**
  Shows information on Flash memory device
- **Show ip interface brief**
  Show the assigned ip address and status of the interfaces

Securing Router Access Through Passwords

```
Router(config)#line console 0
Router (config-line) #login
Router (config-line) #Password cisco123
```

Setting an Enable Mode Password

```
Router (config) #enable password cisco123
```

Setting an Encrypted Enable Mode Password

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

Setting Telnet Password

```
Router (config) #line vty 0 4
Router (config-line) #login
Router (config-line) #Password cisco123
```

Difference between enable password and enable secret password

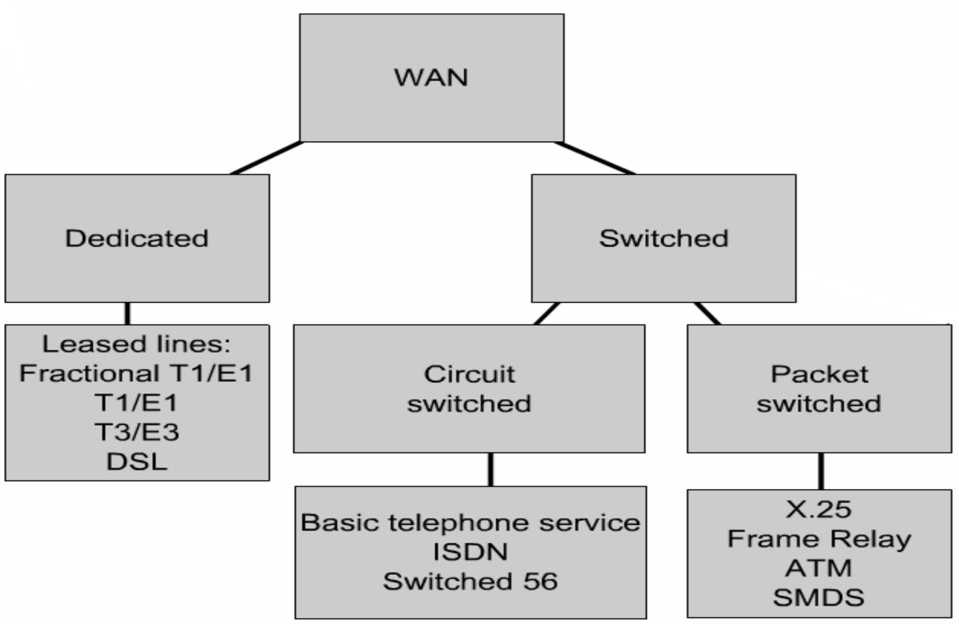
1. Enable secret is a secure password keeps the password encrypted in the configuration.
2. Whereas enable password is clear text no security
3. Enable secret has more priority and preference over enable password

4. If both the passwords are configured enable secret password will be active and enable password becomes useless

WAN Connectivity

WAN connections are divided into three types

1) Dedicated line
2) Circuit switched
3) Packet switched



\

Dedicated line:-

- ✓ Permanent connection for the destination
- ✓ Used for short or long distance
- ✓ Bandwidth is fixed
- ✓ Availability is 24/7

- ✓ Charges are fixed whether used or not.
- ✓ Uses analog circuits
- ✓ Always same path is used for destination
- ✓ Example is Leased Line

Circuit switched:-

- ✓ It is also used for short and medium distances.
- ✓ Bandwidth is fixed
- ✓ Charges depend on usage of line
- ✓ Also called as line on demand.
- ✓ Usually used for backup line
- ✓ Connects at BRI port of router

ISDN and PSTN are the examples

Packet switched:-

- ✓ Used for medium or longer connections
- ✓ Bandwidth is shared
- ✓ Many virtual connections on one physical connection

Example: - Frame Relay

Leased line: - A permanent /dedicated physical connection which is used to connect two different geographical areas. This connection is provided by telecommunication companies like BSNL in India.

Leased line provides service 24/7 through out the year, not like Dial-up Connection which can be connected when required. Leased Lines are obtained depending on the annual rental basis. Moreover, its rent depends on the distance between the sites.

Leased Line is of three types

1) Short Leased Line
2) Medium Leased Line
3) Long Lease Line (IPLC)

Short leased line which is used with in the city and cost is also less for it.

Medium leased line is used to connect sites in two different states like Hyderabad and Chennai.

Long Leased Line also called as IPLC. It stands for International private lease circuit uses to connect two different countries. It’s the most expensive among all.

I. Leased Line provides excellent quality of service with high speed of data transmission.
II. As it's a private physical connection assures complete security and privacy even with voice.
III. Speed of the leased line varies from 64 kbps to 2 Mbps or more. Always Leased Line has fixed bandwidth.

Note:-
Once leased line is setup not only we can send data but transmission of voice is also possible. In addition to this, both voice and date can be sent simultaneously.

Coming to the hardware requirements

1) **Leased Line Modem**
2) **V.35 connector & cable**
3) **G.703 connector & cable**

Leased line Modem also called as CSU/DSU (Channel Service Unit and Data Service Unit). It acts as a DCE device which generates clock rate.

Note: - while practicing labs we use V.35 cable for back to back connection with router where as in real time V.35 cable terminates at the Lease Line Modem. That's the reason we have to use clock rate command in the labs where as it's not require in the real scenario. CSU/DSU is used to generate the speed.

In different countries different codes are used for Leased Line with different speeds. In Europe its is identified as E whereas in UK its is identified with letter T

In Europe, there are five types of lines distinguished according to their speed:

- E0 (64Kbps),
- E1 = 32 E0 lines (2Mbps),
- E1 = 128 E0 lines (8Mbps),
- E3 = 16 E1 lines (34Mbps),
- E4 = 64 E1 lines (140Mbps)

In the United States, the concept is as follows:

- *T1* (1.544 Mbps)
- *T2* = 4 T1 lines (6 Mbps),
- *T3* = 28 T1 lines (45 Mbps),
- *T4* = 168 T1 lines (275 Mbps)
-

Advantages	**Disadvantages**

○ Complete secure ○ High Bandwidth ○ High speed connection ○ Superior quality ○ Reliable	○ Expensive ○ Permanent physical connection

WAN Protocols

Leased Lines uses two types of WAN encapsulation protocols:

1) High Data Link Protocol (HDLC)
2) Point to Point Protocol (PPP)

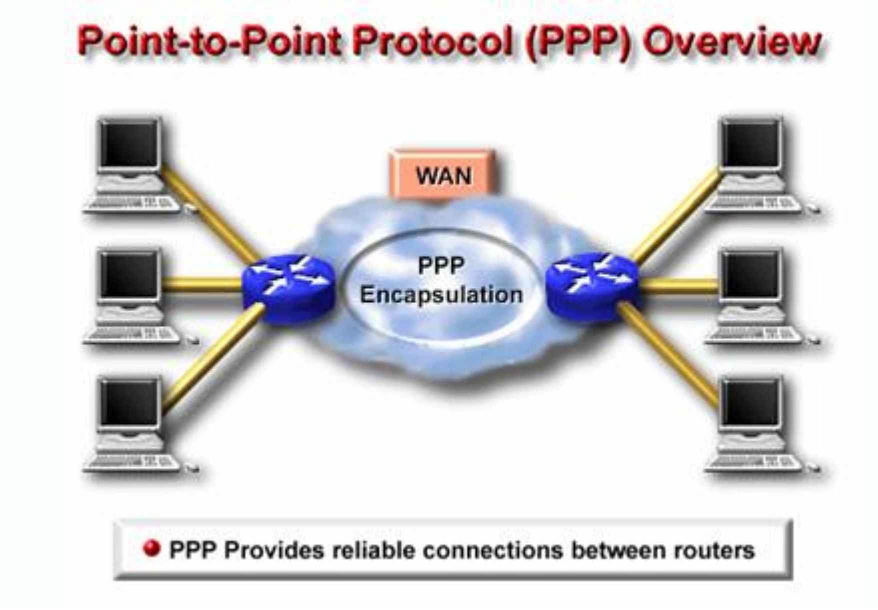
<u>HDLC Encapsulation:-</u>

- HDLC (High-level Data Link Control) is a CISCO proprietary.
- It is a default setting for CISCO routers in serial interfaces.
- It is used whenever you are going to connect a serial circuit with CISCO routers across the entire network.
- HDLC doesn’t support authentication and compression.
- HDLC protocol is faster than PPP.
- If both ends of a leased-line connection are routers running Cisco IOS software, HDLC encapsulation is typically used.
- Cisco HDLC is a point-to-point protocol that can be used on leased lines between two Cisco devices.
- If the serial interface is configured with another encapsulation protocol, use the *encapsulation hdlc* command to specify the encapsulation protocol on the interface.

<u>Configuration of HDLC:-</u>

```
Router(config)#interface serial 0/0
Router(config-if)#encapsulation hdlc
```

Note: - In point to point links both sides protocols must be same like HDLC-HDLC and PPP-PPP.
If the protocols mismatch then in “show interface x.x” *command line protocol down* message will appear.


Point-to-Point Protocol (PPP) Overview
WAN
PPP
Encapsulation
PPP Provides reliable connections between routers

- ✓ PPP (Point to Point Protocol) is a standard encapsulation.
- ✓ PPP encapsulation provides Cisco IOS software to devices that are not running Cisco IOS software connectivity over leased WAN lines.
- ✓ It is a little more complex than HDLC.

PPP Features:-
1) Authentication
2) Multilink
3) Compression

PPP is made up of two sub-protocols:-
1)Link Control Protocol - Used for establishing the point-to-point link.
2)Network Control Protocol - Used for configuring the various network layer protocols.

Link Control Protocol (LCP)
Link-establishment :- In this process frames are used to establish and configure a link
Link-termination:-In this process frames are used to terminate a link
Link-maintenance:-In this process frames are used to manage and debug a link

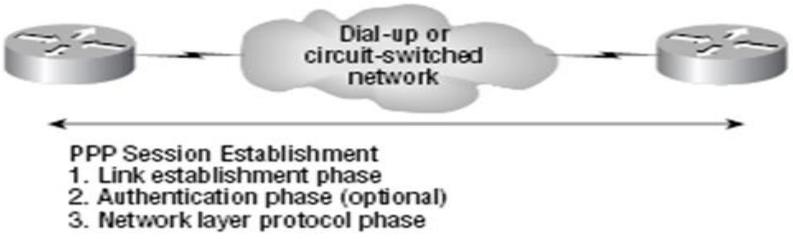
Network Control Protocol (NCP)
PPP uses the Network Control Protocol (NCP) component to specify, encapsulate and negotiate options for multiple network layer protocols.

For every network layer protocol used, a separate Network Control Protocol (NCP) is provided.

For example, Internet Protocol (IP) uses the IP Control Protocol (IPCP), and Internetwork Packet Exchange (IPX) uses the Novell IPX Control Protocol (IPXCP).

PPP session establishment

When PPP connections are started, the links go through three phases of Session establishment.

