



## CCNA :- Cisco Certified Network Associate



Router



Wireless Router



Secure Router



Firewall



Home Office



Workgroup Switch



Access Point



IP Phone



Mobile Access Phone



Small Business



Wireless Connectivity



Line: Serial



Line: Ethernet



### About Cisco :-

CISCO company name derived from SANFRANCISCO

Cisco Systems, Inc. is an American multinational corporation headquartered in San Jose, California, United States, that designs, manufactures, and sells networking equipment.



### About us :-

**N**etwork **Kings** stands as an undisputed brand name/company in the IT industry due to its sincere efforts and remarkable services it has provided over time. All this made Network Kings stand apart and shine bright amongst the crowd of countless analogous competitors. IT has been expanding itself in terms of infrastructure and IT Solutions, ever since its inception.

**Website :-** [www.networkkings.org](http://www.networkkings.org)

**Facebook page** [www.facebook.com/networkkingss](https://www.facebook.com/networkkingss)

## Basics of Networking

### **What is a network anyway?**

*A network is just a collection of devices and end systems connected to each other and able to communicate with each other. These could be computers, servers, smartphones, routers etc. A network could be as large as the internet or as small as your two computers at home sharing files and a printer.*

### **Some of the components that make up a network:**

**Personal Computers (PC):** These are the endpoint of your network, sending and receiving data.

**Interconnections:** These are components that make sure data can travel from one device to another, you need to think about:

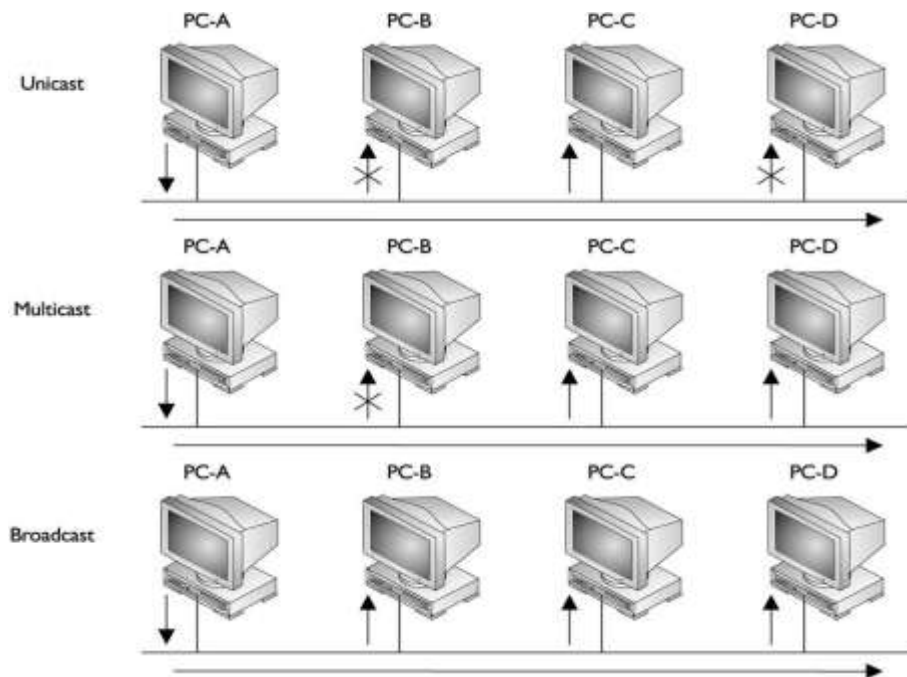
**Network Cards:** they translate data from your computer in a readable format for the network.

**Media:** network cables, perhaps wireless.

**Connectors:** the plug you plug in your network card.

**Switches:** These boxes are network devices which provide a network connection for your end devices like PC's.

**Routers:** Routers interconnect networks and choose the best path to each network destination



### SOME BASIC THINGS BEFORE STARTING CCNA !

**ping** :- packet internet gopher

it uses icmp ( internet control message protocol) protocol

for verification the other device is reachable to me or not ??

**ipconfig** :- to check the ip address of a computer

ipconfig /all :- to check the ip address + mac address

getmac :- to check the mac address of a computer

netstat :- to check the session's

nslookup :- to check the all servers of a website

arp -a :- to check arp table

arp -d :- to delete arp table ( run as administrator)

### **TO check public ip**

Visit :- [www.whatismyipaddress.com](http://www.whatismyipaddress.com) to check your public ip

### **To assign address to your PC**

1. windows button + R
2. type `ncpa.cpl` to go to your network connections
- 3 choose your lan adapter and go to properties and click on IPV4

### **NIC :- NETWORK INTERFACE CARD** **Mac address is embeded on nic**

is a [computer hardware](#) component that connects a [computer](#) to a [computer network](#).



## **TYPES of APPLICATIONS**

### **Batch applications**

File transfers like FTP, TFTP, perhaps a HTTP download. Could be a backup at night.  
No direct human interaction.  
High bandwidth is important but not critical.

### **Interactive applications**

Human-to-Human interaction  
Someone is waiting for a response, so response time (delay) is important

### **Real-time applications**

Also Human-to-Human interaction  
VoIP (Voice over IP) or live Video conferencing.  
End-to-end delay is critical

## Devices

### HUB

- ALWAYS do Broadcast
- Layer 1 device
- Shared bandwidth
- Less no of ports
- Doesn't learn mac address



### SWITCH

- which connects two or more computers together
- Many no of ports
- Learn mac address
- Two types of switch :-
- Manageble switch and unmanageable switch
- Layer 2 devices, datalink layer ( mac address )

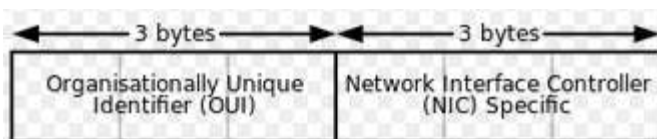


### ROUTER:



- *It is an internetworking device used to connect two or more different networks*
- *It works on layer 3 i.e. network layer*
- *.It Performs Routing*

### MAC Address vs IP Address



IP networks require two types of addresses. *MAC* and *IP*. Each station stores it's MAC address and IP address in it's own IP stack. It stores MAC and IP addresses of other stations on it's LAN or subnet in the ARP cache.

- When the packet is being sent out to a station that is on the same network LAN segment, *only the MAC address is needed.*
- When the packet goes beyond, to different networks and travels through routers, the MAC address is still contained in the packet, but *only the IP address is used by the routers.*

## IP ADDRESS

- An Internet Protocol address is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication
- *IP Address is Logical Address. It is a Network Layer address (Layer 3)*
- *Two Versions of IP:*  
*IP version 4 is a 32 bit address*  
*IP version 6 is a 128 bit address*

### IP version 4

*Bit is represent by 0 or 1 (i.e. Binary)*

*IP address in binary form (32 bits):*

**01010101000001011011111100000001**

*32 bits are divided into 4 Octets:*

**01010101. 00000101. 10111111. 00000001**

*IP address in decimal form:*

**85.5.191.1**

### IP version 6

*128-bit address is divided along 16-bit boundaries, and each 16-bit block is converted to a 4-digit hexadecimal number and separated by colons (Colon-Hex Notation)*

**FEDC:BA98:7654:3210:FEDC:BA98:7654:3210**

## IPV4

*Total IP Address Range of IPv4 is **0.0.0 .0 to 255.255.255.255***

*IP Addresses are divided into 5 Classes*

*CLASS A, B, C                      used in LAN & WAN*

*CLASS D                              reserved for Multicasting*

*CLASS E                              reserved for R & D*



CLASS	Class Ranges	Octet Format	No. Networks & Hosts
<b>A</b>	<b>0.0.0.0 - 127.255.255.255</b>	<b>N.H.H.H</b>	<b>126 Networks &amp; 16,777,214 Hosts per Network</b>
<b>B</b>	<b>128.0.0.0 - 191.255.255.255</b>	<b>N.N.H.H</b>	<b>16384 Networks &amp; 65534 Hosts per Network</b>
<b>C</b>	<b>192.0.0.0 - 223.255.255.255</b>	<b>N.N.N.H</b>	<b>2097152 Networks &amp; 254 Hosts per Network</b>
<b>D</b>	<b>224.0.0.0 - 239.255.255.255</b>		
<b>E</b>	<b>240.0.0.0 - 255.255.255.255</b>		

### IP Terminology:

<b>Bit(s)</b>	A bit has 2 possible values, 1 or 0. (on or off)
<b>Byte</b>	A byte is 8 bits.
<b>Octet</b>	An octet is just like a byte 8 bits, you often see byte or octet both being used.
<b>Nibble</b>	A nibble is 4 bits, we'll talk about this more in the Hexadecimal chapter.
<b>Network address</b>	When we talk about routing, the network address is important. Routers use the network address to send IP packets to the right destination. 192.168.1.0 with subnet mask 255.255.255.0 is an example of a network address.
<b>Subnet</b>	A subnet is a network that you split up in multiple smaller subnetworks.
<b>Broadcast address</b>	The broadcast address is being used by applications and computers to send information to all devices within a subnet, 192.168.1.255 with subnet mask 255.255.255.0 is an example of a broadcast address.

### Network & Broadcast Address

- The network address is represented with all bits as ZERO in the host portion of the address
- The broadcast address is represented with all bits as ONES in the host portion of the address
- Valid IP Addresses lie between the Network Address and the Broadcast Address.
- Only Valid IP Addresses are assigned to hosts/clients

### Private IP Address

There are certain addresses in each class of IP address that are reserved for Private Networks. These addresses are called private addresses.

<b>Class A</b>	<b>10.0.0.0</b>	<b>to</b>	<b>10.255.255.255</b>
<b>Class B</b>	<b>172.16.0.0</b>	<b>to</b>	<b>172.31.255.255</b>
<b>Class C</b>	<b>192.168.0.0</b>	<b>to</b>	<b>192.168.255.255</b>

PRIVATE IP	PUBLIC IP
<ul style="list-style-type: none"> <li>• Used with the LAN or within the organization</li> <li>• Not recognized on internet</li> <li>• Given by the administrator</li> <li>• Unique within the network or organization</li> <li>• Free</li> <li>• Unregistered IP</li> </ul>	<ul style="list-style-type: none"> <li>• Used on public network ( INTERNET)</li> <li>• Recognized on internet</li> <li>• Given by the service provider ( from IANA)</li> <li>• Globally unique</li> <li>• Pay to service provider ( or IANA )</li> <li>• Registered</li> </ul>

### Subnet Mask

*Subnet Mask:-Its an address used to identify the network and host portion of the ip address*

<b>Class A</b>	<b>N.H.H.H</b>	<b>255.0.0.0</b>
<b>Class B</b>	<b>N.N.H.H</b>	<b>255.255.0.0</b>
<b>Class C</b>	<b>N.N.N.H</b>	<b>255.255.255.0</b>

*Note:- "255" represents the network and "0" represents host.*

**Network:-** collection / group hosts

**Host:-** Single PC/ computer.

**Default Gateway:-** Its an entry and exit point of the network.  
ex:- The ip address of the router ethernet address.

## SUBNETTING

*It is the process of Dividing a Single Network into Multiple Networks.  
Converting Host bits into Network Bits i.e. Converting 0's into 1's  
Subnetting can be perform in two ways.*

1. FLSM (Fixed Length Subnet Mask)
2. VLSM (Variable Length subnet mask)

*Subnetting can be done based on requirement .*

*Requirement of Hosts ?  $2^h - 2 \geq \text{requirement}$*

*Requirement of Networks ?  $2^n \geq \text{requirement}$*

### 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).*



$$2^1 = 2$$

$$2^2 = 4$$

$$2^3 = 8$$

$$2^4 = 16$$

$$2^5 = 32$$

$$2^6 = 64$$

$$2^7 = 128$$

$$2^8 = 256$$

$$2^9 = 512$$

$$2^{10} = 1024$$

$$2^{11} = 2048$$

$$2^{12} = 4096$$

$$2^{13} = 8192$$

$$2^{14} = 16384$$

$$2^{15} = 32768$$

$$2^{16} = 65536$$

$$2^{17} = 131072$$

### FLSM : Example-- 1

**Req = 40** hosts using C-class address network 192.168.1.0/24

1.  $2^h - 2 \geq \text{req}$

$$2^6 - 2 \geq 40$$

$$64 - 2 \geq 40$$

$$62 \geq 40$$

Host bits required (**h**) = **6**

2. Converted network Bits (n) = Total. H. Bits -- req. H. Bits  
 $= 8 - 6 = 2$  (**n**)

4. Total . Network Bits = total network bits + converted bits =  $24 + 2 = /26$   
 subnet mask = (/26) = 255.255.255.192

5. Blocksize =  $2^h = 2^6 = 64$

6. Subnets =  $2^n = 2^2 = 4$  Subnets

7. Range :

Network ID --- Broadcast ID

192.168.1.0/26 ----- 192.168.1.63/26

192.168.1.64/26 ----- 192.168.1.127/26

192.168.1.128/26 ----- 192.168.1.191/26

192.168.1.192/26 ----- 192.168.1.255/26

**FLSM : Example-- 2**

1. Req = 500 hosts using B-class address network 172.16.0.0/16

$2^h - 2 \geq \text{req}$

$2^9 - 2 \geq 500$

$512 - 2 \geq 500$

$510 \geq 500$

2. Host bits required (h) = 9

3. **Converted network Bits (n)** = Total. H. Bits -- req. H. Bits  
 $= 16 - 9 = 7 \text{ (n)}$

3. Total . Network Bits = total network bits + converted bits  $= 16 + 7 = /23$   
 subnet mask = (/23) = 255.255.254.0

6. **Blocksize** =  $2^h = 2^9 = 512$

7. **Subnets** =  $2^n = 2^7 = 128$  Subnets

**Range**

Network ID --- Broadcast ID

172.16.0.0/23 --- 172.16.1.255/23

172.16.2.0/23 --- 172.16.3.255/23

172.16.4.0/23 --- 172.16.5.255/23

172.16.6.0/23 --- 172.16.7.255/23

**FLSM : Example-- 3**

1. Req = 2000 hosts using A-class address network 10.0.0.0/8

$2^h - 2 \geq \text{req}$

$2^{11} - 2 \geq 2000$

$2048 - 2 \geq 2000$

$2046 \geq 2000$

2. Host bits required (h) = 11

3. **Converted network Bits (n)** = Total. H. Bits -- req. H. Bits  
 $= 24 - 11 = 13 \text{ (n)}$

4. **Converted network Bits (n)** = 13

5. Total . N. Bits =  $8 + 13 = /21$

subnet mask = (/21) = 255.255.248.0

6. **blocksize** =  $2^h = 2^{11} = 2048$

7. **Subnets** =  $2^n = 2^{13} = 8192$  Subnets

**8. Range:**

Network ID --- Broadcast ID

10.0.0.0/21 ... 10.0.7.255/21

10.0.8.0/21 ... 10.0.15.255/21

10.0.16.0/21 ... 10.0.23.255/21

...