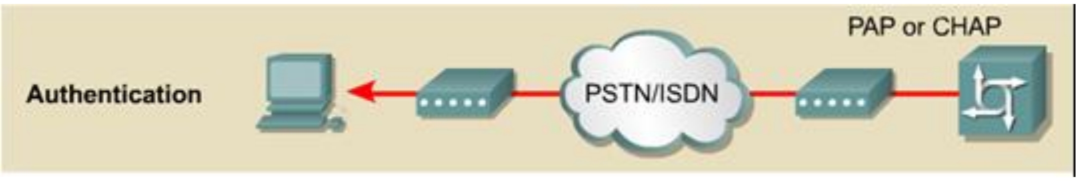

Dial-up or circuit-switched network
PPP Session Establishment
1. Link establishment phase
2. Authentication phase (optional)
3. Network layer protocol phase

Link-establishment phase LCP packets are sent by each PPP device to configure and test the link. These packets contain a field called the Configuration Option that allows each device to see the size of the data, compression, and authentication. If no Configuration Option field is present, then the default configurations are used.

Authentication phase If required, either CHAP or PAP can be used to authenticate a link. Authentication takes place before Network layer protocol information is read. It is possible that link-quality determination may occur at this same time.

Network layer protocol phase PPP uses the *Network Control Protocol (NCP)* to allow multiple Network layer protocols to be encapsulated and sent over a PPP data link. Each Network layer protocol (e.g., IP, IPX, and AppleTalk, which are routed protocols) establishes a service with NCP.

PPP supports two authentication protocols:
1) PAP (Password Authentication Protocol)
2) CHAP (Challenge Handshake Authentication Protocol)

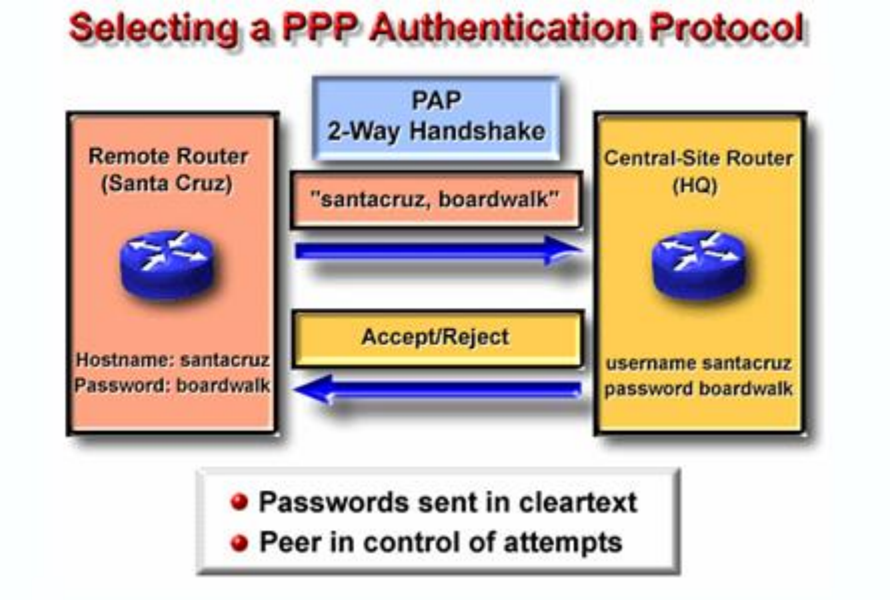


PAP (Password Authentication Protocol)

- PAP provides a simple method for a remote node to establish its identity using a two-way handshake.
- PAP is done only upon initial link establishment

After the PPP link establishment phase is complete:

- A username/password pair is repeatedly sent by the remote node to the router until authentication is acknowledged, or the connection is terminated.
- PAP is not a strong authentication protocol.
- Passwords are sent across the link in clear text.
- There is no protection from playback or repeated trial-and-error attacks.
- The remote node is in control of the frequency and timing of the login attempts.



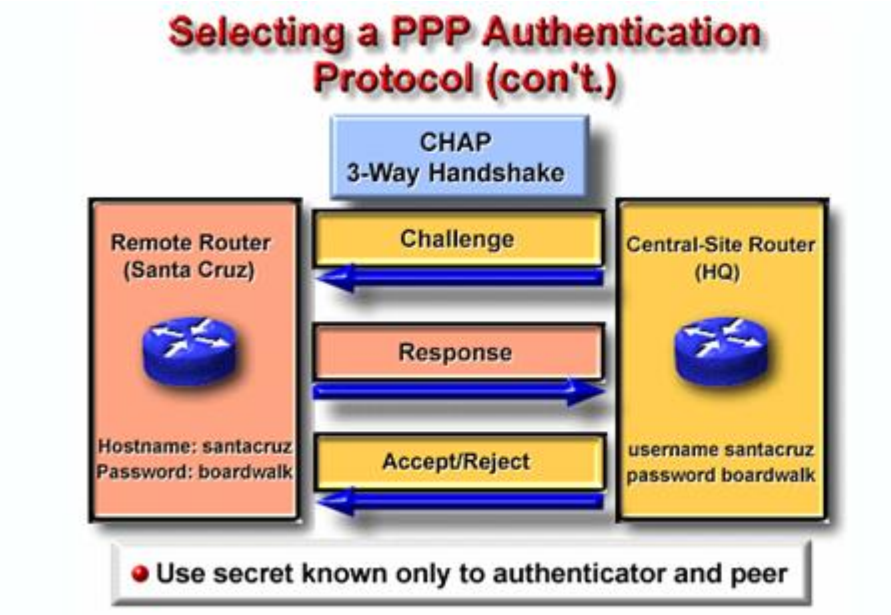
CHAP (Challenge Handshake Authentication Protocol)

- After the PPP link establishment phase is complete, the local router sends a unique “challenge” message to the remote node.
- The remote node responds with a value (MD5)
- The local router checks the response against its own calculation of the expected hash value.
- If the values match, the authentication is acknowledged. Otherwise, the connection is terminated immediately.

Advantages

- ➢ CHAP provides protection against playback attack through the use of a variable challenge value that is unique and unpredictable.

- The use of repeated challenges is intended to limit the time of exposure to any single attack.
- The local router is in control of the frequency and timing of the challenges.



Selecting a PPP Authentication Protocol (con't.)

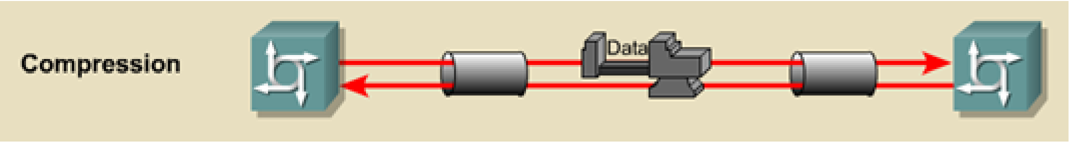
- Use secret known only to authenticator and peer

Configuration of PPP protocol

The following example enables PPP encapsulation on serial interface 0/0:

```
Router#configure terminal
Router(config)#interface serial 0/0
Router(config-if)#encapsulation ppp
```

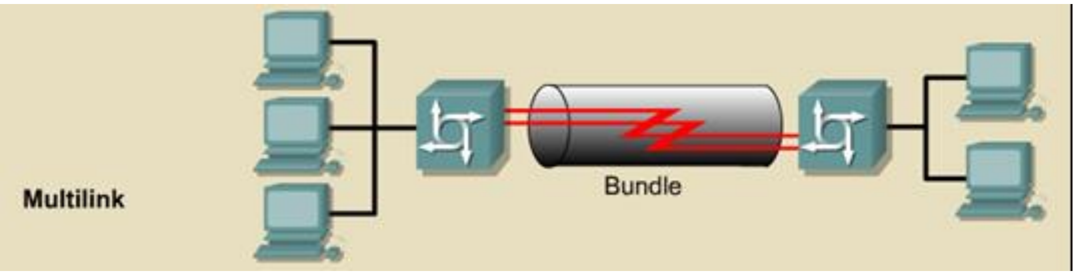
Configuring PPP Compression



To configure compression over PPP, enter the following commands:

```
Router(config)#interface serial 0/0
Router(config-if)#encapsulation ppp
Router(config-if)#compress [predictor | stac]
```

Configuring PPP Multilink

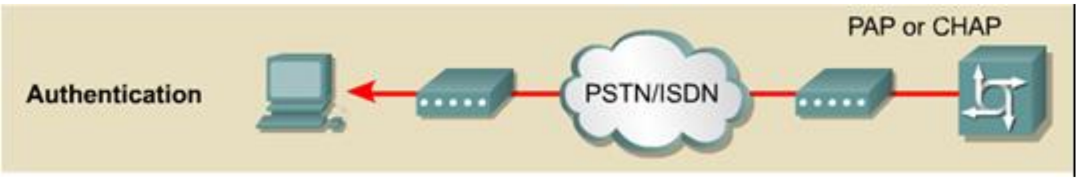


The following commands perform load balancing across serial s0/0 and s0/1 multiple links:

```
Router(config)#interface serial 0/0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp multilink 1
Router(config)#interface serial 0/1
Router(config-if)#encapsulation ppp
Router(config-if)#ppp multilink 1

Router(config)# interface multilink 1
Router(config-if)#ip address 1.1.1.1 255.0.0.0
Router(config-if)#
```

Configuring PPP Authentication



Enable CHAP Authentication

```
Router(config)#interface serial 0/0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp authentication chap
```

Enable PAP Authentication:-

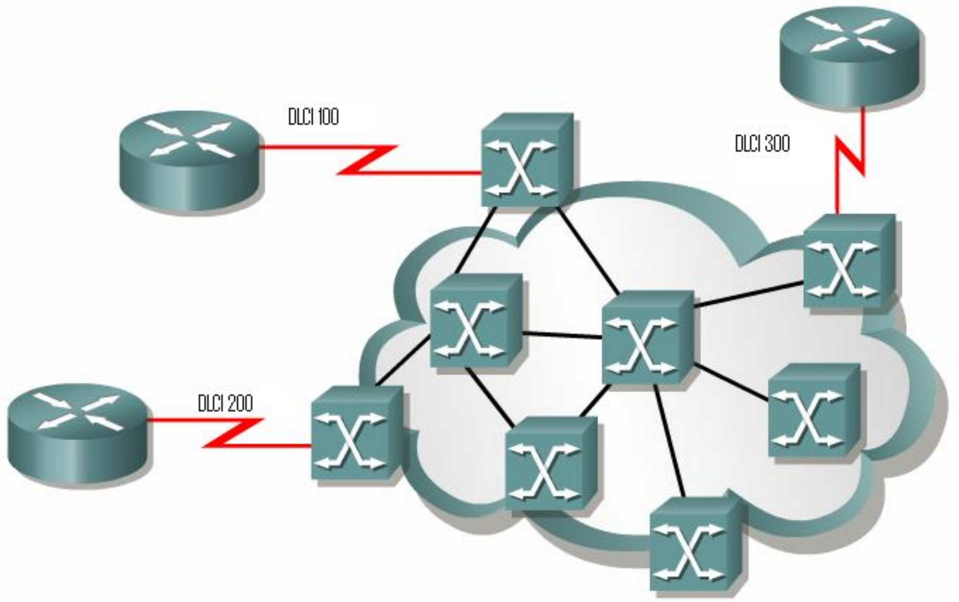
```
Router(config)#interface serial 0/0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp authentication pap
```

Difference Between HDLC and PPP

HDLC	PPP
Higher level data link Control protocol	Point to Point Protocol
Cisco Proprietary Layer 2 WAN Protocol	Standard Layer 2 WAN Protocol
Doesn’t support Authentication	Supports Authentication
Doesn’t support Compression and error correction	Support error correction
Doesn’t support Multilink	Support Multilink

FRAME RELAY

- ✓ Frame Relay is a connection oriented, standard NBMA layer 2 WAN protocol
- ✓ Connections in Frame Relay are provided by Virtual circuits.
- ✓ Virtual circuits are multiple logical connections on same physical connection



Frame Relay virtual connection types.

a) PVC
b) SVC

A) **PVC (permanent virtual connection):-**

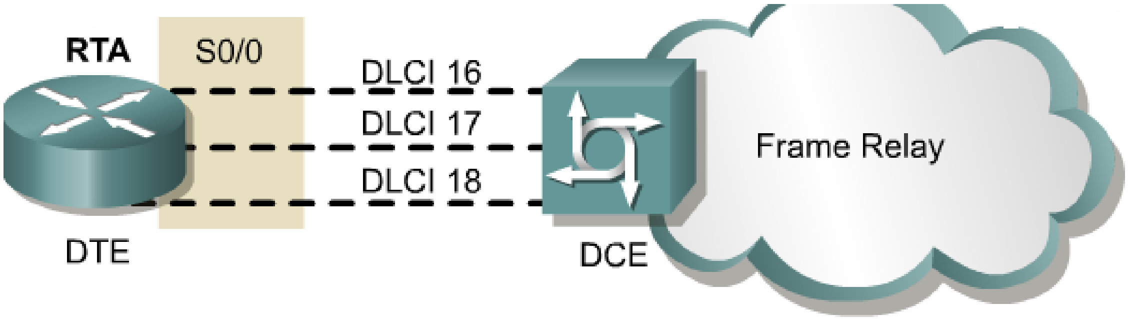
- ✓ Similar to the dedicated leased line.
- ✓ Permanent connection is used.
- ✓ When constant data has to be sent to a particular destination.
- ✓ Always use the same path.

B) **SVC (switched virtual connection)**

- ✓ Virtual connection is dynamically built when data has to be send and torn down after use.
- ✓ It is similar to the circuit switched network like dial on demand.
- ✓ Also called as semi-permanent virtual circuit.
- ✓ For periodic intervals of data with small quantity

There are two types of Frame relay encapsulations
1. Cisco (default and Cisco proprietary)
2. IETF (when different vendor routers are used)

DLCI (data link connection identifier):-



- ✓ Address of Virtual connections
- ✓ For every VC there is one DLCI number.
- ✓ Locally significant and provided by Frame Relay service provider.
- ✓ Inverse ARP (address resolution protocol) is used to map local DLCI to a remote IP.

<u>LMI (Local management interface):-</u>

LMI allows DTE (router) to send status enquiry messages (keep alive)to DCE (frame relay switch) to exchange status information about the virtual circuits devices for checking the connectivity.

Frame relay LMI types?

1. CISCO (Default)
2. ANSI
3. Q933A

Note:- On Cisco router LMI is auto sense able no need to configure

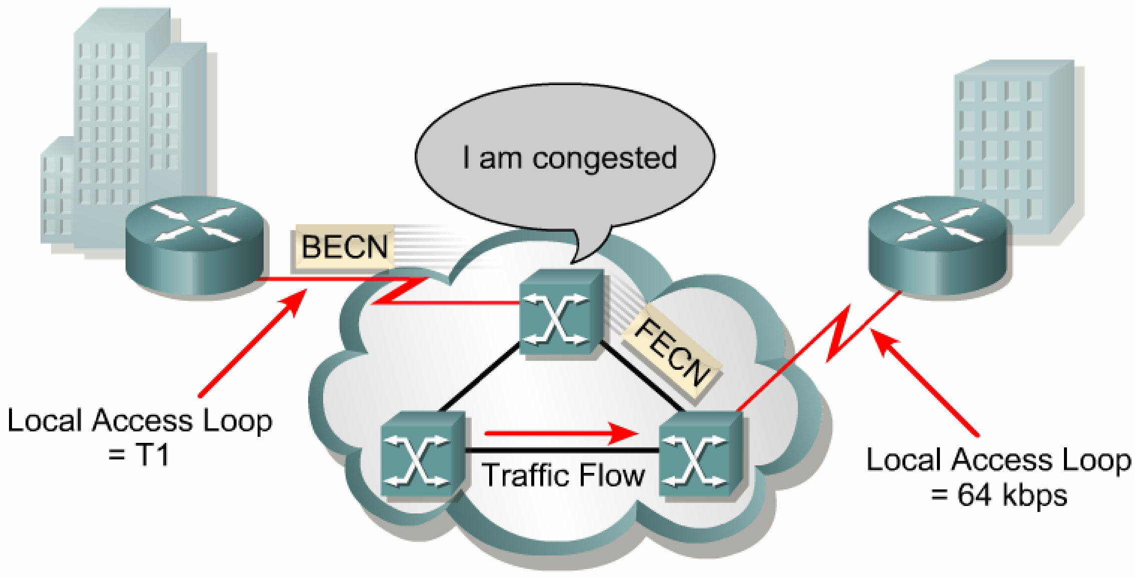
Frame relay **virtual connection status types**:-
1) **Active**: - Connection is up and operation between two DTE's exist
2) **Inactive**: - Connection is functioning between at least between DTE and DCE
3) **Deleted**: - The local DTE/DCE connection is not functioning.

DLCI (data link connection identifier):-

- ✓ Address of Virtual connections
- ✓ For every VC there is one DLCI number.
- ✓ Locally significant and provided by Frame Relay service provider.
- ✓ Inverse ARP (address resolution protocol) is used to map local DLCI to a remote IP.

Frame relay network connections.
1)Point to Point
2)Point to Multipoint (NBMA)

Congestion indicates traffic problem in the path when more packets are transmitted in one direction.



Congestion notifications
1) FECN (forward explicit congestion notification)
2) BECN (backward explicit congestion notification)

FECN

- ✓ Indicates congestion as frame goes from source to destination
- ✓ Used this value inside frame relay frame header in forward direction
- ✓ FCEN =0 indicates no congestion

BECN

- ✓ Used by the destination (and send to source) to indicate that there is congestion.
- ✓ Used this value inside frame relay frame header in backward direction
- ✓ BCEN =0 indicates no congestion

ADVANTAGES

- ✓ VC’s overcome the scalability problem of leased line by providing the multiple logical circuits over the same physical connection
- ✓ Cheaper
- ✓ Best quality
- ✓ VC’s are full duplex

Routing Protocols

Routing?

- Forwarding of packets from one network to another network choosing the best path from the routing table.
- Routing table consist of only the best routes for every destinations.
- By default router will have the directly connected networks in the routing table
- To check the routing table of a router issue “show ip route” command.

Note: - Nature or the Behavior of the routers is, it drops the packet when destination address information is not available in the routing table.

Types of Routing?

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

Routing Tables

- Routers build routing tables initially based on their directly connected networks.
- In addition to directly connected networks, Routers can learn about destinations in one of three ways:
  - **Static Routes**: Manually added to the routing tables by the administrator.
  - **Default Routes**: Manually added to the routing table by the administrator to define a Default Gateway for the router.
    If the routing table does not have an entry for a destination network, send the packet to the Default Route.
  - **Dynamic routes** learned automatically through dynamic routing Protocol.
- Routing tables are used to send data along specific paths to reach a particular destination.
- Routers need to exchange routing tables so they can route data to networks that are not directly connected to them.
- Routers require a ***Routing Protocol*** in order to exchange routing tables with their neighboring routers and advertise networks.

Static Routes

- Static Routes are User-defined, manually created routes
- Destination address must be known to configure static route
- Administrative distance is **1**
- ***IP Route*** Command is used to configure.
- Used for small organization
- Provides security and fast

Syntax: **ip route** *destination-network subnet-mask Next-Hop-Router-IP-Address* {distance}

Example: ip route 11.0.0.0 255.0.0.0 10.0.0.2

Default Routes

- Manually adding the single route for all the destination. Default route is used when destination is unknown
- Last preferred route in the routing table
- Configure for stub and internet routes
- When there is no entry for the destination network in a routing table, the router will forward the packet to its default router.
- Default routes help in reducing the size of your routing table.

Syntax: **ip route 0.0.0.0 0.0.0.0 *next-hop-router or exit interface***

Example: ip route 0.0.0.0 0.0.0.0 10.0.0.2 or s0

Routing Protocols

- A ***Routable Protocol*** is a network protocol that transports data across a network with a structure, which allows it to be routed to the specified destination network.
- A ***Routing Protocol*** is a method by which routers exchange information about the networks they can reach. Exchange of information allows routing tables to be built and exchanged. The process of updating routers is called ***convergence***.
- Routing Protocols determine the best path for the transport of data using some criteria, such as distance or metric. Examples include bandwidth, delay, hops and reliability.

<u>Routing Protocols are divided into two types</u>

- **Interior Routing Protocol (Used within the AS(Autonomous System))**
  - ✓ Routing Information Protocol(RIPv1 and RIPv2)
  - ✓ Interior Gateway Routing Protocol(IGRP)
  - ✓ Open Shortest Path First(OSPF)
  - ✓ Enhanced Interior Gateway Routing Protocol(EIGRP)
- **Exterior Routing Protocols include(Used between the AS)**
  - ✓ Border Gateway Protocol(BGP)
  - ✓ Exterior Gateway Protocol(EGP)

Types of Interior Routing Protocols

- **Distance Vector Protocol**
- **Link State protocol**
- **Hybrid Protocol**

Dynamic Routing Protocol

- Need to configure only directly connected network
- Provides scalability so can be used for major corporate
- No need to know destination address
- Administrative work is reduce
- Neighbor routers exchange routing information and build the routing table automatically.
- Network changes are automatically updated

Distance Vector Protocol

- The Routing update includes the entire routing table.
- Uses Bellman Ford algorithm
- It uses a periodic update.
- Routing Update packets are sent as broadcast. Unicast packets can also be specified.

Examples of Distance Vector Routing Protocols are RIP 1, RIP 2, IGRP

Link State Routing Protocols

- The Routing updates include only new changes to the routing table which saves bandwidth.
- Works on Dijikstra or SPF (shortest path first) algorithm
- Handles larger networks and is more scalable than Distance Vector Routing Protocols.
- Classless routing protocol
- Works on multicast address
- Example OSPF, IS-IS

Hybrid Protocol

- Works on DUAL algorithm
- It’s a Cisco proprietary
- Classless routing protocol
- Also called as Advance Distance Vector Protocol
- Uses multicast address for sending updates
- Trigger or incremental updates are used

  Example: - EIGRP

Administrative Distance

- Rating of the Trustworthiness of a routing information source.
- The Number is between 0 and 255
- The higher the value, the lower the trust. For example, 255 signify no trust and therefore are ignored.
- Lowest administrative distance is always chosen as the routing protocol to use to transport data.
- Default administrative distances are as follows :
  - **Directly Connected = 0**
  - **Static Route = 1**
  - **IGRP = 100**
  - **OSPF = 110**
  - **RIP = 120**
  - **EIGRP = 90/170**

Autonomous System

An autonomous system is one network or sets of networks under a single administrative control. An autonomous system might be the set of all computer networks owned by a company, or a college.
The AS number will be from 1 to 64511
PRIVATE AS NUMBERS (64512 - 65535)

Routing Information Protocol (RIP)

- Distance Vector protocol
- Works on Bellman Ford Algorithm
- Open standard
- Administrative distance is 120
- Metric is hop count
- Classful routing protocol
- Supports 4 equal cost load balancing

- Operating from UDP port 520
- Maximum hop count is 15, 16th hop is unreachable
- Periodic Updates are sent
- Exchange entire routing table for every 30 second
- Works on broadcast address 255.255.255.255

RIP Version 2

- Classless routing protocol
- Supports VLSM
- Auto summary can be done on every router
- Supports authentication
- Trigger updates
- Uses multicast address 224.0.0.9.
- Uses Split horizon technique, Root poisoning and Hold down timers for loop avoidance.