...

10.0.248.0/21 ... 10.0.255.255/21

10.1.0.0/21 --- 10.1.7.255/21

10.1.8.0/21 --- 10.1.15.255/21

10.1.16.0/21 --- 10.1.23.255/21

.....

10.1.248.0/21 ... 10.1.255.255/21

10.2.0.0/21 --- 10.2.7.255/21

10.2.8.0/21 --- 10.2.15.255/21

10.2.16.0/21 --- 10.2.23.255/21

...

...

10.2.248.0/21 ... 10.2.255.255/21

...

...

...

10.255.0.0/21 --- 10.0.7.255/21

10.255.8.0/21 --- 10.0.15.255/21

10.255.16.0/21 --- 10.0.23.255/21

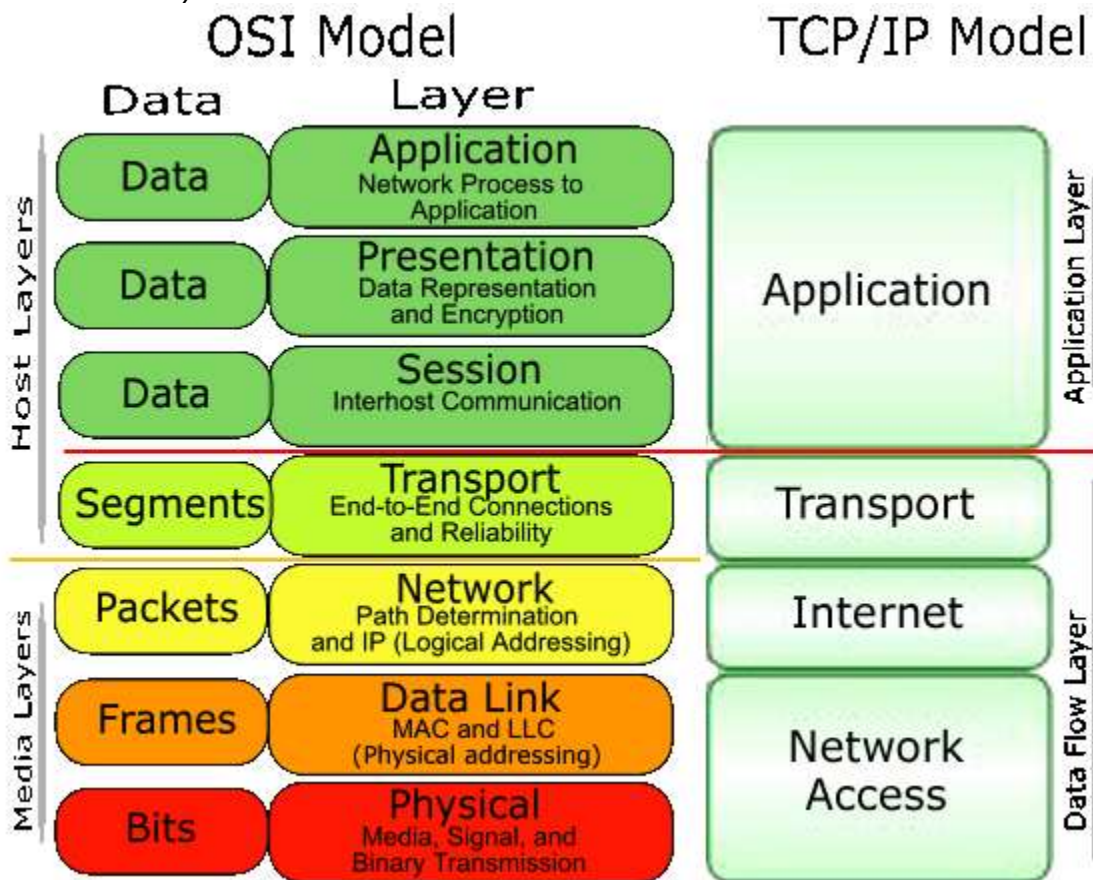
...

...

10.255.248.0/21 ... 10.255.255.255/21

## OSI Reference Model

- OSI was developed by the International Organization for Standardization (ISO) and introduced in 1984.
- It is a layered architecture (consists of seven layers).
- Each layer defines a set of functions in data communication.



## **All People Seem To Need Data Processing**

**Physical Layer:** This layer describes stuff like voltage levels, timing, physical data rates, physical connectors and so on. Everything you can “touch” since it’s physical.

- *It deals with physical transmission of Binary data on the given media (copper, Fiber, wireless..).*
- *It also deals with electrical, Mechanical and functional specifications of the devices, media.. etc*
- *The major functions described at this layer are..*

**Encoding/decoding:** *It is the process of converting the binary data into signals based on the type of the media.*

Copper media :	Electrical signals of different voltages
Fiber media :	Light pulses of different wavelengths
Wireless media:	Radio frequency waves

**Mode of transmission of signals:** *Signal Communication happens in three different modes Simplex, Half-duplex, Full-duplex*

*Devices works at physical layer are Hub, Modems, Repeater, Transmission Media*

**Data Link:** This layer makes sure data is formatted the correct way, takes care of error detection and makes sure data is delivered reliably. This might sound a bit vague now, for now try to remember this is where “Ethernet” lives. MAC Addresses and Ethernet frames are on the Data Link layer.

*Data link layer comprises of two sub-layers.*

### **1) MAC (Media Access Control)**

*It deals with hardware addresses (MAC addresses).*

*MAC addresses are 12 digit Hexa-decimal identifiers used to identify the devices uniquely on the network segment.*

*It also provides ERROR DETECTION using CRC (Cyclic Redundancy Check) and FRAMING (Encapsulation).*

*Ex: Ethernet, Token ring...etc*

### **2) LLC (Logical Link Control)**

*It deals with Layer 3 (Network layer)*

*Devices works at Data link layer are Switch, Bridge, NIC card.*

**Network:** This layer takes care of connectivity and path selection (routing). This is where IPv4 and IPv6 live. Every network device needs a unique address on the network.

*It is responsible for end-to end Transportation of data across multiple networks.*

*Logical addressing & Path determination (Routing) are described at this layer.*

*The protocols works at Network layer are*

**Routed Protocols:**

*Routed protocols acts as data carriers and defines logical addressing.*

IP, IPX, AppleTalk.. Etc

**Routing Protocols:**

*Routing protocols performs Path determination (Routing).*

RIP, IGRP, EIGRP, OSPF.. Etc

*Devices works at Network Layer are Router, Multilayer switch etc..*

**Transport:** The transport layer takes care of transport, when you downloaded this book from the Internet the file was sent in segments and transported to your computer.

- o TCP lives here; it's a protocol which send data in a reliable way.
- o UDP lives here; it's a protocol which sends data in an unreliable way.
  - ICMP lives here; when you send a ping you are using ICMP.
    - Identifying Service
    - Multiplexing & De-multiplexing
    - Segmentation
    - Sequencing & Reassembling
    - Error Correction
    - Flow Control

**Identifying a Service :** Services are identified at this layer with the help of Port No's. The major protocols which takes care of Data Transportation at Transport layer are...TCP,UDP

<b>Transmission Control Protocol</b>	<b>User Datagram Protocol</b>
<ul style="list-style-type: none"> <li>• Connection Oriented</li> <li>• Reliable communication( with Ack's )</li> <li>• Slower data Transportation</li> <li>• Protocol No is 6</li> <li>• Eg: HTTP, FTP, SMTP</li> </ul>	<ul style="list-style-type: none"> <li>• Connection Less</li> <li>• Unreliable communication ( no Ack's )</li> <li>• Faster data Transportation</li> <li>• Protocol No is 17</li> <li>• Eg: DNS, DHCP, TFTP</li> </ul>

**FLOW CONTROL**

*Flow control is used to control the data flow between the connection. If for any reason one of the two hosts are unable to keep up with the data transfer, it is able to send special signals to the other end, asking it to either stop or slow down so it can keep up.*

*The following diagram explains the procedure of the 3-way handshake:*



### 3-way handshake

**STEP 1:** Host A sends the initial packet to Host B. This packet has the "SYN" bit enabled. Host B receives the packet and sees the "SYN"

**STEP 2:** Assuming Host B has enough resources, it sends a packet back to Host A and with the "SYN and ACK".

**STEP 3:** After all that, Host A sends another packet to Host B and with the "ACK" bit set (1), it effectively tells Host B 'Yes, I acknowledge your previous request'.

**Session:** The session layer takes care of establishing, managing and termination of sessions between two hosts. When you are browsing a website on the internet you are probably not the only user of the webserver hosting that website. This webserver needs to keep track of all the different "sessions".

**Presentation:** This one will make sure that information is readable for the application layer by formatting and structuring the data. Most computers use the ASCII table for characters. If another computer would use another character like EBCDIC than the presentation layer needs to "reformat" the data so both computers agree on the same characters.

**Application:** Here are your applications. E-mail, browsing the web (HTTP), FTP and many more.

## PortNumbers

**TCP/UDP :- Both have 65535 ports**

1- 1023	well known
1024 - 49151	registered ports
49152 - 65535	dynamic ports ( generated by host)



Port Number	Protocol	Application
20	TCP	FTP data
21	TCP	FTP control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP	DNS
67, 68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
16,384–32,767	UDP	RTP-based Voice (VoIP) and Video

## Cabling

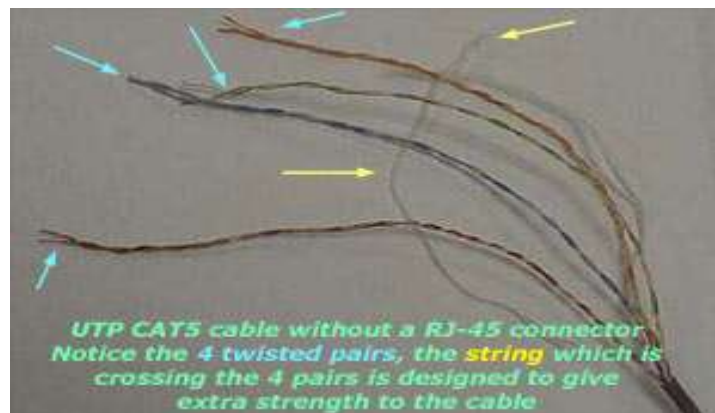
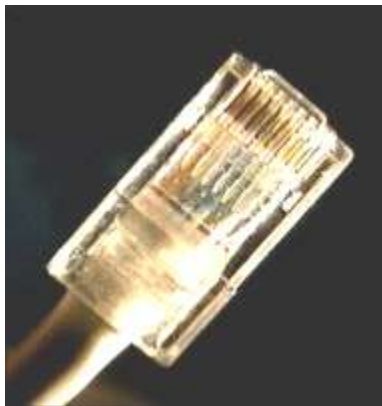
The UTP Categories		
<b>Cat 1</b>	<b>Data rate up to 1Mbps</b>	<b>- Traditional Telephone &amp; ISDN - Modem</b>
<b>Cat 2</b>	<b>Data rate up to 4 Mbps</b>	<b>- Token Ring</b>
<b>Cat 3</b>	<b>Data rate up to 10Mbps</b>	<b>- Token Ring &amp; 10BASE-T</b>
<b>Cat 4</b>	<b>Data rate up to 16Mbps</b>	<b>- Token Ring</b>
<b>Cat 5</b>	<b>Data rate up to 100Mbps</b>	<b>- Ethernet (10Mbps), Fast Ethernet (100Mbps) and Token ring (16Mbps)</b>
<b>Cat 5e</b>	<b>Data rate up to 1000Mbps</b>	<b>- Gigabit Ethernet</b>
<b>Cat 6</b>	<b>Data rate up to 1000Mbps</b>	<b>- Gigabit Ethernet</b>
<i>The 6 different Unshielded Twisted Pair catagories  Max length depends on network topology and protocol  UTP is mostly used in Star Topologies</i>		

UTP has 4 twisted pairs of wires, we'll now look at the pairs to see what colour codes they have:



As you can see in the picture above, the 4 pairs are labeled. Pairs 2 & 3 are used for normal 10/100Mbit networks, while Pairs 1 & 4 are reserved. In Gigabit Ethernet, all 4 pairs are used.