Advantages of RIP

- Easy to configure
- No design constraints
- No complexity
- Less overhead

Disadvantage of RIP

- Bandwidth utilization is very high as broadcast for every 30 second
- Works only on hop count
- Not scalable as hop count is only 15
- Show convergence
- Routing loops are formed

RIP Timers

- Update timer
- Invalid timer
- Holddown timer
- Flush timer

Update timer:-
It is a time period between two updates .For every 30 second whole routing table is sent on the broadcast address 255.255.255.255.

Invalid timer:-
If the updates don’t come from the neighbor for 180 second i.e. six update time interval then that route will be mark as unreachable.

Holddown timer:-

If the hop count to a given destination increases, the router sets a hold down timer for that route. By implementing this refinement we have reduced the likelihood of a bad or corrupted information getting into the routing table, but once again understand that nothing is free and in this case the trade off is convergence time.

Flush timer:-

Time period is 240 seconds. It's a time period after the router is marked as unreachable to remove it from the routing table.

Routing Loops and Solutions

Routing Loops

Routing Loops occur because of slow convergence.

Solutions to Routing Loops

1) Counting to Infinity:-

Distance Vector Routing Protocols define a maximum value for Hops. The maximum Hop Count is 15 is commonly used.

Spilt Horizon: Spilt Horizon has two flavors

- ✓ **Simple Split Horizon**
- ✓ **Spilt Horizon with Poison Reverse**.

The logic behind **Simple Spilt Horizon** is that it is never useful to send information about a route back in the direction from which the information originally came. So if Router A learns about a Route through Router B, it will never send the same route back to Router A. This is known as suppressing routes.

Split Horizon with Poison Reverse does not work based on suppression, and it will include every route in its updates but it will tag them as unreachable. Lets say Router B receives a corrupted update believing that it can reach network 1.0 through Router C, Simple Split Horizon will not be able to avoid the loop, whereas Poison Reverse will definitely fix the problem. Router B will say 1.0 can be reached via Router C, but this time Router C will poison that route eliminating the routing loop.

Triggered Updates:

Also known **as flash updates.** Changes to the network topology are sent instantaneously to neighboring routers.

Holddown Times: If the hop count to a given destination increases, the router sets a hold down timer for that route. By implementing this refinement we have reduced the likelihood of a bad or corrupted information getting into the routing table, but once again understand that nothing is free and in this case the trade off is convergence time.

Interface Configuration

1. Assign IP address and subnet mask on serial and Ethernet interfaces
2. Set Clock Rate on Serial Interface at the DCE (only for lab not in real time)
3. Start the Interface

Example:

- Interface serial 0/0
- Ip address 110.0.0.1 255.0.0.0
- Clock rate 64000
- No shutdown

Global Configuration

1. Select Routing Protocol
2. Specify the Interface Network Addresses

Example for RIP:

- Router Rip
- Network 10.0.0.0
- Network 11.0.0.0

Example for RIP version 2:

- Router Rip
- Network 10.0.0.0
- Network 11.0.0.0
- Version 2

Interior Gateway Routing Protocol

- Distance Vector
- Uses Autonomous Systems
- Routing Domains can have multiple IGPs.
- IGPs Discover routes between networks
- EGPs Discover routes between two different Autonomous systems
- Update Timers = 90 sec

- Default maximum hop Count = 100, configurable to a maximum of 255.
- Split Horizon with Poisoned Reveres, Triggered Updates, and Holddown Timers are used for stability of the operation.
- Metrics used: BDRLM. **By Default it only uses Bandwidth and Delay**
  - Bandwidth = Default is 1544.
  - Delay = 10 Millisecond units.
  - Reliability = Can equal number of errors, a fraction of 255, 255 means 100% reliable.
  - Load = A fraction of 255, 0 means no load
  - MTU = The MTU value of the path.

Open Shortest Path First (OSPF)

OSPF Features

- OSPF stand for Open Shortest path first
- Standard protocol
- It's a link state protocol
- It uses SPF (shortest path first) or dijkistra algorithm
- Unlimited hop count
- Metric is cost (cost=10 ^8/B.W.)
- Administrative distance is 110
- It is a classless routing protocol
- It supports VLSM and CIDR
- It supports only equal cost load balancing
- Introduces the concept of Area's to ease management and control traffic
- Provides hierarchical network design with multiple different areas
- Must have one area called as area 0
- All the areas must connect to area 0
- Scales better than Distance Vector Routing protocols.
- Supports Authentication
- Updates are sent through **multicast address 224.0.0.5**
- Uses Multicast versus Broadcasts.
- Faster convergence.
- Sends Hello packet every 10 seconds
- Trigger/Incremental updates
- Router's send only changes in updates and not the entire routing tables in periodic updates

Advantages of OSPF

- ✓ Open standard
- ✓ No hop count limitations
- ✓ Loop free
- ✓ Faster convergence

Disadvantages

- ✓ Consume more CPU resources
- ✓ Support only equal cost balancing
- ✓ Support only IP protocol don't work on IPX and APPLE Talk
- ✓ Summarization only on ASBR and ABR

OSPF tables

1) Neighbor table
2) Database/topology table
3) Routing table

Neighbor table:-
It contains the information about the directly connected ospf neighbors.

Database table
It contains information of entire view of topology with respect to each router in the same area.
It contains all the possible paths for the particular destination.

Routing table
It contains the information about the best path for the destinations.
SPF algorithm is used to calculate the best path depending upon the cost.
Best path is calculated from the database table.

Router Types

In OSPF depending upon the network design and configuration we have different types of routers.

Internal Routers are routers whose interfaces all belong to the same area. These routers have a single Link State Database.

Area Border Routers (ABR)

It connects one or more areas to the backbone area and has at least one interface that belongs to the backbone,

Backbone Router Area 0 routers

Autonomous System Boundary Router (ASBR) Router participating in OSPF and other protocols (like RIP, EIGRP and BGP)

Router States

Intit State: First Hello is sent
2-Way: Neighbor discovered, but adjacency not built
Exstart: Neighbor's form a Master/Slave Relationship. Based on the Highest IP address. Initial sequence number established
Exchange: The router's exchange Database Description packets to tell each other about the routes it knows about. A request list is created.
Loading: Link State Request is sent to each other and based on the LSR's received; Link State Update packets are sent back in both directions.
Full: All Neighbors have a consistent Database

Note: - OSPF neighbor relationship should be in **FULL** state before exchange the routes. If the neighbor relationship is anything other than **FULL** then there is a problem in ospf neighbor ship and the ospf routes cannot be changed

Enhanced IGRP (EIGRP)

- ✓ Cisco proprietary routing protocol
- ✓ First released in 1994 with IOS version 9.21.
- ✓ Advance Distance Vector/Hybrid routing protocol that has the behavior of distance vector with several Link State features, such as dynamic neighbor discovery.

Characteristic of EIGRP

- ➢ It's a Cisco proprietary
- ➢ It uses DUAL (diffusion update algorithm)
- ➢ Its support multiple protocols (IP,IPX and APPLE TALK)
- ➢ Administrative distance is 90 internal and 170 external
- ➢ Rapid convergence
- ➢ Classless routing protocol
- ➢ Support VLSM and CIDR
- ➢ Summarization can be done on every router
- ➢ It uses composite metric 32 bits
- ➢ Trigger updates
- ➢ Supports equal const an unequal cost load balancing
- ➢ Multicast updates are sent on 224.0.0.10
- ➢ Also called as advance distance vector protocol
- ➢ It's a loop free protocol
- ➢ Usually keep two paths successor and feasible successor in topology table

It maintains three tables

- ❖ Neighbor table
- ❖ Topology table
- ❖ Routing table

Features

- ❖ **Rapid Convergence**: EIGRP uses DUAL to achieve rapid convergence. It stores a backup route if one is available, so it can quickly re-converge incase a route goes down. If no backup route exists, EIGRP will send a query to its neighbor/s to discover an alternate path. These queries are propagated until an alternate route is found.

- ❖ **Classless Routing Protocol:** This means that advertised routes will include their subnet mask, this feature will eliminate the issue pertaining to discontiguous networks. VLSM and Manual Summarization is also supported on any router within the enterprise.

- **Security:** With IOS version 11.3 or better, EIGRP can authenticate using only MD5, the reason EIGRP does not support clear text is because, EIGRP can only be used within CISCO routers, and all Cisco routers support MD5 authentication. But the routes are not encrypted, so a sniffer can easily see the password/s.

- **Multiple Network Layer Protocol Support:** EIGRP can support IP, IPX, and AppleTalk, whereas the other routing protocols support only one routed protocol. EIGRP will also perform auto-redistribution with NLSP, IPXRIP, RTMP. EIGRP supports incremental SAP and RIP updates, 224 HOPS, and it uses bandwidth + delay which is far better than just Ticks and Hops used by IPXRIP. For RTMP it supports event driven updates, but it must run in a clientless networks (WAN), and also a better metric calculation.

- **Use of Multicast Instead Of Broadcast:** EIGRP uses multicast address of 224.0.0.10 instead of broadcast.

- **Unequal and Equal Cost Path Load-Balancing:** This feature will enable the administrators to distribute traffic flow in the network. By default EIGRP will use up to 4 paths and this can be increased to 6.

- **Easy configuration:** The configuration of EIGRP is very similar to IGRP which is very simple.

- **100% Loop Free:** EIGRP uses DUAL to attain fast convergence while maintaining a totally loop free topology at every instance.

.

Access Lists

Overview

- Its is a method to make router as a packet firewall
- Used to define the type of traffic that should be allowed or restricted from crossing a router (entering or exiting a router interface)
- Set of rules that help control flow of packets into or out of a router
- Statements that specify how the router will handle the traffic flow through specified interfaces

Uses of Access List

- Filter packet flow in/out of router interfaces
- Restrict/reduce contents of routing updates, e.g. from RIP, IGRP
- Identify packets that will initiate dial-on-demand connections (interesting packets)

Types of Access List

- ***Standard Access Lists:*** Check source address of packets and permit or deny the packets based on network, subnet or host address.

- ***Extended Access Lists:*** Check both source and destination addresses for filtering. Packets can be filtered based on protocols within a suite (e.g. TCP/IP) and port numbers. Extended Access Lists add more granularity than Standard Access Lists.