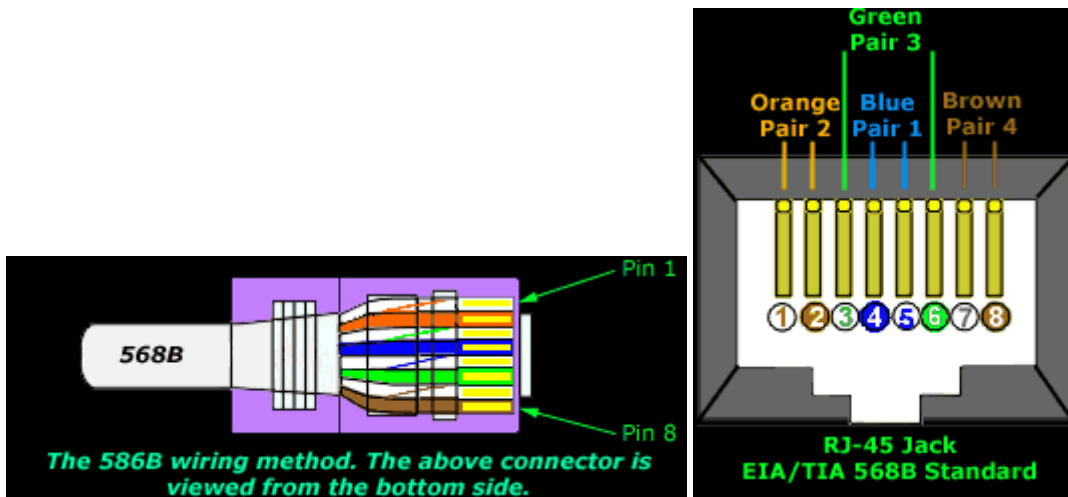
UTP CAT5, 5e & 6 cable is the most common type of UTP around the world ! It's flexible, easy to install and very reliable when wired properly.



There are two wiring standards for these cables, called "T568A" (also called "EIA") and "T568B" (also called "AT&T" and "258A"). They differ only in connection sequence - that is, which color is on which pin, not in the definition of what electrical signal is on a particular color.

#### Pin Number Designations for T568B

Note that the odd pin numbers are always the white with stripe color (1,3,5,7). The wires connect to RJ-45 8-pin connectors as shown below:

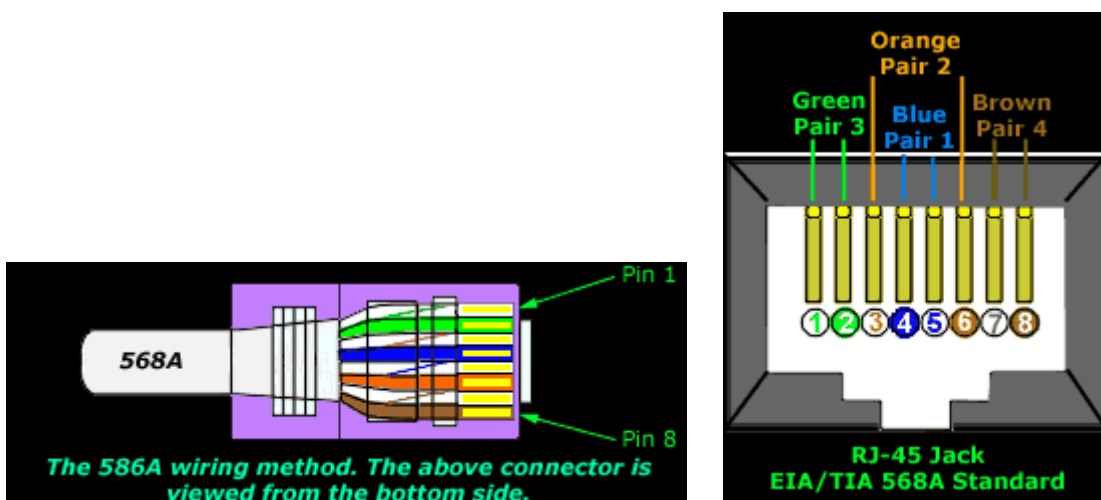


#### Color Codes for T568B

Pin	Color	Pair Name
1	white/orange (pair 2)	TxData +
2	orange (pair 2)	TxData -
3	white/green (pair 3)	RecvData+
4	blue (pair 1)	
5	white/blue (pair 1)	
6	green (pair 3)	RecvData-
7	white/brown (pair 4)	
8	brown (pair 4)	

#### Pin Number Designations for T568A

The T568A specification reverses the orange and green connections so that pairs 1 and 2 are on the centre 4 pins, which makes it more compatible with the telco voice connections. (Note that in the RJ-11 plug at the top, pairs 1 and 2 are on the centre 4 pins.) T568A goes:



Color Codes for T568A

Pin	Color -	Pair Name
1	white/green (pair 3)	RecvData+
2	green (pair 3)	RecvData-
3	white/orange (pair 2)	TxData +
4	blue (pair 1)	
5	white/blue (pair 1)	
6	orange (pair 2)	TxData -
7	white/brown (pair 4)	
8	brown (pair 4)	

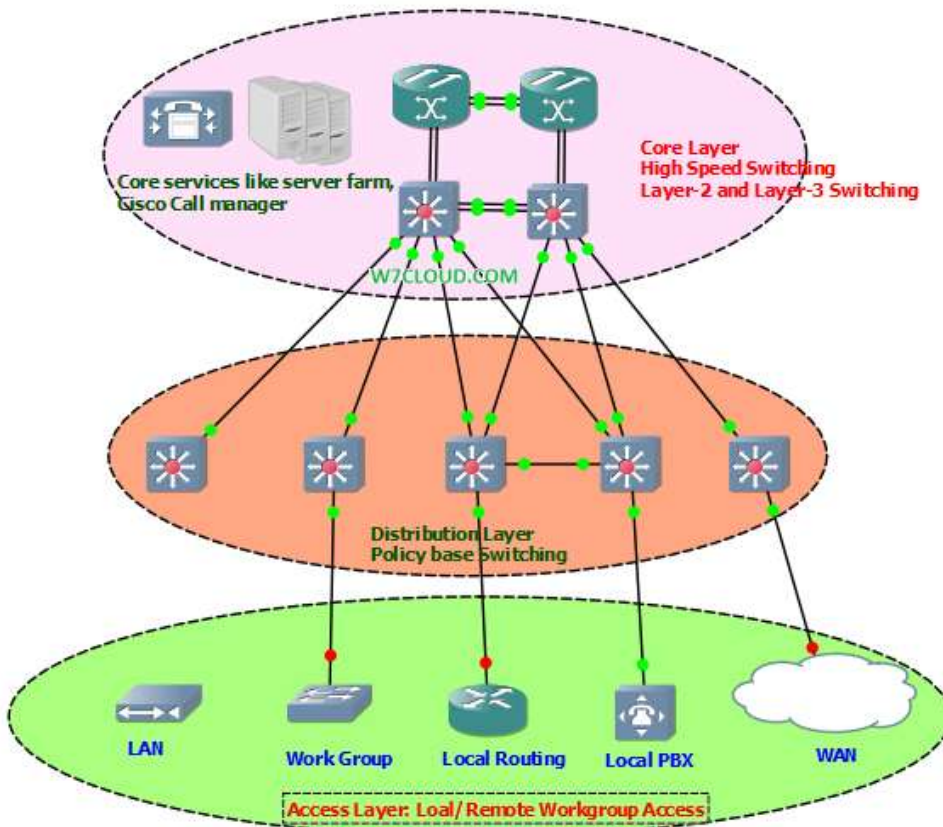
## Advantages of Cisco 3-Layered model:

Provide the flexibility in our network with three layers distribution, each layer is mapped with physical implementation and each of layers has its own features and functionality.

3 layer model is easier to understand and easy to grow your network.

3 layer model is easy to troubleshoot because of its logical distribution into layer, as each layer has its own functionality.

Allow us the lower cost in implementation.



Some of key characteristics of core-layer are as following:

- Fast transport and large amount of data
- Redundancy
- High reliability and availability
- Low latency and good manageability
- Quality of service (QoS) classification, or other processes
- Fault tolerance
- Limited and consistent diameter

**Some of key characteristics of distribution-layer are as following:**

- Route filtering by source or destination address and filtering on input or output ports
- Hiding internal network numbers by route filtering
- Policy-based connectivity
- Static routing
- QoS mechanisms, such as priority-based queuing

**Some of key characteristics of access-layer are as following:**

- High availability
- Layer 2 switching
- Port security

## INTRODUCTION TO ROUTERS

### What is a Router ?

- Router is a device which makes communication possible between two or more different networks present in different geographical locations.
  - 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:-
  - Select the best path from the routing table.
  - Forward the packet on that path

### Which Routers to buy ?

Many companies are manufacturing Router :

- Cisco
- Nortel
- Multicom
- Cyclades
- Juniper
- Dlink
- Linksys
- 3Com

But Cisco is having Monopoly in the market of Routers

### Cisco's Hierarchical Design Model

Cisco divided the Router into 3 Layers

- Access Layer Router
- Distribution Layer Router
- Core Layer Router

### Access Layer Router

- Routers which are used by the Small Organization and are also known as Desktop or Company Layer Routers.

Router Series : 800, 1900, Old ones :- 1600, 1700, 2500



**Cisco 800**



**Cisco 1700**



**Cisco 1760**

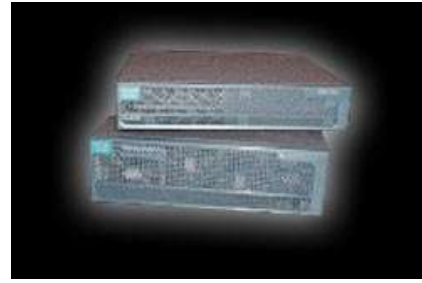
### Distribution Layer Router

- Routers which are used by the ISPs and are also known as ISP Layer Routers  
Router Series : 3800, 3900 old one :- 2600, 3200, 3600, 3700

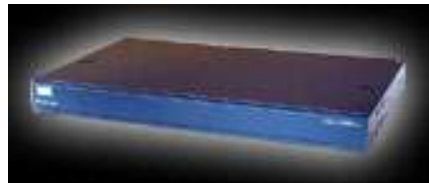




**Cisco 3600**



**Cisco 3700**



**Cisco 2600XM/2691**

### **Core Layer Router**

- Routers which are used by the Global ISPs and are also known as Backbone Routers  
Router Series : 6400, 7200, 7300, 7400, 7500, 7600, 10000, 12000



**Cisco 7000**

### **Router Classification**

<b>FIXED ROUTER</b>	<b>MODULAR ROUTER</b>
<ul style="list-style-type: none"> <li>• Fixed router (Non Upgradable cannot add and remove the Ethernet or serial interfaces)</li> <li>• Access Layer Routers are example of Fixed Router except 1600 and 1700 series</li> </ul>	<ul style="list-style-type: none"> <li>• Modular router (Upgradable can add and remove interfaces as per the requirement)</li> <li>• Distribution and Core Layer Routers example of Modular Router</li> </ul>

### Example Modular Router



### Attachment Unit Interface

- AUI pin configuration is 15 pin female.
- It is known as Ethernet Port or LAN port or Default Gateway.
- It is used for connecting LAN to the Router.
- **Transceiver** is used for converting 8 wires to 15 wires. i.e. RJ45 to 15 pin converter.



### Serial Port

- Serial pin configuration is 60 pin configuration female (i.e. 15 pins and 4 rows) and Smart Serial pin configuration is 26 pin configuration female.
- It is known as WAN Port
- It is used for connecting to Remote Locations
- V.35 cable is having 60 pin configuration male at one end and on the other end 18 pin configuration male.

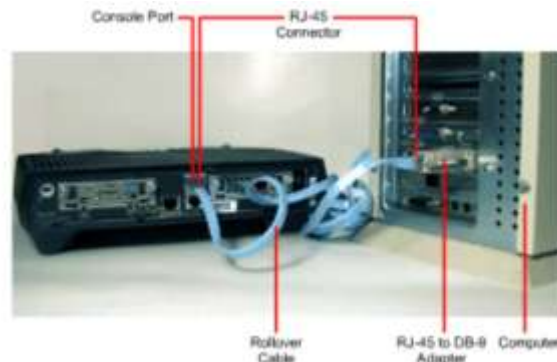


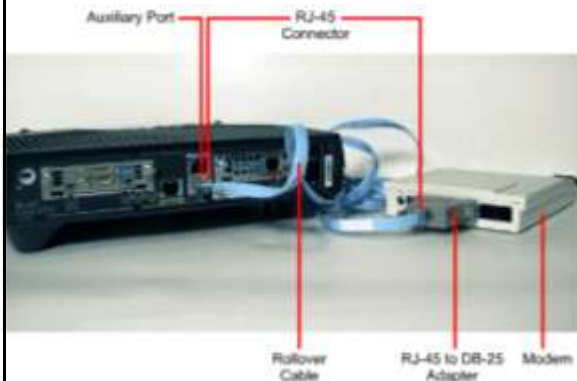
### Console Port

- It is known as Local Administrative Port
- It is generally used for Initial Configuration, Password Recovery and Local Administration of the Router. It is RJ45 Port
- **IMP** : It is the most delicate port on the Router. So make less use of the Console Port.