Access Lists Operation and Application

- Operate in sequential order, following a top to down
- Always one invisible deny any statement exist.
- If no conditions, or tests, are met, a final implicit deny will drop that particular packet
- Routers stop processing once the first instance of a condition is met in the written access list
- Access lists can be inbound or outbound, with reference to a router interface
- Location and sequential order can affect performance of router
- Written in global configuration mode (by the **access-list** command) and grouped, or linked in interface mode for the appropriate router interface (by the **ip access-group** command)

Verifying Access List

- **show [ip] interface**
  Use to see if an interface is grouped to an access list
  Returns IP addresses and all configuration parameters
- **Show access-lists**
  Shows details of all access lists configured
- **Show [ip| access-list**
  Show access list for specified protocol

Wildcard Mask Bits

- 0 indicates that the corresponding bit should be checked
- 1 indicates that the corresponding bit should be ignored

Examples:-

- **Match a specific/Single Host** 10.1.1.1 0.0.0.0 (or **host 10.1.1.1** is same)
- Match a whole network address 200.1.1.0 0.0.0.255
- **Match any IP address** 0.0.0.0 255.255.255.255 (It is equivalent to "any" command)
  0.0.0.0 255.255.255.255 = any (both are same)

Configure Standard IP Access List

Two Steps to configure any ACL

1. **Creating the access list**

Router (config) #**access-list** [1-99] [permit|deny] *source_address wildcard_mask*

2. **Apply it in the interface**

Router (config-if) #**ip access-group** [1-99] [in|out]

Note: - The last statement in the access-group statement. In or out specifies incoming or outgoing traffic. By default, all access lists are applied to outgoing traffic, i.e. if the in or out statement is omitted, out will be applied.

Examples

Permitting only a specific network

To allow only traffic from 172.16.0.0 to pass through the router

Access-list 1 permit 172.16.0.0 0.0.255.255

Configuring Extended IP Access Lists

Overview

- Extended IP Access Lists filter based on source and destination addresses, specific protocols and even ports defined by TCP or UDP
- Extended IP Access Lists offer more granularity than Standard Access Lists and can be used in a wider range of situations in providing access security to a network through a router

Configuration

- **Creating the access list**

```
Router (config)#access-list [100-199] [permit|deny] [ip|tcp|icmp] source_address
source_mask  destination_address  destination_mask [eq|neq|lt|gt] port_number
```

- **Applying it to an interface**

```
Router (config-if)#ip access-group [100-199] [in|out]
```

Verifying Access Lists

Show Access-lists displays the definition of all access lists that are created on the router.

Show IP access-lists display the definition of IP access lists on this router.

Show IP interface displays the interface that is using a given access-list.

NAT (Network Address Translation)

Natting means "**Translation of private IP address into public IP address** ".
In order to communicate with internet we must have public IP address.

Types of NAT:-

1. Dynamic NAT
2. Static NAT
3. PAT

Dynamic NAT:-

- ✓ Many privates IP addresses is mapped to many of IP addresses. One to one Mapping.
- ✓ **Advantage** is it provides only security.
- ✓ **Disadvantages are w**e need to buy many public IP which is equal to private IP.(Expensive)
- ✓ It provides only one way access.
- ✓ From inside to outside access is allowed. Outside to inside access is not allowed.

Static NAT:-

- ✓ One single private IP address is mapped to single public IP address.
- ✓ It gives access to the servers from outside.
- ✓ One to one mapping
- ✓ It gives two way accesses.
- ✓ Users from inside can access outside.
- ✓ Outside users can also access inside.

PAT (Port Address Translation)

- ✓ Many private ip's is mapped to one single public IP address.
- ✓ Advantage is both save the public IP address and security.
- ✓ Disadvantage is some applications will not support by PAT.
- ✓ Also provides only one way access.
- ✓ From inside to outside.
- ✓ Outside to inside not allowed.

Steps to configure NAT:-

1. Define private IP address range in global config mode using "**access list**"
2. Define public IP address pool in global config mode using "**ip nat pool**"
3. Map private IP range with public pool in global config mode using “ip **nat inside source**"
4. Apply Nat the interface mode using "**ip nat inside**" and "**ip nat outside**".

Dynamic NAT:-Example

STEP 1:-
Define private IP address

```
Router(config)#access-list 1 permit 10.0.0.0 0.255.255.255
```

STEP 2:-
Define public IP address

```
Router(config)#ip nat pool p1 200.1.1.1 200.1.1.100 netmask 255.255.255.0
```

STEP 3:-
Map private pool with public IP address

```
Router(config)#ip nat inside source list 1  pool p1
```

STEP 4:-
Apply Nat in the interface

```
int e0=>ip nat inside
int s0=>ip nat outside
```

PAT Example:-

STEP 1:-
Define private IP address

```
router(config)#access-list 1 permit 10.0.0.0 0.255.255.255
```

STEP 2:-
Define public IP address

```
router(config)#ip nat pool p1 200.1.1.101 200.1.1.101 netmask 255.255.255.255
```

STEP 3:-
Map private pool with public IP address or interface

```
router(config)#ip nat inside source list 1 pool p1 overload
```

OR

```
 router(config)#ip nat inside source list 1 interface s0 overload.
```

STEP 4:-
Apply Nat in the interface

```
 int e0=>ip nat inside
 int s0=>ip nat outside
```

Static Nat Example:-

STEP 1:-

Map private pool with public IP address or interface

```
router(config)#ip nat inside source static 10.1.1.1 200.1.1.101
```

STEP 2:-

Apply Nat in the interface

```
 int e0=>ip nat inside
 int s0=>ip nat outside
```

IPv6 Addressing

- ✓ IPv6 is a 128 bit addressing scheme
- ✓ It allows 3.4*10 power 8 addresses which are enough for many IP address for each person on this earth.
- ✓ IPv6 addressing is a hexadecimal format.
- ✓ It has eight sets of 4 hexadecimal numbers separated by: (colon).
- ✓ IPv6 address looks in this way **ABCD:2345:9876:4543:3456:3432:CABD:4533**
- ✓ If we have successive fields of zero in between like **ABCD:6876:9876:0000:0000:0000:4564:0000** then we can represent it using the **::** double colons but only once in the address
- ✓ So the resultant address will be **ABCD: 6876:9876::FFCA:0000.It** represent after 9868 we have three quad zero fields
- ✓ IPv6 header is also simplified than complex IPv4 header.
- ✓ As IPv6 uses the hexadecimal format. In hexadecimal format
- ✓ A represent 10
- ✓ B represent 11
- ✓ C represent 12
- ✓ D represent 13
- ✓ E represent 14
- ✓ F represent 15
- ✓ IPsec (internet protocol security) is inbuilt into the IPv6 protocol.
- ✓ IPv6 has different types of addresses.
- ✓ **Any cast**: - Anycast address refers to as **one-to-the-nearest-address** .It is a hybrid of unicast and multicast. Packet is sent to any one member of a group of devices that are configuring with the unicast address. In anycast many devices share can share the same address
- ✓ **Multicast**: - **One to Many**. It is similar to the IPv6 addressing. Sending the message to one group of devices.

- ✓ **Unicast:-One to One**.Represent the single interface. One packet is sent to one destination.
- ✓ **Global** unicast address begin with 2000::/3
- ✓ **Private** address range from FE8 through FFF
- ✓ **Loop back** address is ::1
- ✓ **Unspecified** address **::**
- ✓ **Subnet ID** is the first 64 bit and **interface ID** is the last 64 bit.
- ✓ **DHCPv6** allows learning IPv6 address dynamically through DHCP server.

IPv6 Routing Protocols

- ✓ **RIPng**
- ✓ **Static**
- ✓ **OSPFv3**
- ✓ **ISIS for IPv6**
- ✓ **MP BGP 4**
- ✓ **EIGRP IPv6**
- ✓ Router running both IPv6 and IPv4 are referred to as **dual stack.**
- ✓ Connecting IPv6 networks by tunneling it in IPv4 packets is referred to as **6to4 tunneling**.
- ✓ **Tunneling (6to4 tunneling), DUAL stack and Transition** are the three methods for migration from IPv4 to IPv6.
- ✓ RIPng is based on the RIPv2.
- ✓ All RIP routes multicast address is FF02::9
- ✓ RIPng uses the UPD port no 521
- ✓ On the router **ipv6 unicast-routing** command globally enable the IPv6 and it must be the first command executed on the router.
- ✓ Suppouse if u want to enable the RIPng routing
- ✓ **Ipv6 router rip** command has to be used
- ✓ **Show ipv6 route rip** displays the RIPng route in the routing table.

Configuration of IPv6 addresses scheme

Assigning IPv6 address on serial 0/0 interface

```
Router#configure terminal
Router(config)#int serial 0/0
Router(config-if)#ipv6 address 5001:4323::3/64
Router(config)#exit
```

To enable routing

```
Router(config)#ipv6 unicast routing
```

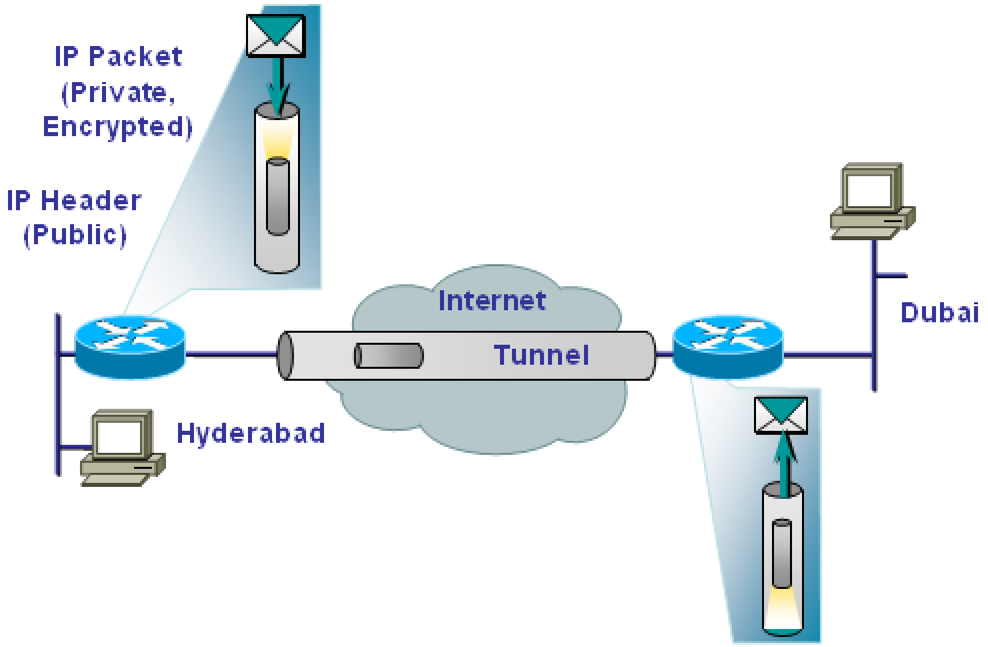
Configure OSPF on IPv6

```
Router (config)#ipv6 router ospf 3
Router(config-rtr)#exit
Router(config)#int serial 0/0
Router(config-if)#ipv6 router ospf 3 area 0
```

To see the output

- ✓ Router# show ipv6 protocol
- ✓ Router# show ipv6 ospf
- ✓ Router# show ipv6 neighbor
- ✓ Router# show ipv6 database
- ✓ Router# show ipv6 route

Virtual Private Network (VPN)



- VPN stands for virtual private network.
- VPN carries private data over the public network (internet) usually in encrypted form.
- **V** means virtual. Physical connection not establish between two sites
- **P** means private. Data must be secure and should not be alter (change).
- **N** means network. To connect different geographical locations
- VPN is similar to Virtual Connection in the Frame Relay.
- Only the difference is FR uses private connection but VPN is over internet (public connection).
- The VPN provides the secure connectivity and privacy as Leased Line or Frame Relay does.
- Much cheaper cost as uses Internet.\
- Provides Scalability as companies can add large number of uses offices without any WAN infrastructure

- Tunnel concept is used in VPN.
- **Tunneling** means from source original packet is converted into encrypted form (coding) and at destination decryption (decoding) is done.

VPN = TUNNELING + ENCRYPTION

Advantages of VPN

- VPNs reduce costs
- VPNs improve connectivity
- VPNs maintain security
- VPNs offer flexibility
- VPNs are reliable

Types of VPN

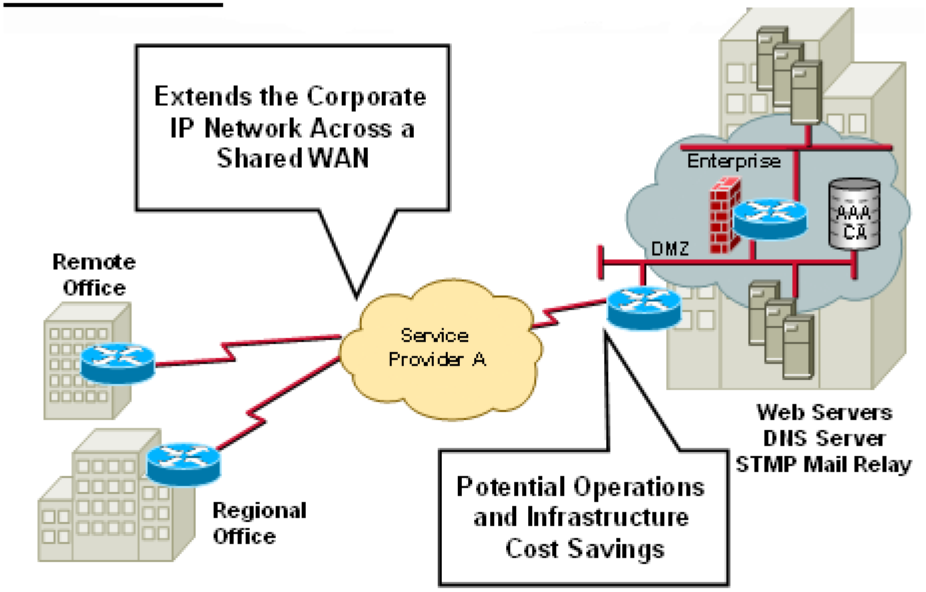
1) Site to Site VPN
   a) Intranet VPN
   b) Extranet VPN

2) Remote Access VPN

Site to site VPN

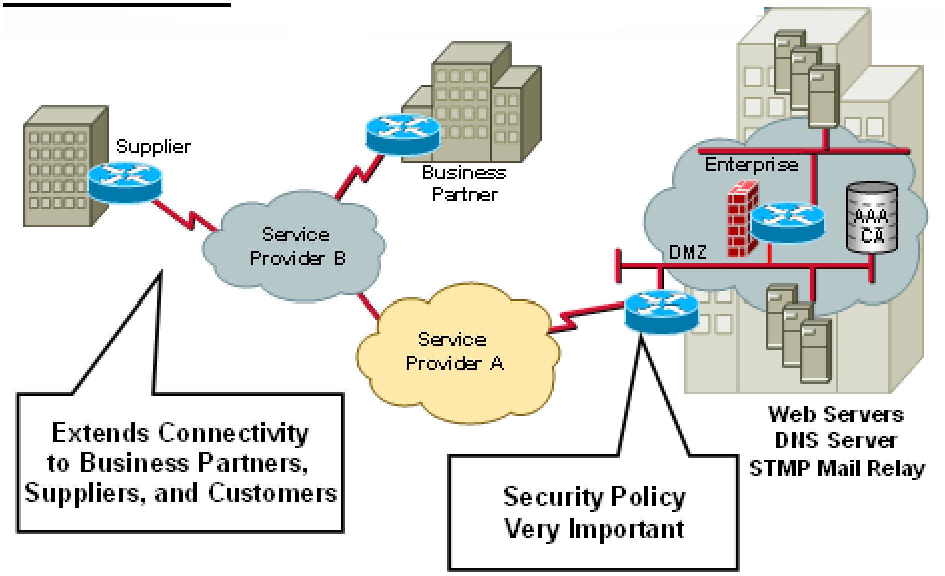
- **Site to site VPN** is also called as LAN-to-LAN VPN or L2L VPN.
- Tunnel is created between two sites or offices.
- **Tunneling** means from source original packet is converted into encrypted form (coding) and at destination decryption (decoding) is done.

Intranet VPN


Extends the Corporate IP Network Across a Shared WAN
Remote Office
Regional Office
Service Provider A
Enterprise
DMZ
AAA CA
Web Servers
DNS Server
STMP Mail Relay
Potential Operations and Infrastructure Cost Savings

- **Intranet VPN** connects two offices of same company like head office in Hyderabad and Branch office in Saudi Arabia over public network i.e. internet
- The VPN typically is an alternative to a leased line.
- It provides the benefit of extended connectivity and lower cost.

Extranet VPN



- **Extranet VPNs** connects two different companies usually business partners like Dell in Hyderabad and IBM in U.A.E over internet (public network).
- Some restrictions are exist only limited date can be shared between them.
- Firewalls are used to allow access to require servers and services
- The extranet VPN facilitates e-commerce

Remote VPN

- Remote VPN is also called as Access VPN.
- Remote access VPNs connects the Head or Branch Office network to, mobile workers, and remote offices with less WAN traffic.
- Remote users of company can connect to their corporate intranets or extranets whenever, wherever, or however they require over the public network i.e. internet.
- Remote VPN are typically an alternative to dedicated dial or ISDN connections.
- They offer users a range of connectivity options as well as a much lower cost solution.

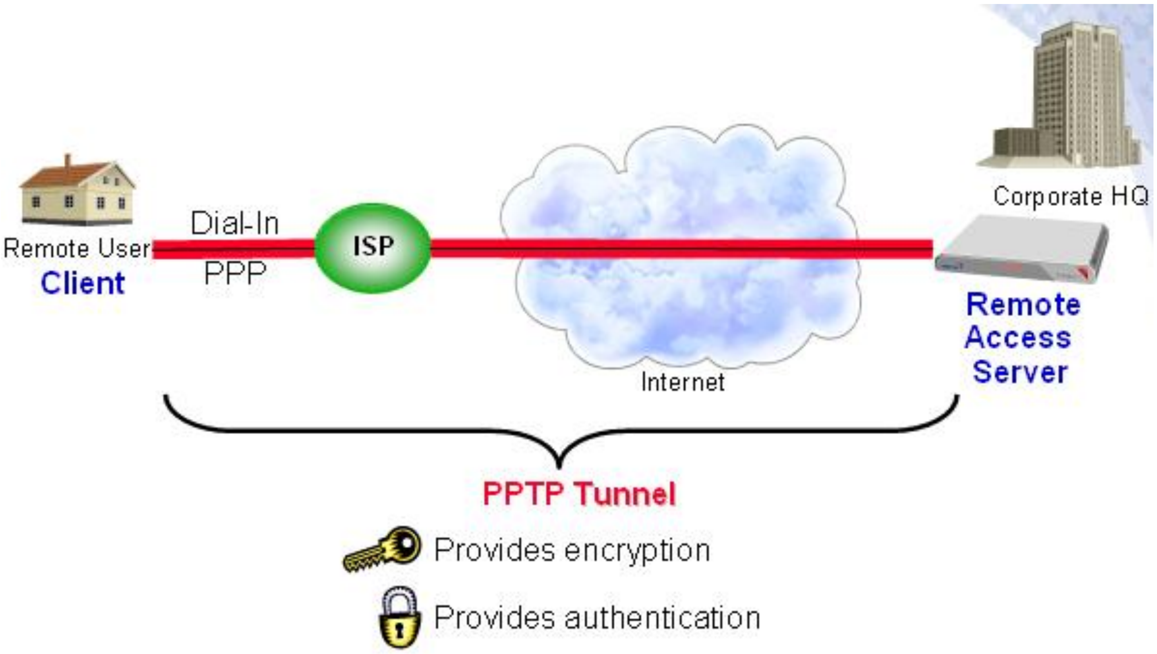
VPN Tunneling Protocols

Layer 2 (data link layer) protocols

Layer 2 tunneling protocols are the protocols that can be used to establish a secure tunnel between a remote user and a remote access server.

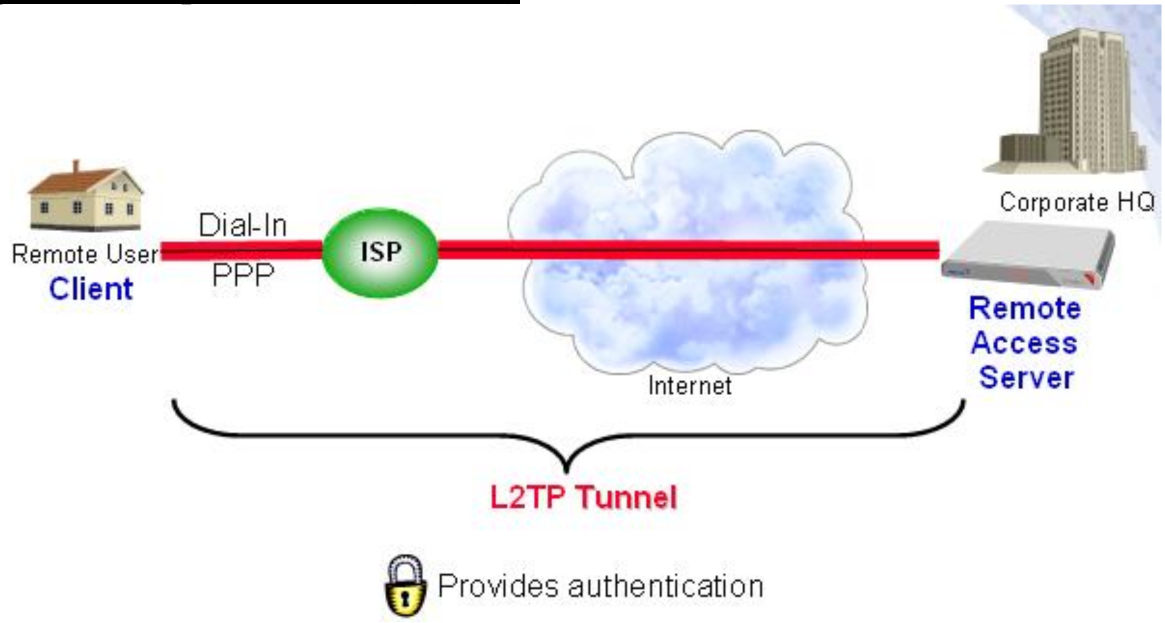
1) Point to Point Tunneling Protocol (PPTP)
2) Layer 2 Transport Protocol (L2TP)

1) PPTP (point-to-point tunneling protocol)