### Console Connectivity

- Connect a rollover cable to the router console port (RJ-45 connector).
- Connect the other end of the rollover cable to the RJ-45 to DB-9 converter
- Attach the female DB-9 converter to a PC Serial Port.
- Open Emulation Software

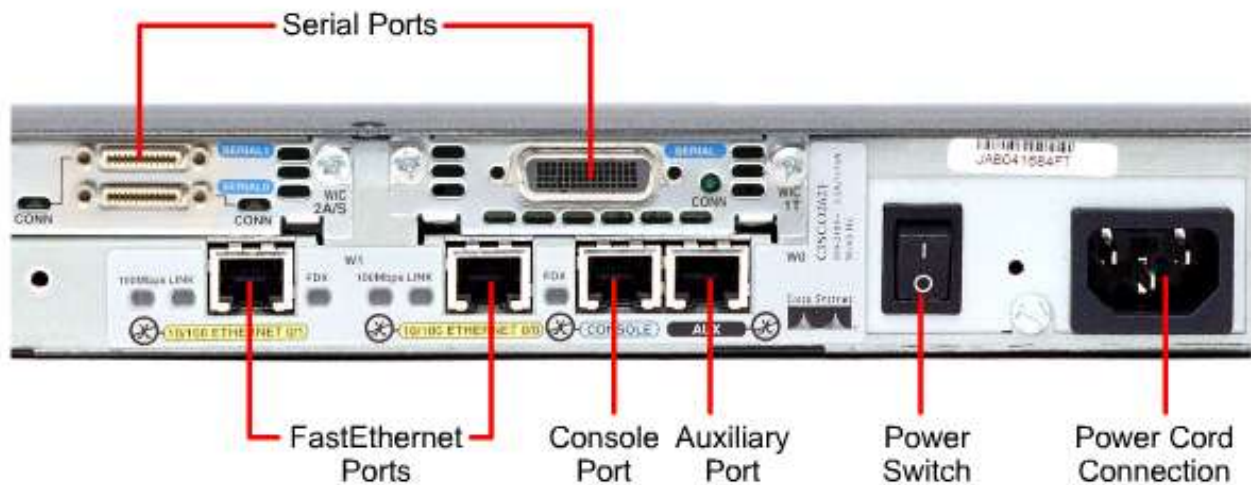




### Auxiliary Port

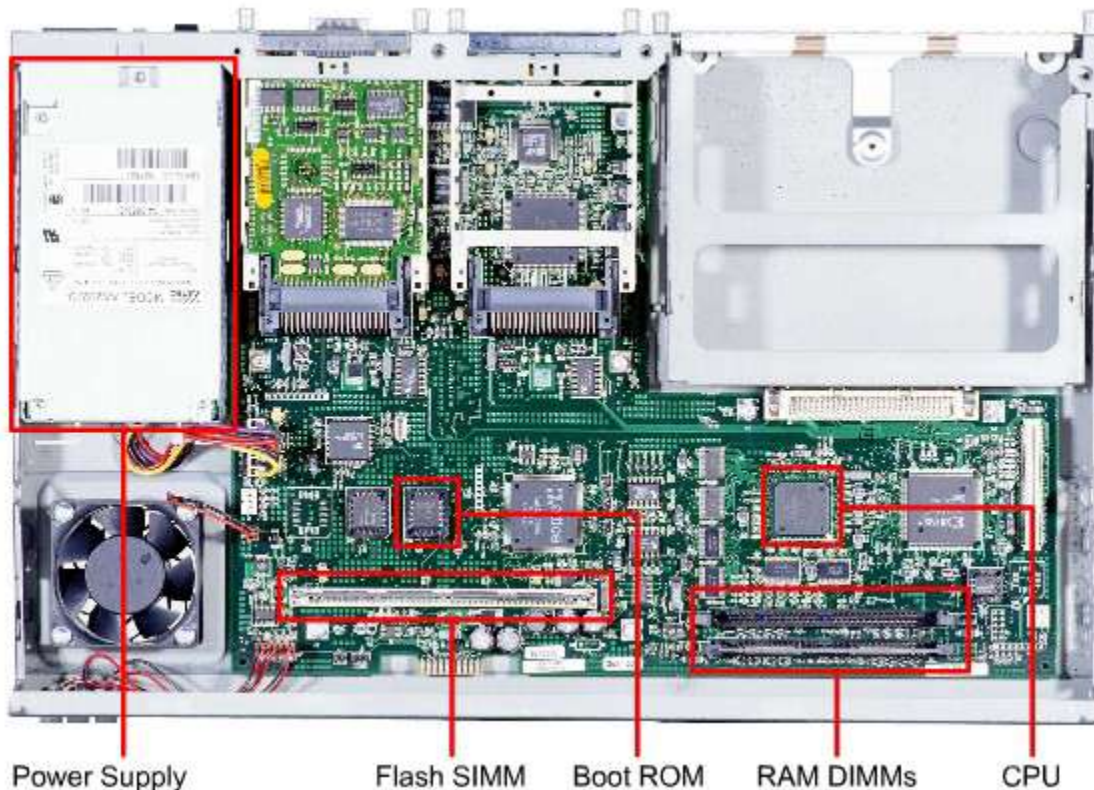
- It is known as Remote Administrative Port.
- Used for remote administration
- Its an RJ-45 port
- A console or a rollover cable is to be used.

## 2601 Model Router



### Brief Overview

- WAN interfaces
  - Serial interface (S0, S1 etc) - 60 pin/26 pin (smart serial)
  - ISDN interface (BRI0 etc) - RJ45
- LAN interfaces - Ethernet
  - AUI (Attachment Unit Interface) (E0) - 15 pin
  - 10baseT - RJ45
- Administration interfaces
  - Console - RJ45 - Local Administration
  - Auxiliary - RJ45 - Remote Administration

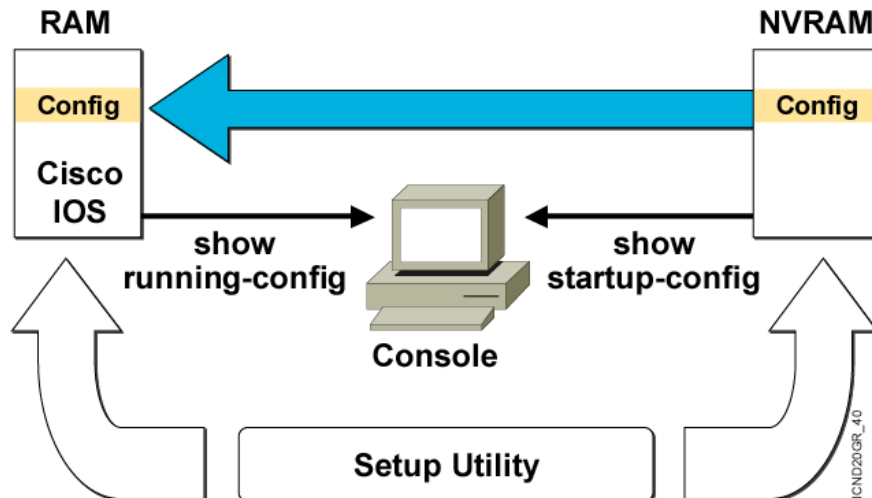


### Internal Components

- **ROM**  
A bootstrap program is located here. It is same as the BIOS of the PC. Bootstrap program current version is 11.0
- **Flash**  
Internetwork Operating System (IOS) developed by Cisco is stored here. IOS is Command line interface.
- **NVRAM**  
Non volatile RAM, similar to Hard Disk It is also known as Permanent Storage or Startup Configuration. Generally size of NVRAM is 32 KB.
- **RAM**  
It is also known as Temporary Storage or running Configuration. Minimum size of RAM is 2MB. The size of RAM is greater than NVRAM in the Router.
- **Processor**  
Motorola Processor 70 Mhz, RISC based processor (Reduced Instruction Set Computer)

### Router Start-up Sequence

- Bootstrap program loaded from ROM
- Bootstrap runs the POST
- Bootstrap locates IOS in Flash
- IOS is expanded and then loaded into RAM
- Once IOS is loaded into RAM, it looks for startup-config in NVRAM
- If found, the configuration is loaded into RAM

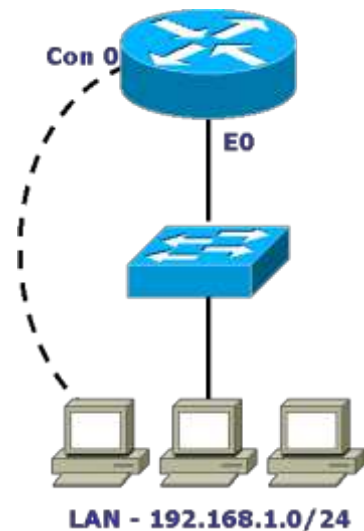


## MODES OF A ROUTER:-

- **User Mode:-**  
Only some basic monitoring
- **Privileged Mode:-**  
monitoring and some troubleshooting
- **Global Configuration mode:-**  
All Configurations that effect the router globally
- **Interface mode:-**  
Configurations done on the specific interface
- **Rommon Mode:-** Reverting Password

### Console Connectivity

- Connect a rollover cable to the router console port (RJ-45 connector).
- Connect the other end of the rollover cable to the RJ-45 to DB-9 converter
- Attach the female DB-9 converter to a PC Serial Port.
- Open emulation software on the PC.



### IN WINDOWS

- Start → Programs → Accessories → Communications → HyperTerminal → HyperTerminal.
- Give the Connection Name & Select Any Icon
- Select Serial (Com) Port where Router is Connected.
- In Port Settings → Click on Restore Defaults

### IN LINUX

- # minicom -s



## **Exercise- 1**

### **BASIC COMMANDS**

#### **User mode:**

Router >  
Router > enable

#### **Privilege mode:**

Router # show running-config  
Router # show startup-config  
Router # show flash  
Router # show version  
Router #show ip interface brief

Router # configure terminal ( to enter in Global configurarion mode)

#### **Global configuration mode:**

Router(config) #

#### **Assigning ip address to Ethernet interface:**

Router(config) # interface <interface type> <interface no>  
Router(config-if) # ip address <ip address> <subnet mask> (Interface Mode)  
Router(config-if) # no shut

#### **Assigning Telnet password:**

Router(config) # line vty 0 4  
Router(config-line) #login (line mode)  
Router(config-line) #password <password>  
Router(config-line) #exit  
Router(config) #exit

#### **Assigning console password:**

Router(config) # line con 0  
Router(config-line) # login (line mode)  
Router(config-line) # password <password>  
Router(config-line) # exit  
Router(config) # exit

#### **Assigning Auxiliary password:**

Router(config) # line aux 0  
Router(config-line) # login (line mode)  
Router(config-line) # password <password>  
Router(config-line) # exit  
Router(config) # exit

#### **Assigning enable password:**



Router(config) # enable secret <password>  
 Router(config) # enable password <password>

(To encrypt the password)

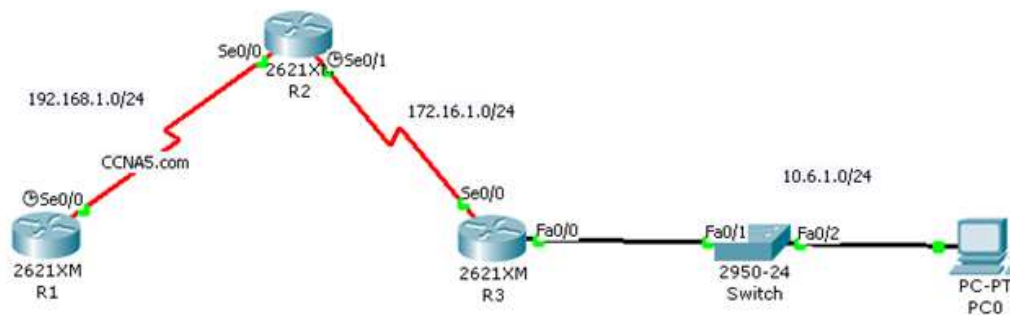
### **Show commands:**

Router # show running-config  
 Router # show startup-config  
 Router # show version  
 Router # show flash

### **Commands to save the configuration:**

Router # copy running-config startup-config  
 ( OR )  
 Router # write memory  
 ( OR )  
 Router # write

## **ROUTING**



### **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.

### **Rules of Routing**

- 1) All The Lan Should Be In Diffrenet Networks ( Should Not Repeat The Same Net)
- 2) Router Ethernet And The Pc's --> Same Networks
- 3) Routers Ports Facing Each Other --> Same Networks
- 4) All The Interfaces Of The Router --> Different Network

### **Types of Routing**

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

### Static Routing

- It is configured by Administrator manually.
- Mandatory need of Destination Network ID
- It is Secure & fast
- Used for Small organizations with a network of 10-15 Routers.
  - Administrative distance for Static Route is 0 and 1.
  - It is the "trustworthiness" of the routing information. Lesser the Administrative distance, higher the preference.

### Disadvantages :-

- Used for small network.
- Everything to manually
- Network change effect complete n/W

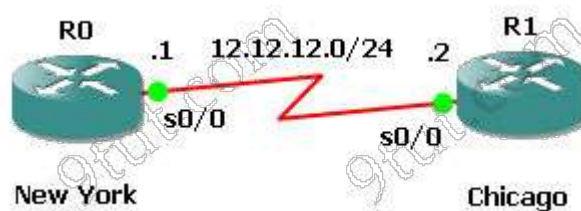
### Configuring Static Route

```
Router(config)# ip route <Destination Network ID>
<Destination Subnet Mask>
<Next-hop IP address >
```

Or

```
Router(config)# ip route <Destination Network ID>
<Destination Subnet Mask>
<Exit interface type> <interface number>
```

### Practical



### Configuring interfaces on R0

```
R0(config)#interface s0/0
R0(config-if)#ip address 12.12.12.1 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#interface lo0
R0(config-if)#ip address 10.0.0.1 255.0.0.0
R0(config-if)#exit
```

### Configuring interfaces on R1

```
R0(config)#interface s0/0
R0(config-if)#ip address 12.12.12.2 255.255.255.0
R0(config-if)#no shutdown
```

```
R0(config-if)#interface lo0
R0(config-if)#ip address 172.16.0.1 255.255.0.0
R0(config-if)#exit
```

Configuring static route on R0

```
R0(config)#ip route 172.16.0.0 255.255.0.0 12.12.12.2
```

Configuring static route on R1

```
R1(config)#ip route 10.0.0.0 255.0.0.0 12.12.12.1
```

## 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
- 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.

## Configuring Default Route

```
Router(config)# ip route <Destination Network ID> <Destination Subnet Mask>
                        <Next-hop IP address >
```

Or

```
Router(config)# ip route <Destination Network ID> <Destination Subnet Mask>
                        <Exit interface type><interface number>
```

## Troubleshooting commands:

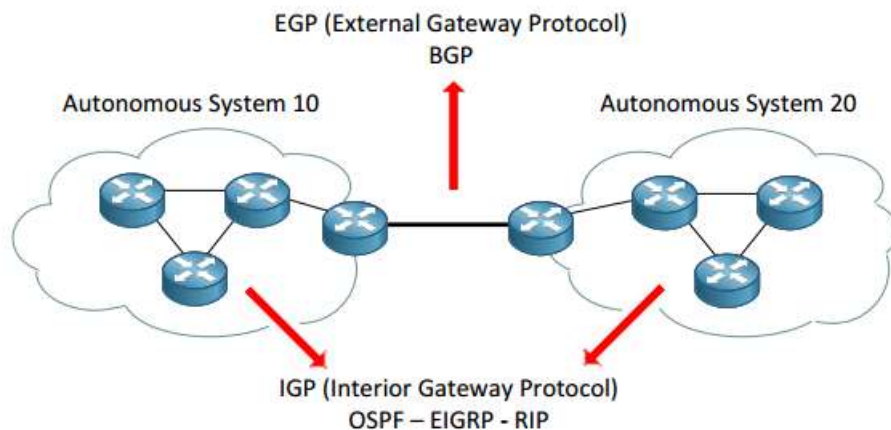
**Router # show ip interface Brief**

- 1) Serial is up , line protocol is up** (connectivity is fine)
- 2) Serial is administratively down, line protocol is down**  
(No Shutdown has to be given on the local router serial interface)
- 3) Serial is up, line protocol is down**  
(Encapsulation mismatch or clock rate has to be given on dce)
- 4) Serial is down, line protocol is down**  
(Serial interface on the remote router has to be configured)

## Routing Protocol Classification

IGP	EGP
<ul style="list-style-type: none"> <li>• Interior Gateway Protocol</li> <li>• Routing protocols used within an autonomous system</li> <li>• All routers will be routing within the same Autonomous boundary</li> <li>• RIP, IGRP, EIGRP, OSPF, IS-IS</li> </ul>	<ul style="list-style-type: none"> <li>▪ Exterior Gateway Protocol</li> <li>▪ Routing protocol used between different autonomous systems</li> <li>▪ Routers in different AS need an EGP</li> <li>▪ Border Gateway Protocol is extensively used as EGP</li> </ul>

- IGP's operate within an autonomous system
- EGP's connect different autonomous systems



## Dynamic Routing

*Advantages of Dynamic over static :*

- There is no need to know the destination networks.
- Need to advertise the directly connected networks.
- Updates the topology changes dynamically.
- Administrative work is reduced
- Used for large organizations.
- Neighbor routers exchange routing information and build the routing table automatically.

### Types of Dynamic Routing Protocols

- Distance Vector Protocol
- Link State Protocol
- Hybrid Protocol

Distance Vector Protocol	Link State Protocol	Hybrid Protocol
<ul style="list-style-type: none"> <li>• Works with Bellman Ford algorithm</li> <li>• Periodic updates</li> <li>• Classful routing protocol</li> </ul>	<ul style="list-style-type: none"> <li>• Works with Dijkstra algorithm</li> <li>• Link state updates</li> <li>• Classless routing</li> </ul>	<ul style="list-style-type: none"> <li>• Also called as Advance Distance vector Protocol</li> <li>• Works with DUAL algorithm</li> </ul>

- Full Routing tables are exchanged
- Updates are through broadcast
- Example: RIP 1, RIP 2, IGRP

- protocol
- Missing routes are exchanged
- Updates are through multicast
- Example : OSPF, IS-IS

- Link state updates
- Classless routing protocol
- Missing routes are exchanged
- Updates are through multicast
- 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.
- Default administrative distances are as follows :
  - Directly Connected = 0
  - Static Route = 1
  - IGRP = 100
  - OSPF = 110
  - RIP = 120
  - EIGRP = 90/170

### **Routing Information Protocol v1**

- Open Standard Protocol
- Classful routing protocol
- Updates are broadcasted via 255.255.255.255
- Administrative distance is 120
- Metric : Hop count
  - Max Hop counts : 15
  - Max routers : 16
- Load Balancing of 4 equal paths
- Used for small organizations
- Exchange entire routing table for every 30 seconds

### **Rip Timers**

- Update timer : 30 sec
  - Time between consecutive updates
- Invalid timer : 180 sec
  - Time a router waits to hear updates
  - The route is marked unreachable if there is no update during this interval.
- Flush timer : 240 sec
  - Time before the invalid route is purged from the routing table

### **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.

### **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
- Slow convergence

### **Configuring RIP 1**

```
Router(config)# router rip
Router(config-router)# network <Network ID>
```

### **Configuring RIP 2**

```
Router(config)# router rip
Router(config-router)# network <Network ID>
Router(config-router)# version 2
```

## **RIP other concepts**

### **SPLIT HORIZON:**

A router never sends information about a route back in same direction which is original information came, routers keep track of where the information about a route came from. Means when router A sends update to router B about any failure network, router B does not send any update for same network to router A in same direction.

### **ROUTE POISONING:**

Router consider route advertised with an infinitive metric to have failed ( metric=16) instead of marking it down. For example, when network 4 goes down, router C starts route poisoning by advertising the metric (hop count) of this network as 16, which indicates an unreachable network.

### **POISON REVERSE:**

The poison reverse rule overwrites split horizon rule. For example, if router B receives a route poisoning of network 4 from router C then router B will send an update back to router C (which breaks the split horizon rule) with the same poisoned hop count of 16. This ensures all the routers in the domain receive the poisoned route update.

Notice that every router performs poison reverse when learning about a downed network. In the above example, router A also performs poison reverse when learning about the downed network from B.

### **HOLD DOWN TIMERS:**

After hearing a route poisoning, router starts a hold-down timer for that route. If it gets an update with a better metric than the originally recorded metric within the hold-down timer period, the hold-down timer is



removed and data can be sent to that network. Also within the hold-down timer, if an update is received from a different router than the one who performed route poisoning with an equal or poorer metric, that update is ignored. During the hold-down timer, the "downed" route appears as "possibly down" in the routing table.

For example, in the above example, when B receives a route poisoning update from C, it marks network 4 as "possibly down" in its routing table and starts the hold-down timer for network 4. In this period if it receives an update from C informing that the network 4 is recovered then B will accept that information, remove the hold-down timer and allow data to go to that network. But if B receives an update from A informing that it can reach network by 1 (or more) hop, that update will be ignored and the hold-down timer keeps counting.

Note: The default hold-down timer value = 180 second.

#### TRIGGERED UPDATE :

When any route failed in network ,do not wait for the next periodic update instead send an immediate update listing the poison route.

#### COUNTING TO INFINITY:

Maximum count 15 hops after it will not be reachable.

#### Configuring RIP

Router(config)#router rip	Enter router RIP configuration mode
Router(config-router)#network<address>	Identify networks that will participate in the router protocol. Notice that you identify networks, and not interfaces.

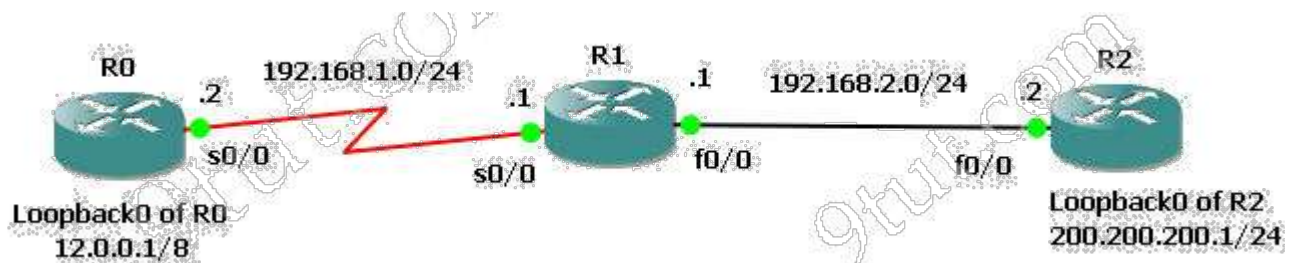
NOTE: You need to advertise only the classful network number, not a subnet:

Router(config-router)#network 172.16.0.0

not

Router(config-router)#network 172.16.10.0

## Practical



Configuring interfaces for R0, R1 & R2:

**R0(config)#interface s0/0**

**R0(config-if)#ip address 192.168.1.2 255.255.255.0**

**R0(config-if)#no shutdown**

```

R0(config-if)#interface lo0
R0(config)#ip address 12.0.0.1 255.0.0.0

R1(config)#interface s0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#interface f0/0
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#no shutdown

R2(config)#interface f0/0
R2(config-if)#ip address 192.168.2.2 255.255.255.0
R2(config-if)#interface lo0
R2(config-if)#ip address 200.200.200.1 255.255.255.0

```

### Now enable RIPv2 on three routers

```

R0(config)#router rip
R0(config-router)#version 2
R0(config-router)#network 12.0.0.0
R0(config-router)#network 192.168.1.0

R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0

R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 200.200.200.0
R2(config-router)#network 192.168.2.0

```

If you want to check what is inside the update packet, use the command **debug ip rip**.

To turn off the debug ip, use the command **undebug ip rip**. If you want to disable all the debug processes, use the command **undebug all**.

## Autonomous System Number

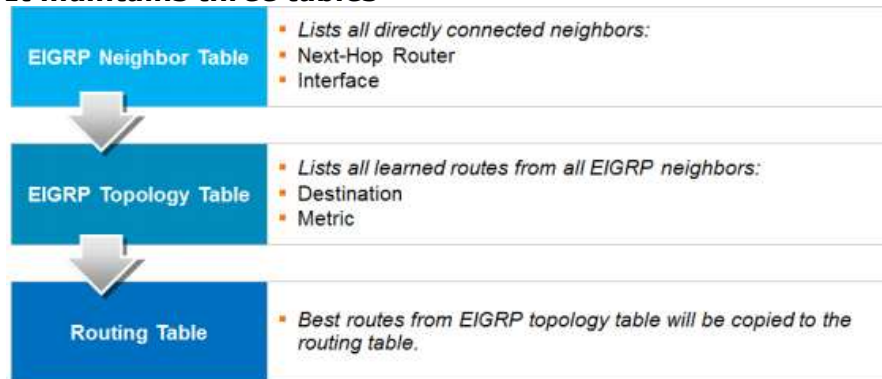
- A unique number identifying the Routing domain of the routers.
- An autonomous system is a collection of networks under a common administrative domain
- Ranges from 1- 65535
- Public – 1 – 64512                      Private – 64513 – 65535

## EIGRP - Enhanced Interior Gateway Routing Protocol

- Cisco proprietary protocol
- Classless routing protocol
- Includes all features of IGRP

- *Metric (32 bit) : Composite Metric (BW + Delay + load + MTU + reliability )*
- *Administrative distance is 90*
- *Updates are through Multicast (224.0.0.10 )*
- *Max Hop count is 255 (100 by default)*
- *Supports IP, IPX and Apple Talk protocols*
- *Hello packets are sent every 5 seconds*
- *Convergence rate is fast*
- *First released in 1994 with IOS version 9.21.*
- *Support VLSM and CIDR*
- *It uses DUAL (diffusion update algorithm)*
- *Summarization can be done on every router*
- *Supports equal and unequal cost load balancing*

- ***It maintains three tables***



- Neighbor table
- Topology table
- Routing table

### ***Disadvantages of EIGRP***

- *Works only on Cisco Routers*

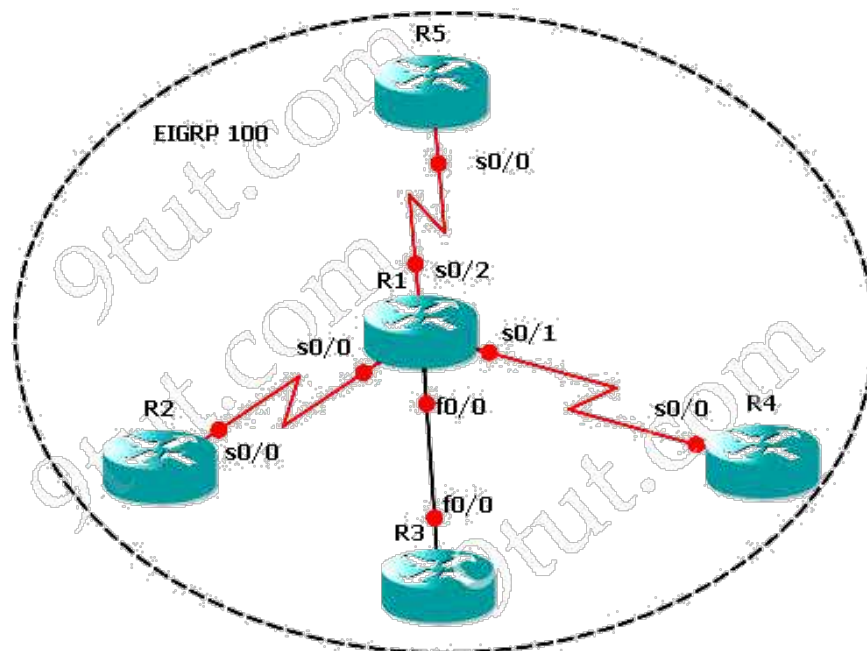
### ***Configuring EIGRP***

```
Router(config)# router eigrp <as no>
Router(config-router)# network <Network ID>
```

## ***Practical***

In this tutorial we will learn how to use EIGRP to run a small network with 5 routers. Below is the topology of this lab

This lab consists of 5 routers and we need to configure EIGRP among them. It is done when we can successfully ping among R2, R3, R4 & R5 and the routing tables of these routers show that they are running EIGRP (with letter "D").



### IP addresses of routers:

#### + R1:

s0/0 – 192.168.30.12/28

s0/1 – 192.168.30.18/28

s0/2 – 192.168.30.35/28

f0/0 – 192.168.60.10/28

#### + R2:

s0/0 – 192.168.30.13/28

#### + R3:

f0/0 – 192.168.60.13/28

#### + R4:

s0/0 – 192.168.30.20/28

#### + R5:

s0/0 – 192.168.30.40/28

### Some important notes about EIGRP:

+ All routers must use the same Autonomous System (AS) number to recognize each other. In this case the chosen AS is 100.