- **PPTP** was introduced by Microsoft.
- It provides only authentication and encryption
- PPTP has been shown to have security weaknesses, for example an eavesdropper could discover a user’s password.
- PPTP use RADIUS protocol for authentication to remote access servers

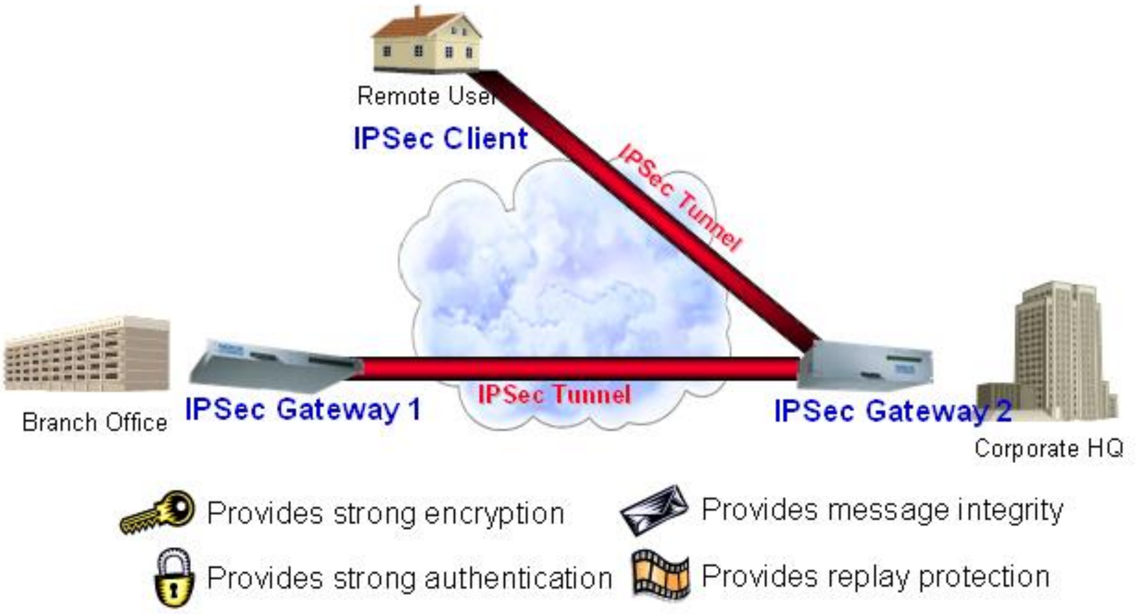
Layer 2 Transport Protocol (L2TP)



- L2TP is a TCP/IP standard that resulted from the merging of Microsoft's PPTP with L2F (layer 2 forward protocol) developed by Cisco.
- L2TP provides a better form of authentication than PPTP, but it does not provide support for encryption and does not perform integrity checking on data.
- L2TP also uses RADIUS protocol for authentication to remote access servers

Layer 3 network layer protocols

IPSec (Internet Protocol Security)


Remote User
IPSec Client
IPSec Tunnel
Branch Office
IPSec Gateway 1
IPSec Tunnel
IPSec Gateway 2
Corporate HQ
Provides strong encryption
Provides message integrity
Provides strong authentication
Provides replay protection

- IPSec was developed as a standard by the ITEF
- IPSec does both tunneling and encryption.
- It eliminates the limitation of the Layer 2 tunneling protocols—PPTP and L2TP.
- IPSec provides
- Message integrity assures data cannot be altered.
- Privacy assures data transmitted in encryption format.
- Authentication assure verification of remoter clients using digital signatures
- Replay protections assure unique packets. Drops duplicate packets
- IPSec tunnels are most often used between two IPSec gateways or between an IPSec gateway and an IPSec client.

OSI Reference Model

Layering Benefits & Reasons

- It’s a standard for network architecture.
- It explains how the data will flow from application to the physical cable.
- The main reason to define standard interfaces was to achieve compatibility and multi-vendor integration.
- To divide the interrelated aspects of network operation into less complex operations.
- To achieve a modular approach to networking protocols so new applications and services can be deployed without redesigning other layers.
- To keep changes in one area from affecting other layers.
- To ease troubleshooting using data packets this will have specific information about each layer.

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

Application Layer (Layer 7)

- It is an interface to the users.
- Provides network services to user client/server-based applications
- Establishes and defines program-to-program communication
- Application layer has application layer protocols.
- WWW (world wide web)
- TELNET
- FTP (File Transfer Protocol)
- TFTP (Trival File Transter Protocol)
- SMTP (simple mail transfer protocol) and so on

Presentation Layer (Layer 6)

- Defines data format for transmission
- Also called as data representer.
- Ensures arriving data from the network can be used by the application and information sent by the application can be transmitted on the network
- Performs encryption (coding), decryption (encoding) and compression
- Example representations include ASCII, EBCDIC, JPEG, MPEG, MIDI, HTML

Session Layer (Layer 5)

- Defines how to start, control and end sessions
- It check whether destination is alive or not.
- RPCs (remote procedure call) operate at this layer
- Logon Validation happens at this layer.
- Session layer organizes communication through simplex, half-duplex or full-duplex
- Example protocols include SQL, RPC, NetBIOS, Named Pipes.

Transport Layer (Layer 4)

- It is used to transport the data from source to destination
- Segmented (blocks of data) data to be passed down to the Network layer and reassembles data for the Session and upper layers
- With respect to TCP/IP it uses two protocols
    - **TCP (Transmission Control Protocol)**
    - **UDP (user datagram protocol)**
        - **TCP** is a connection oriented, reliable and efficient protocol
        - **UDP** is connection less, not reliable, no t efficient protocol
- UDP is faster than TCP
- Provides the choice of connection-oriented and guaranteed (TCP) or connectionless and non-guaranteed (UDP) delivery of data
- The first 1023 ports are reserved, or well-known ports used by the Operating System
- The remaining ports (1024 – 65,535) are available for use by client/server-based applications

20, 21	FTP
23	Telnet
25	SMTP
53	DNS
67	DHCP Server
68	DHCP Client

69	TFTP
70	Gopher
80	http
119	NNTP
161	SNMP
179	BGP

Network Layer (Layer 3)

- It is responsible for routing (forwarding or packets from one network to another network choosing the best path)
- This layer manages logical device addressing and determines the best way to move data
- Routers operate at this layer

- Segments from the Transport layer are placed into packets and passed down to the Data Link layer
- Network layer routes data from one node to another
- Network layer maintains routing table
- IP addressing works at this layer.
- ICMP protocol is another protocol that works at this layer. It is used to generate an echo reply in response to a PING test
- It is also used to send a host or port unreachable message from a router to the source of an undeliverable packet.

Data Link Layer (Layer 2)

- Provides error-free link between 2 devices – CRC used for error checking
- This layer can also provide flow control services if protocol requires it.
- Packets from the Network layer are placed into frames
- Data Link layer handles physical transmission of data from one node to another
- Handles error notification
- IEEE subdivided this layer into 2 sublayers

  Logical Link Control (LLC)

  - **LLC used to support multiple network protocols with single NIC card.**
  - Uses Destination Service Access Points (DSAP) and Source Service Access Points (SSAP) to help lower protocols access Network layer protocols

  Media Access Control (MAC)

  - **MAC is the physical address of the pc of size 48-bit.**
  - Handles MAC addresses – first 6 digits of 12 hex define vendor ID, next 6 is the serial number for that vendor ID
  - Builds frames from bits
  - Performs CRC
- Internetworking devices used at the 2nd layer
  - ***Bridges***
  - ***Switches***

Physical Layer (Layer 1)

- It transfers the data in bits format i.e. 01010101010 (zeros and ones).
- Places frames, represented as bits, onto media as electric signals or pulses of light
- **Hubs and repeaters operate at this layer**

Switching

Network connection devices

- ➢ Hub
- ➢ Repeater
- ➢ Switch
- ➢ Bridge
- ➢ Router

Hub

- ✓ It’s a layer one device
- ✓ It has one broadcast domain
- ✓ It has one collision domain
- ✓ It uses CSMA/CD
- ✓ It works on shared bandwidth
- ✓ It does half duplex transmission

Repeater

- ✓ It a layer one device
- ✓ It amplifies(strength) the signal and send to destination
- ✓ Used for long distance communications where signal strength become weak.

Switch

- ✓ It a layer 2 device
- ✓ It has one broadcast domain
- ✓ Each port is consider as one collision domain
- ✓ Number of port is equal to number of collision domain
- ✓ It is an intelligent device
- ✓ It uses ARP (address resolution protocol)
- ✓ Works on MAC (media access control) addresses
- ✓ It maintains CAM (content addressable memory) table
- ✓ It works on full duplex
- ✓ It uses hardware called ASIC

Bridges

- ✓ It is a layer 2 device
- ✓ Works on software
- ✓ Slower than switch
- ✓ It has lesser number of ports than switch

Router

- ✓ It's a layer 3 device
- ✓ It is an intelligent device
- ✓ It is used to connect two different networks
- ✓ In router Number of broadcast domain is equal to Number of interfaces
- ✓ It can also work as packet filtering firewall, VPN server, NAT Server,DHCP server etc

It does two basic functions

- ✓ Select the **best path** from the routing table
- ✓ **Forward** the packet on it

Broadcast Domain

- ❖ Set of all devices that receive broadcast frame originating from one device from the set.

Collision Domain

- ❖ A group of network nodes on an Ethernet network that share the network media that can experience collisions within a collision domain.
- ❖ Networks can be segmented into multiple collision domains for optimization of network functionality.

<u>Switch Functions</u>

- ❖ **Address learning**
  - Initially MAC address table is empty – switch will flood networks to forward data
  - Hosts are added to the table as soon they start communicating
- ❖ **Frame filtering**
  - If the destination MAC address exists in the MAC address table, frame is not flooded, it is sent out only on the appropriate port
  - Broadcasts and multicasts are flooded to all ports, except the originating port
- ❖ **Loop avoidance**
  - Duplicate frames must be prevented from traveling over redundant paths that may exist for backup or transmission redundancy.
  - Broadcasts will continually flood around a loop structure – broadcast storm
  - Multiple copies of non-broadcast frames may be delivered to the same destination, causing errors
  - The same frame will be received on different ports of the same switch, causing instability in the MAC address table

Modes of Communication

- **Half Duplex**
  - Hubs communicate half duplex
  - With Half-duplex transmission frames feed into a single cable in one direction at a time.
  - 4 wires used – 2 used for collision detection, 2 used for either transmit or receive
  - Bandwidth utilization 50-60%
- **Full Duplex**
  - Switches normally communicate full duplex, hubs don't
  - 4 wires – 2 for transmit, 2 for receive
  - Must disable collision detection on NIC
  - NIC must support full duplex
  - Bandwidth utilization 100%
  - There are no collisions that are caused by transmitting and receiving frames simultaneously in a full-duplex Ethernet technology, hence no need for Collision detection.