+ The major network in this lab is 192.168.30.0 & 192.168.60.0 so there will be discontinuous networks -> need to use the "no auto-summary" command.

Now let's begin the lab!

**Step 1 – Configuring IP addresses on the all the routers****Configure IP address Yourself !****Step 2 – Enable EIGRP on all the routers**

\*On R1

```
R1(config)#router eigrp 100
R1(config-router)#network 192.168.30.0
R1(config-router)#network 192.168.60.0
R1(config-router)#no auto-summary
```

\*On R2

```
R2(config)#router eigrp 100
R2(config-router)#network 192.168.30.0
R2(config-router)#no auto-summary
```

\*On R3

```
R3(config)#router eigrp 100
R3(config-router)#network 192.168.60.0
R3(config-router)#no auto-summary
```

\*On R4

```
R4(config)#router eigrp 100
R4(config-router)#network 192.168.30.0
R4(config-router)#no auto-summary
```

\*On R5

```
R5(config)#router eigrp 100
R5(config-router)#network 192.168.30.0
R5(config-router)#no auto-summary
```

After typing above commands we will see the neighbors adjacency on these routers are up. For example on R1 we will see

```

% Invalid input detected at '^' marker.

R1(config-router)#no auto-summary
R1(config-router)#net 192.168.60.0
R1(config-router)#
R1(config-router)#
R1(config-router)#
*Mar 1 01:05:08.583: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.30.13
  (Serial0/0) is up: new adjacency
*Mar 1 01:05:10.399: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.30.13
  (Serial0/0) is down: Interface Goodbye received
*Mar 1 01:05:15.379: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.30.13
  (Serial0/0) is up: new adjacency
*Mar 1 01:06:10.731: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.30.20
  (Serial0/1) is up: new adjacency
*Mar 1 01:06:11.475: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.30.20
  (Serial0/1) is down: Interface Goodbye received
*Mar 1 01:06:16.443: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.30.20
  (Serial0/1) is up: new adjacency
*Mar 1 01:06:26.535: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.30.40
  (Serial0/2) is up: new adjacency
*Mar 1 01:06:27.187: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.30.40
  (Serial0/2) is down: Interface Goodbye received
*Mar 1 01:06:31.827: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.30.40
  (Serial0/2) is up: new adjacency

```

Now the EIGRP process is up and we can ping from anywhere. For example a ping from R2 to s0/0 of R4 (192.168.30.20) will be successful now.

```

R2#ping 192.168.30.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.20, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/48/64 ms
R2#

```

By checking the routing table of R2, R3, R4 & R5 we can confirm EIGRP has been implemented successfully. For example, using the "show ip route" command on R5 we see

```

R5#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

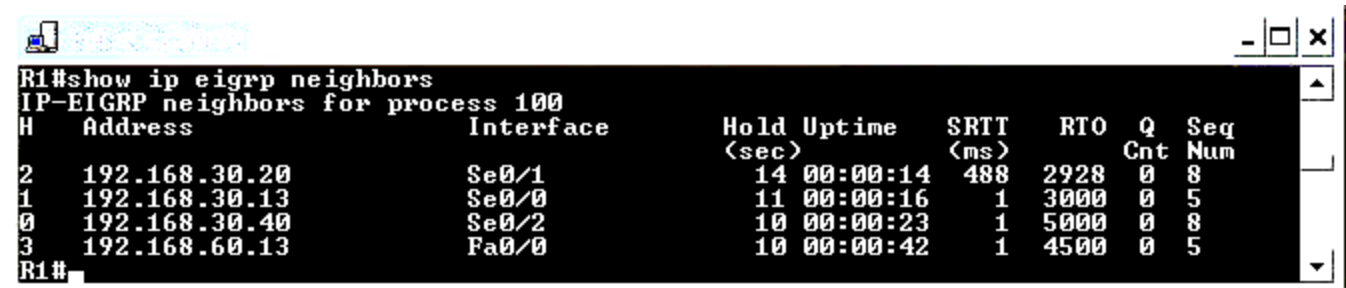
Gateway of last resort is not set

  192.168.30.0/28 is subnetted, 3 subnets
C       192.168.30.32 is directly connected, Serial0/0
D       192.168.30.16 [90/2681856] via 192.168.30.35, 00:09:46, Serial0/0
D       192.168.30.0 [90/2681856] via 192.168.30.35, 00:09:46, Serial0/0
  192.168.60.0/28 is subnetted, 1 subnets
D       192.168.60.0 [90/2172416] via 192.168.30.35, 00:09:46, Serial0/0
R5#

```

Notice that the routes to 192.168.30.16 & 192.168.60.0 are marked with a letter "D", meaning it is learned via EIGRP. Maybe you are wondering "why is the letter "D" used for EIGRP, not "E"? Well, the answer is the letter "E" has been "stolen" for EGP – an external routing protocol – but it is not popular nowadays :)

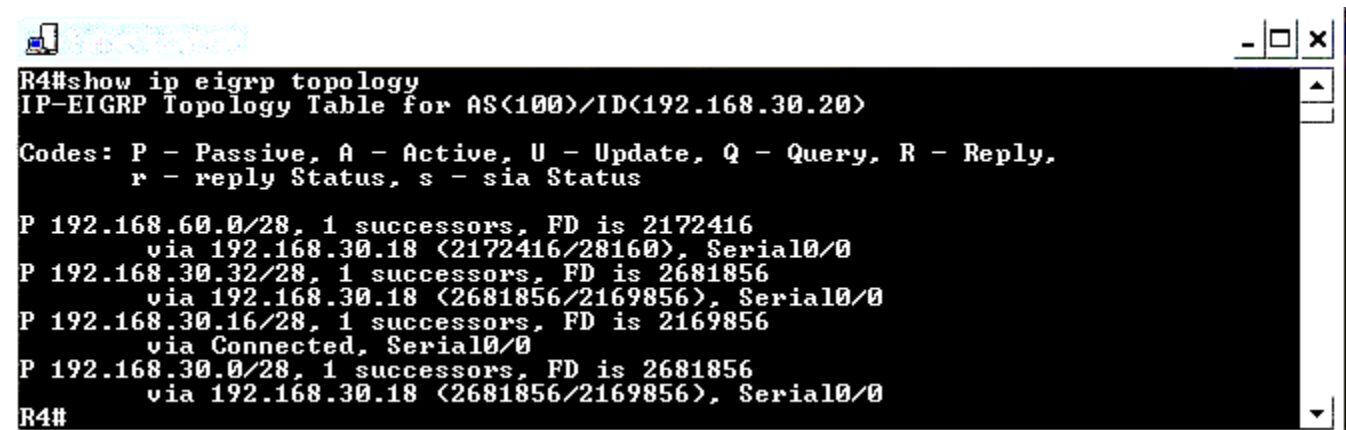
We can check the neighbor relationships on these routers with the "show ip eigrp neighbors" command. Below is an example of R1:



```

R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address             Interface      Hold Uptime    SRTT    RTO  Q  Seq
                   (sec)          (ms)
2   192.168.30.20         Se0/1         14 00:00:14    488   2928  0  8
1   192.168.30.13         Se0/0         11 00:00:16     1   3000  0  5
0   192.168.30.40         Se0/2         10 00:00:23     1   5000  0  8
3   192.168.60.13         Fa0/0         10 00:00:42     1   4500  0  5
R1#
  
```

To see the topologies of these routers, use the "show ip eigrp topology" command. Below is the output of R4



```

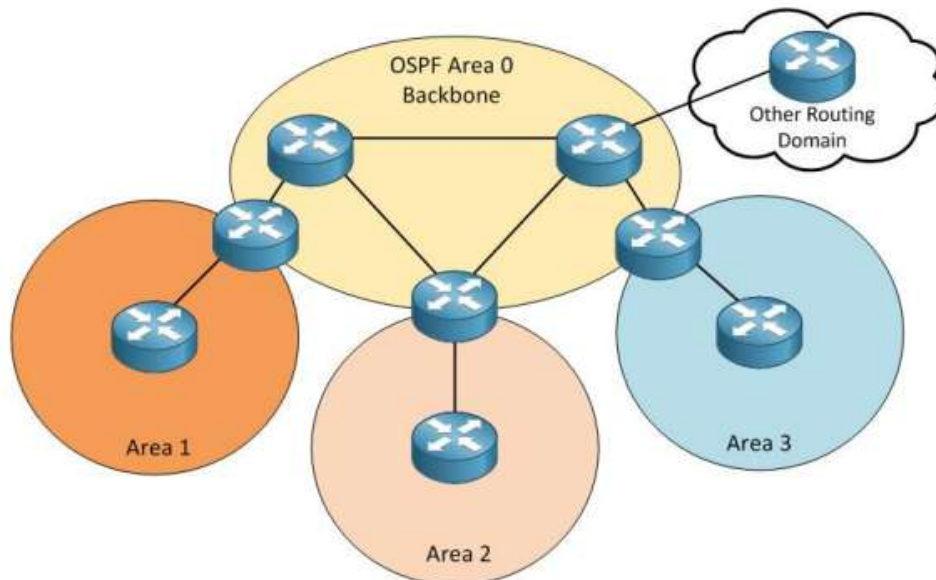
R4#show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(192.168.30.20)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.60.0/28, 1 successors, FD is 2172416
   via 192.168.30.18 (2172416/28160), Serial0/0
P 192.168.30.32/28, 1 successors, FD is 2681856
   via 192.168.30.18 (2681856/2169856), Serial0/0
P 192.168.30.16/28, 1 successors, FD is 2169856
   via Connected, Serial0/0
P 192.168.30.0/28, 1 successors, FD is 2681856
   via 192.168.30.18 (2681856/2169856), Serial0/0
R4#
  
```

## OSPF - Open Shortest path first

- 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 ( $\text{cost} = 10^8 / \text{B.W.}$ )
- 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

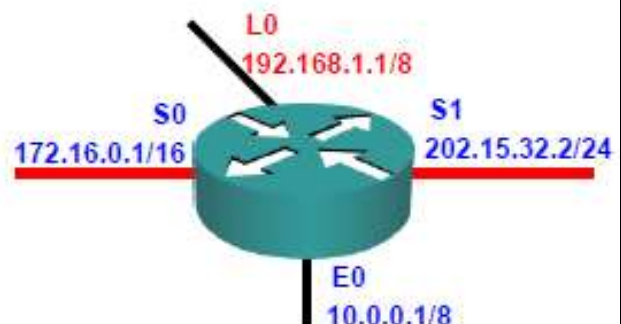


- Provides hierarchical network design with multiple different areas
- Must have one area called as area 0
- All the areas must connect to area 0
- Scales better than Distance Vector Routing protocols.
- Supports Authentication
- Updates are sent through multicast address 224.0.0.5
- Faster convergence.
- 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

### Router ID

The highest IP address of the active physical interface of the router is Router ID.

If logical interface is configured, the highest IP address of the logical interface is Router ID





## 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

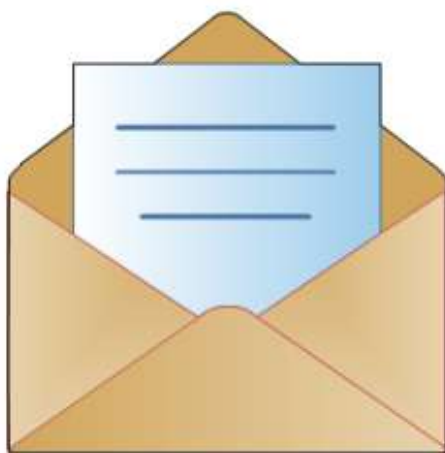
**Autonomous System Boundary Router (ASBR)** Router participating in OSPF and other protocols (like RIP, EIGRP and BGP)

## OSPF maintains three tables :

- 1) Neighbor Table** Neighbor table contains information about the directly connected ospf neighbors forming adjacency.
- 2) Database table** Database table contains information about the entire view of the topology with respect to each router.
- 3) Routing information Table** Routing table contains information about the best path calculated by the shortest path first algorithm in the database table.

## Hello Packet :-

Once you configure OSPF your router will start sending hello packets. If you also receive hello packets from the other router you will become neighbors.

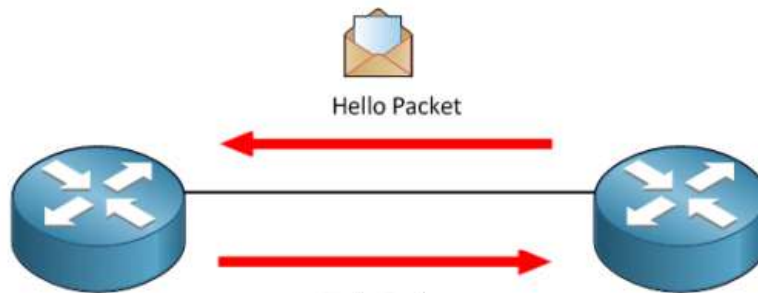


Router ID  
Hello / Dead Interval \*  
Neighbors  
Area ID \*  
Router Priority  
DR IP Address  
BDR IP Address  
Authentication Password \*  
Stub Area Flag \*

# Hello Packet

## OSPF PACKET TYPES:-

- **Hello:** Establishes and maintains neighbor relationships.



- **Database Description:** Describes the contents of the topological database. These messages are exchanged when an adjacency is initialized.
- **Link-state Request:** Requests pieces of the topological database from neighbor routers. These messages are exchanged after a router discovers (by examining
- **database-description** packets that parts of its topological database are out of date.
- **Link-state Update:** Responds to a link-state request packet. These messages also are used for the regular dispersal of Link-State Acknowledgments (LSA). Several LSAs can be included within a single link-state update packet.
- **Link-state Acknowledgment:** Acknowledges link-state update packets.

### 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

### Wild Card Mask

- Tells the router which addressing bits must match in the address of the ACL statement.
- It's the inverse of the subnet mask, hence is also called as Inverse mask.
- A bit value of 0 indicates MUST MATCH (Check Bits)
- A bit value of 1 indicates IGNORE (Ignore Bits)
- Wild Card Mask for a Host will be always 0.0.0.0
- A wild card mask can be calculated using the formula :

$$\begin{array}{r}
 \text{Global Subnet Mask} \\
 - \quad \text{Customized Subnet Mask} \\
 \hline
 \text{Wild Card Mask}
 \end{array}$$

E.g.

```

      255.255.255.255
    - 255.255.255.240
    -----
      0. 0. 0. 15
  
```

### Configuring OSPF

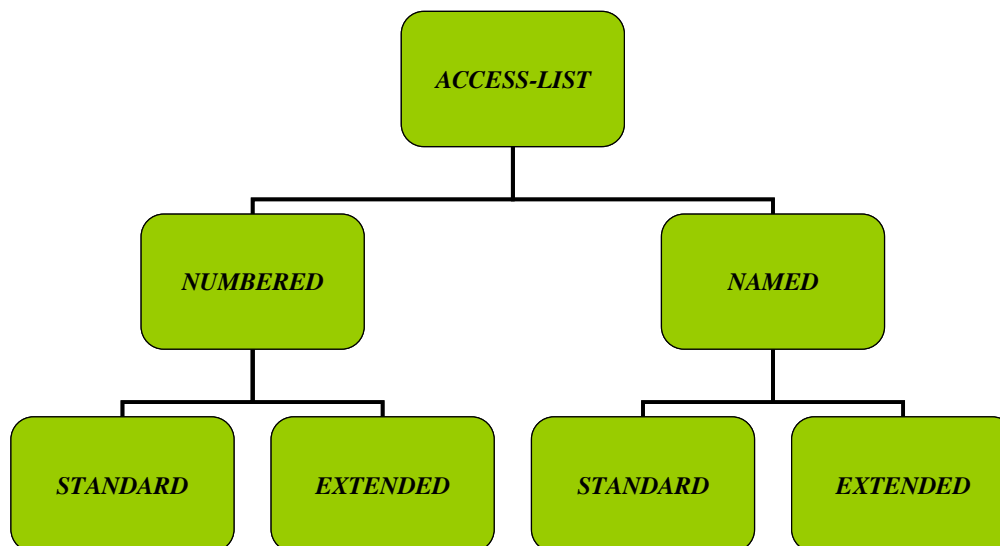
Router(config)# router ospf <pid>

Router(config-router)# network <Network ID> <wildcard mask> area <area id>

The Various Routing Protocols					
Features	RIP v1	RIP v2	IGRP	OSPF	EIGRP
Classful / Classless	Classful	Classless	Classful	Classless	Classless
Metric	Hop	Hop	Composite (bw and delay)	Cost	Composite (bw and delay)
Periodic Advertisement	30 seconds	30 seconds	90 seconds	100,000/BW none	30 seconds
Advertising Address	255.255.255.255 (broadcast)	224.0.0.9 (multicast)	255.255.255.255 (broadcast)	224.0.0.5 224.0.0.6 (multicast)	224.0.0.10 (multicast)
Administrative Cost	120	120	100	110	Internal: 90 External: 170
Category	Distance Vector	Distance Vector	Distance Vector	Link State	Hybrid

## Access Control List

- ACL is a set of rules which will allow or deny the specific traffic moving through the router
- It is a Layer 3 security which controls the flow of traffic from one router to another.
- It is also called as Packet Filtering Firewall.

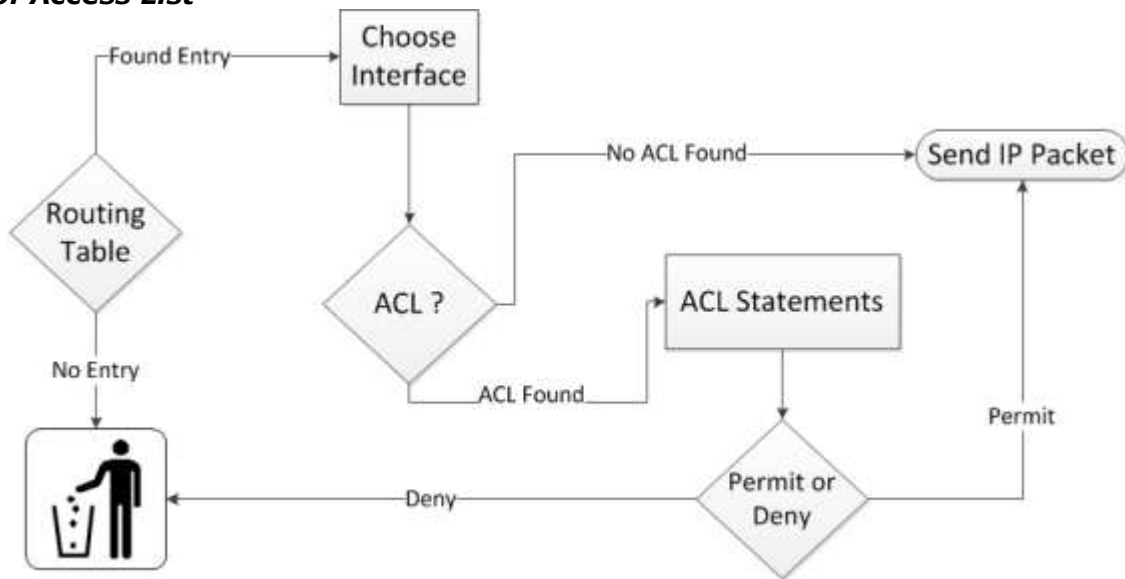


<b>Standard Access List</b>	<b>Extended Access List</b>
<ul style="list-style-type: none"> <li>• The access-list number range is 1 – 99</li> <li>• Can block a Network, Host and Subnet</li> <li>• Two way communication is stopped</li> <li>• All services are blocked.</li> <li>• Implemented closest to the destination.</li> <li>• Filtering is done based on only source IP address</li> </ul>	<ul style="list-style-type: none"> <li>• The access-list number range is 100 – 199</li> <li>• Can block a Network, Host, Subnet and Service</li> <li>• One way communication is stopped</li> <li>• Selected services can be blocked.</li> <li>• Implemented closest to the source.</li> <li>• Checks source, destination, protocol, port no</li> </ul>

### Terminology

- **Deny** : Blocking a Network/Host/Subnet/Service
- **Permit** : Allowing a Network/Host/Subnet/Service
- **Source Address** : The address of the PC from where the request starts.
- **Destination address** : The address of the PC where the request ends.
- **Inbound** : Traffic coming into the interface
- **Outbound** : Traffic going out of the interface

### Rules of Access List



- All deny statements have to be given First

- *There should be at least one Permit statement*
- *An implicit deny blocks all traffic by default when there is no match (an invisible statement).*
- *Can have one access-list per interface per direction. (i.e.) Two access-list per interface, one in inbound direction and one in outbound direction.*
- *Works in Sequential order*
- *Editing of access-lists is not possible (i.e) Selectively adding or removing access-list statements is not possible.*

### **Creation of Standard Access List**

```
Router(config)# access-list <acl no> <permit/deny> <source address>
                        <source WCM>
```

#### **Implementation of Standard Access List**

```
Router(config)# interface <interface type> <interface no>
```

```
Router(config-if)# ip access-group <number> <out/in>
```

#### **To Verify :**

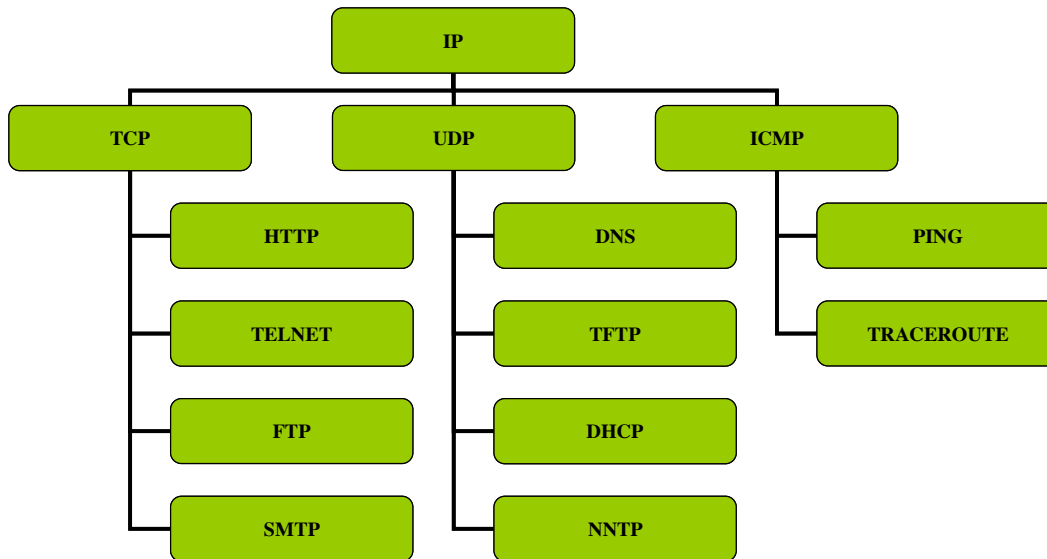
```
Router# show access-list
Router# show access-list <no>
```

### **Creation of Extended Access List**

```
Router(config)#      access-list <acl no> <permit/deny> <protocol>
                        <source address> <source wildcard mask>
                        <destination address> < destination wildcard mask> <operator>
                        <service>
```

#### **Implementation of Extended Access List**

```
Router(config)#interface <interface type> <interface no>
Router(config-if)#ip access-group <number> <out/in>
```



**Operators :** eq (equal to)  
 neq (not equal to)  
 lt (less than)  
 gt (greater than)

### Named Access List

- Access-lists are identified using Names rather than Numbers.
- Names are Case-Sensitive
- No limitation of Numbers here.
- One Main Advantage is Editing of ACL is Possible (i.e) Removing a specific statement from the ACL is possible.

(IOS version 11.2 or later allows Named ACL)

### Creation of Standard Named Access List

```
Router(config)# ip access-list standard <name>
```

```
Router(config-std-nacl)# <permit/deny> <source address> <source wildcard mask>
```

### Implementation of Standard Named Access List

```
Router(config)#interface <interface type><interface no>
```

```
Router(config-if)#ip access-group <name> <out/in>
```

### Creation of Extended Named Access List

```
Router(config)# ip access-list extended <name>
```

```
Router(config-ext-nacl)# <permit/deny> <protocol> <source address>  

  <source wildcard mask> <destination address>  

  < destination wildcard mask> <operator> <service>
```

**Implementation of Extended Named Access List****Router Password Breaking**

1. console connection
2. open hyperterm
3. power on the device
4. press CTRL+SHIFT+BREAK to enter in to rommon mode

5. on modular routers

```
Rommon1> confreg 0x2142
Rommon1> reset
```

OR

on fixed routers  
 >o/r 0x2142  
 >i

6. now the router boots without asking passwords

```
>enable
#copy start run
```

7. change the passwords

8. (config)#config-register 0x2102  
 (config)#exit

```
# write
# reload
```

**Dhcp :-** automatically assign the ip addresss to host

```
router(config)# ip dhcp excluded-address 192.168.1.50 (if you don't want to assign ip's range )
router(config-dhcp)# ip dhcp pool cisco
router(config-dhcp)# network 192.168.1.0 255.255.255.0
router(config-dgcp)# default-router 192.168.1.1
router(config-dgcp)#exit
```

## APIPA:-

Short for Automatic Private IP Addressing, a feature of later Windows operating systems. With APIPA, DHCP clients can automatically self-configure an IP address and subnet mask when a DHCP server isn't available. When a DHCP client boots up, it first looks for a DHCP server in order to obtain an IP address and subnet mask. If the client is unable to find the information, it uses APIPA to automatically configure itself with an IP address from a range that has been reserved especially for Microsoft. The IP address range is 169.254.0.1 through 169.254.255.254. The client also configures itself with a default class B subnet mask of 255.255.0.0. A client uses the self-configured IP address until a DHCP server becomes available.

The APIPA service also checks regularly for the presence of a DHCP server (every five minutes, according to Microsoft). If it detects a DHCP server on the network, APIPA stops, and the DHCP server replaces the APIPA networking addresses with dynamically assigned addresses.

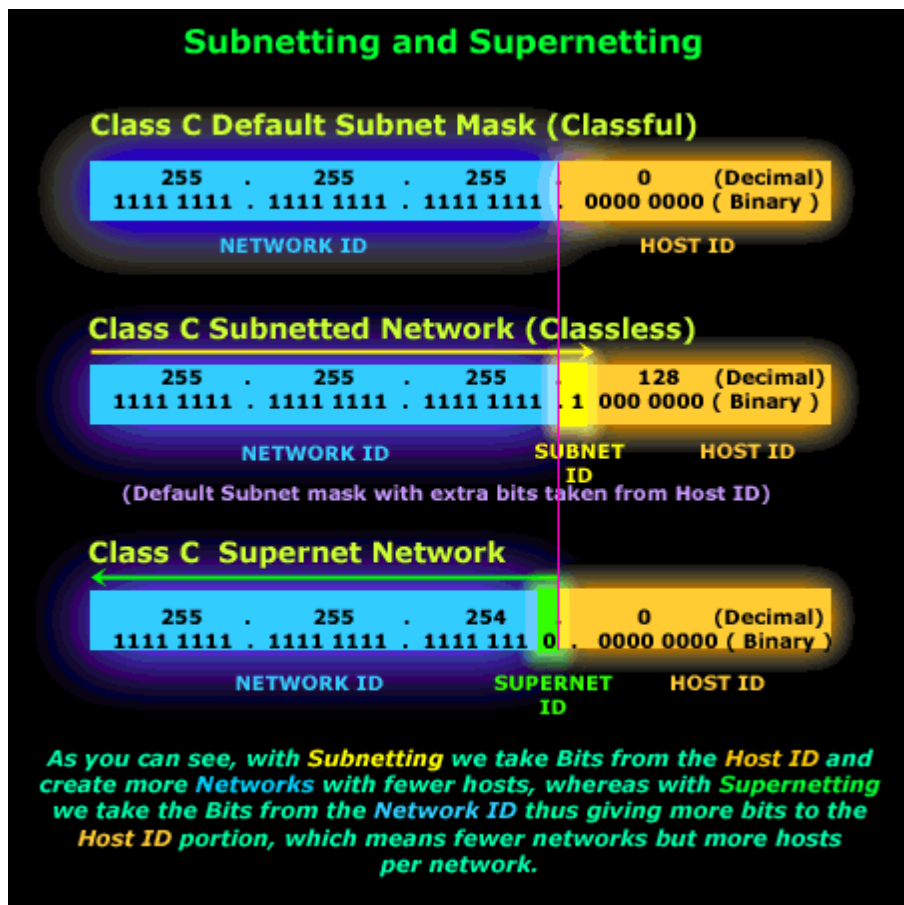
APIPA is meant for nonrouted small business environments, usually less than 25 clients.