Types of switches

1) Manageable switches
2) Unmanageable switches

Manageable switches:-

- ✓ Switches which consists console port are called as manageable switches.
- ✓ Configuration of the switch is possible.
- ✓ IP address can be assign to it
- ✓ Telnet to the switch is possible

Unmanageable switches:-

- ✓ Plug and Play Switches
- ✓ Switches which do not have console port and configuration of the switch is not possible.
- ✓ IP address cannot be assign to it
- ✓ Telnet to the switch is not possible

Hierarchy of switches

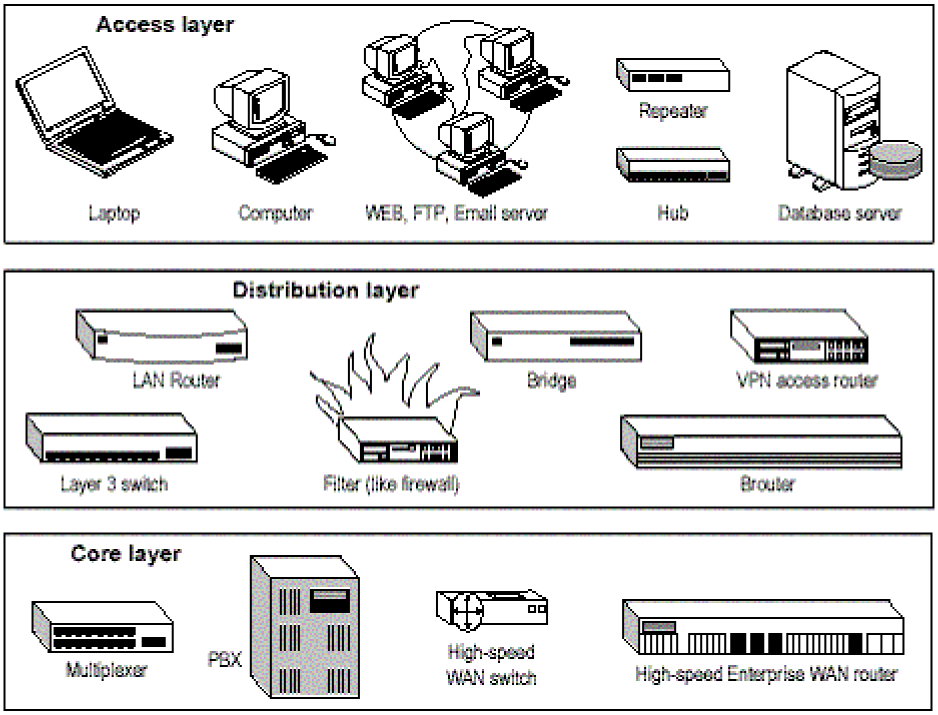
1) Access layer
2) Distribution layer
3) Core layer

Cisco has defined a hierarchical model known as the hierarchical internetworking model. This model simplifies the task of building a reliable, scalable, and less expensive hierarchical internetwork because rather than focusing on packet construction, it focuses on the three functional areas, or layers, of your network:

Core layer: This layer is considered the backbone of the network and includes the high-end switches and high-speed cables such as fiber cables. This layer of the network does not route traffic at the LAN. In addition, no packet manipulation is done by devices in this layer. Rather, this layer is concerned with speed and ensures reliable delivery of packets.

Distribution layer: This layer includes LAN-based routers and layer 3 switches. This layer ensures that packets are properly routed between subnets and VLANs in your enterprise. This layer is also called the Workgroup layer.

Access layer: This layer includes hubs and switches. This layer is also called the desktop layer because it focuses on connecting client nodes, such as workstations to the network. This layer ensures that packets are delivered to end user computers.



Series of switches

- 3550
- 3560
- 3750
- 4500
- 2950

- 6500
- 10000

Modes and configuration of a switch
Modes of the switch is similar to the modes of a router.
Refer the modes of the routers.

Network Segmentation Using Bridges

- Bridges operate at layer 2 and therefore use MAC addresses to decide whether to forward data
- It increases the number of collision domains.
- Bridges build Layer 2 address table also called forwarding tables by *listening* to hosts communicate.
- It looks at the frames destination in its address table and sends the frame towards the destination host.
- Bridges maintain one logical network, network is only physically segmented

Network Segmentation Using Routers

- Routers create separate collision domains by creating separate layer 3 networks.
- Layer 3 networks are referred to as Broadcast domains.
- In large networks, routers need to be able to carry the excessive load placed by a large number of hosts.

Network Segmentation Using Switches

- A switch is essentially a bridge with multiple ports and intelligence
- Switches forward data based on MAC addresses as they operate at layer 2
- Switches will build forwarding tables the same way as bridges.
- Switches increase the number of collision domains
- Enables high speed data exchange
- LAN switches can operate in three different modes:
    - Cut-through
        - Frames forwarded as soon as the destination address is read and the forwarding table is consulted
        - Produces the lowest amount of latency
    - Fragment-free
        - Frames forwarded as soon as the first 64 bytes are received
    - Store and Forward
        - Frames forwarded once the entire frame is received
        - Ensures corrupt frames are not forwarded
        - Latency through the switch varies with frame length.

- The switch receives the complete frame before beginning to forward it.
- Highest latency

Virtual LANs (VLANs)

- ❖ Building the multiple logical topologies over a single physical topology
- ❖ Dividing the one single physical broadcast domain into multiple logical broadcast domains.
- ❖ A VLAN is a broadcast domain, similar in concept to a domain
- ❖ Hosts in different VLANs cannot communicate with each other, unless their data is routed through a router
- ❖ VLANs can exist on a single switch, or they can exist on **2 or more switches**.
- ❖ If two or more switches are used, they must be connected using the **trunk port**
- ❖ By default, all ports have membership of VLAN 1

Trunking encapsulations

- ▪ **ISL (Inter Switch Link) encapsulation.**
- ▪ **802.1q**

ISL

- ✓ It's a Cisco proprietary
- ✓ It adds 30 bytes to the header
- ✓ All VLAN traffic is tagged
- ✓ It works with Ethernet, Token ring, FDDI

802.1q

- ✓ It is an open standard
- ✓ It adds 4 bytes to the header
- ✓ VLAN 1 traffic is untagged
- ✓ It works only on Ethernet

<u>VLAN types</u>

1) Static VLAN
2) Dynamic VLAN

Static VLAN

- ✓ It is port based VLAN
- ✓ Manually we have to assign ports.
- ✓ It can be a member of only single VLAN.

Dynamic VLAN

- ✓ It is a MAC based VLAN
- ✓ It uses the software called as VMPS (VLAN Membership Policy Server)
- ✓ Each port can be a member of multiple VLAN's

Types of ports

- ✓ Access port
- ✓ Trunk port

Access port:-
It is used to connect only computers, printers and laptops

Trunk port:-
It is used to connect two switches or switch to router
It carrier the VLAN's information form one switch to another switch.
Cross cable must be use if connected between two switches

Trunking protocols

1)ISL (inter switch link)
2) 802.1q

<u>Difference Between ISL and 802.1Q</u>

ISL	802.1Q
It's a Cisco proprietary	It is an open standard
It adds 30 bytes to the header	It adds 4 bytes to the header
All VLAN traffic is tagged	VLAN 1 traffic is untagged
It works with Ethernet, Token ring, FDDI	It works only on Ethernet
Frame is not modified	Frame is changed

Looping Solutions –Spanning Tree Protocols (STP)

- ❖ Algorithm developed by DEC, revised by IEEE (Specification 802.1d)
- ❖ Avoids loops by blocking traffic from entering and leaving one of the ports
- ❖ STP reconfigures as the network topology changes to avoid the creation of new loops
- ❖ STP enabled by default on all Cisco Catalyst switches

Rules of Spanning Tree

- ❖ One root bridge per network
  - ▪ All ports are designated ports – i.e. in forwarding state
- ❖ One root port per non designated root bridge
  - ▪ Root port will be the one which has the lowest cost (bandwidth) to root bridge, will be in forwarding state
- ❖ One designated port per segment

  - Designated port will be in forwarding state
  - Others will be non-designated ports and will be in blocking state – this helps break the loop topology

Root bridge selection

- ❖ Switches using STP exchange configuration messages using a multicast frame, called Bridge Protocol Data Unit (BDPU) every 2 seconds by default. One such configuration is the bridge ID, which will be used to determine the root bridge.
- ❖ Bridge ID contains 32768 (hex, default value) followed by MAC address, e.g. 32768.1111.123a.34ef

VTP (VLAN Trunking Protocol)

- ✓ VTP stands for VLAN Trunking Protocol
- ✓ VTP is used to share VLAN information to ensure that swithes have consisent or same VLAN configuration in all the switches with same domain name.
- ✓ It propagates VLAN information form server switch to all Clients.
- ✓ It works only on Trunk line
- ✓ VTP messages are propagated only across trunk.
- ✓ All the clients are in synchronization with server with the help of revision
- ✓ It reduces the Administrative work
- ✓ It provides authentication.
- ✓ In VTP configuration mandatory we have to configure these parameters
- ✓ VTP domain: - must be same in all the switches.
- ✓ VTP mode: - server or client or transparent. By default mode is server.
- ✓ VTP Password: - It’s a optional. To keep authentication among all the switches.
- ✓ **On all switches domain and authentication must be match.**

It has three modes

1) server
2) client
3) transparent

In **server mode** VLANs can be added, deleted or modified.

In **client mode** VLANs cannot be added, deleted or modified. Only it accepts the VLAN form the server and save only in the RAM i.e. running config.

In **Transparent mode** VLANs can be added locally and it passes VLAN information from server mode to client mode. It ignores VTP messages.

Configuration of VTP

```
Switch(config)# vtp domain any-name
Switch(config)# vtp mode server/client/transparent
Switch(config)# vtp password any-password
```

Cisco Discovery Protocol (CDP)

OVERVIEW

- Provides details about directly connected Cisco devices, such as address, protocol used
- CDP starts automatically by default for IOS 10.3 and later
- CDP operates at Layer 2, so it is not necessary for the neighboring device to be in the same domain, or share a common network address for communication
- Advertisements about neighbors are multicast to the address 0100.0ccc.cccc
- Routes are learned through *hello* type updates

CDP Parameters

- **CDP Timer**
  - How often updates are sent
  - Default = 60 seconds
  - To change default time
  - Router(config)#**cdp timer** *new_update_time*

- **CDP Holdtime**
  - The time the CDP packet sent should be kept by the receiving router before being discarded
  - Default = 180 seconds
  - To change default time
  - Router(config)#**cdp holdtime** *new_holdtime*

Disabling and Enabling CDP

- To disable CDP
  Router(config)#**no cdp enable**

- To disable CDP on an interface
  Router(config-if)#**no cdp enable**

- To enable CDP
  Router(config)#**cdp run**

Showing CDP Neighbors

- For each connected Cisco device, the following information can be displayed

  - Device ID router hostname/domain name
  - Local port type and # e.g. Ethernet 0/0
  - Holdtime
  - Device capability e.g. router, switch
  - Hardware platform e.g. 2600, 1900
  - IOS version
  - Neighbour's remote port type and number

- For a brief summary
  Router#**show cdp neighbors**

- For detailed information
  Router#**show cdp neighbors detail**

- To look at a single device
  Router#**show cdp entry** *router_name*

- To display information about your local router
  Router#**show cdp interface**

PORT NUMBERS

Service	Port No.
FTP	20,21
SSH	22
telnet	23
SMTP	25
DNS	53
DHCP	67,68
TFTP	69
HTTP	80
POP3	110
NNTP	119
NTP	123
IMAP4	143
LDAP	389
HTTPS	443
IMAPS	993
RADIUS	1812
AIM	5190