## SUPERNETTING / CIDR CHART

Supernets are the opposite of Subnets in that they combine multiple Class C networks into blocks rather than dividing them into segments.

When Subnetting, we borrow bits from the Host ID portion, which increases the number of bits used for the Network ID portion. With Supernetting we do exactly the opposite, meaning we take

the bits from the Network ID portion and give them to the Host ID portion, as illustrated in the picture below:





Class C			
CIDR Block	Supernet Mask	Number of Class C Networks	Number of Hosts
/14	255.252.0.0	1024	262144
/15	255.254.0.0	512	131072
/16	255.255.0.0	256	65536
/17	255.255.128.0	128	32768
/18	255.255.192.0	64	16384
/19	255.255.224.0	32	8192
/20	255.255.240.0	16	4096
/21	255.255.248.0	8	2048
/22	255.255.252.0	4	1024
/23	255.255.254.0	2	512
/24	255.255.255.0	1	254
/25	255.255.255.128	1/2	126
/26	255.255.255.192	1/4	62
/27	255.255.255.224	1/8	32
/28	255.255.255.240	1/16	16
/29	255.255.255.248	1/32	8
/30	255.255.255.252	1/64	4

## ***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.*

*Address translation was originally developed to solve two problems:*

- 1. to handle a shortage of IPv4 addresses*
- 2. hide network addressing schemes.*

*Small companies typically get their public IP addresses directly from their ISPs, which have a limited number.*

*Large companies can sometimes get their public IP addresses from a registration authority, such as the Internet Assigned Numbers Authority (IANA).*

*Common devices that can perform address translation include firewalls, routers, and servers. Typically address translation is done at the perimeter of the network by either a firewall (more commonly) or a router.*

*There are certain addresses in each class of IP address that are reserved for Private Networks. These addresses are called private addresses.*

*Class A 10.0.0.0 to 10.255.255.255*

*Class B 172.16.0.0 to 172.31.255.255*

*Class C 192.168.0.0 to 192.168.255.255*

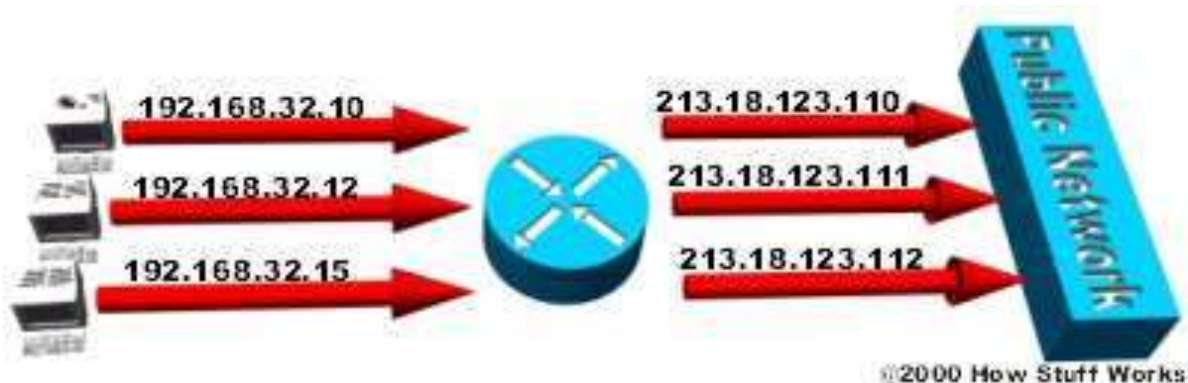
- **Inside Local Addresses** – An IP address assigned to a host inside a network. This address is likely to be a RFC 1918 private address
- **Inside Global Address** – A legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP address to the outside world.
- **Outside Local Address** - The IP address of an outside host as it known to the hosts in the inside network.
- **Outside Global Address** - The IP address assigned to a host on the outside network. The owner of the host assigns this address.

### Types of NAT:-

1. Dynamic NAT
2. Static NAT
3. PAT

### Static NAT

- This type of NAT is designed to allow one-to-one mapping between local and global addresses.
- Keep in mind that the static version requires you to have one real Internet IP address for every host on your network..



### Syntax:

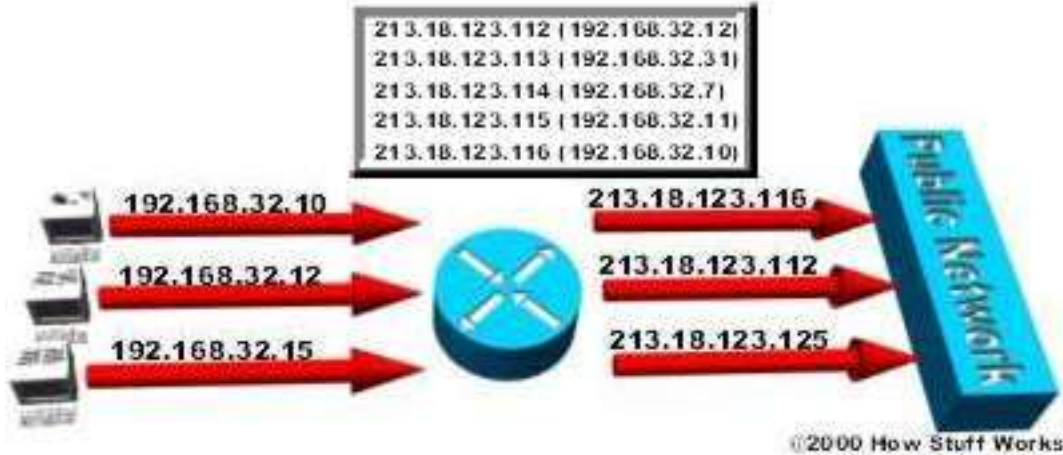
`(Config)# IP nat inside source static <private IP> <public IP>`

### Implementation :

```
(Config) # interface s0
(Config-if)# ip nat outside
(Config)# interface e0
(Config-if)# ip nat inside
```

### Dynamic NAT

- This version gives you the ability to map an unregistered IP address to a registered IP address from out of a pool of registered IP addresses.
- You don't have to statically configure your router to map an inside to an outside address as you would using static NAT, but you do have to have enough real IP addresses for everyone who's going to be sending packets to and receiving them from the Internet.



#### Syntax :

```
(Config)# access-list < NO> permit <net.ID> <WCM>
```

```
(Config)#ip nat inside pool <name> <starting Pub IP> <end Pub IP>  
          <netmask < mask>
```

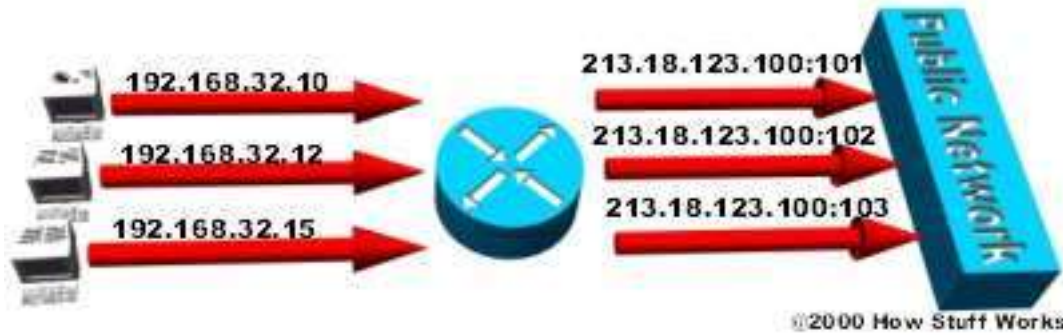
```
(Config)# ip nat inside source list <Aclno> pool <name>
```

#### Implementation :

```
(Config) # interface s0  
(Config-if)# ip nat outside  
(Config)# interface e0  
(Config-if)# ip nat inside
```

#### Dynamic NAT Overload ( PAT )

- This is the most popular type of NAT configuration. Understand that overloading really is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address—many-to-one—by using different ports.
- It is also known as Port Address Translation (PAT), and by using PAT (NAT Overload), you get to have thousands of users connect to the Internet using only one real global IP address.
- NAT Overload is the real reason we haven't run out of valid IP address on the Internet

**Syntax :**

```
(Config)# access-list < NO> permit <net.ID> <WCM>
```

```
(Config)#ip nat inside pool <name> <starting Pub IP><end Pub IP> netmask  
< mask>
```

```
(Config)# ip nat inside source list <Aclno> pool <name> overload
```

**Implementation :**

```
(Config) # interface s0  
(Config-if)# ip nat outside  
(Config)# interface e0  
(Config-if)# ip nat inside
```

## Practical

To configure static NAT we need to complete these tasks:

\* Define the router's interfaces as inside or outside:

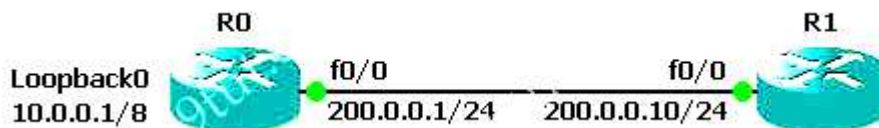
```
R0router(config-if)#ip nat inside (or ip nat outside)
```

\* Define static mapping between the inside address and the outside address:

```
R0router(config)#ip nat inside source static
```

+ Static NAT:

To make everything clear, we will configure static NAT in GNS3. Open your GNS3 and build a topology like this:



We should use 3 routers in this topology but I want to save some RAM and demonstrate how to ping from the loopback interface so I only use two :) Therefore we should configure the loopback interface of R0 as the source IP address and the fa0/0 interface of R0 as the "outgoing static NAT" address.

```
R0#configure terminal
```

```
R0(config)#int loopback0
```

```
R0(config-if)#ip address 10.0.0.1 255.0.0.0
```

```
R0(config-if)#ip nat inside
```

```

R0(config-if)#int f0/0
R0(config-if)#ip address 200.0.0.1 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#ip nat outside
R0(config-if)#exit

```

Finally, we have to tell the router to translate my private IP **10.0.0.1** to public IP **200.0.0.2** so that I can go to the Internet!

```
R0(config)#ip nat inside source static 10.0.0.1 200.0.0.2
```

In R1 we just assign the IP address and no shut its interface.

```

R1#config terminal
R1(config)#int f0/0
R1(config-if)#ip address 200.0.0.10 255.255.255.0
R1(config-if)#no shutdown

```

Check if all things are right or not:

```
R0#show ip nat translations
```

```

Router#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 200.0.0.2          10.0.0.1          ---                ---
Router#

```

In this article we don't use a host attached to R0 so if we want to test our NAT configuration we have to ping from R0's loopback interface by using the ping extended command:

We can use the extended ping command by typing only "ping" at the privileged mode, specify the "target IP address" and type "y" at the "Extended commands" and specify the "source address or interface" at shown below:

```

Router#ping
Protocol [ip]:
Target IP address: 200.0.0.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.0.0.1
Type of service [0]:
Set DF bit in IP header? [n]:
Validate reply data? [n]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.0.10, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/38/88 ms
Router#

```

To approve NAT works well we can disable static NAT with the following command

```
R0(config)#no ip nat inside source static 10.0.0.1 200.0.0.2
```

Now if we use the extended ping command (without NAT configured):

```

Router#ping
Protocol [ip]:
Target IP address: 200.0.0.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.0.0.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.0.10, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.1
.....
Success rate is 0 percent (0/5)
Router#

```

-> We can't ping from the loopback interface.

## + Dynamic NAT:

To configure dynamic NAT we need to complete these tasks:

- \* Define a pool of addresses (public IP) to be used for dynamic NAT allocation

```
Router(config)#ip nat pool pool_name start_ip end_ip { netmask netmask | prefix-length prefix-length }
```

- \* Configure a standard access control list to define what internal traffic will be translated

```
Router(config)#access-list access-list-number permit source [source-wildcard]
```

Link the access list to the NAT pool

```
Router(config)#ip nat inside source list access-list-number pool pool_name
```

Define interfaces as either inside and outside

```
Router(config-if)# ip nat inside (on fa0/0, for example)
```

```
Router(config-if)#ip nat outside (on fa0/1, for example)
```

- \* Dynamic NAT configuration example:

```
RouterA(config)# access-list 1 permit 192.168.0.0 0.0.0.255
```

```
RouterA(config)# ip nat pool PoolforNAT 200.23.123.6 200.23.123.10 netmask 255.255.255.0
```

```
RouterA(config)# ip nat inside source list 1 pool PoolforNAT
```

Note: In the above command, the word "inside" means "I want to NAT from inside to outside"; "list 1" means "the source IP addresses to NAT are included in Access-list 1"; "pool PoolforNAT" means "NAT to the IP addresses specified in PoolforNAT".

```
RouterA(config)# int loopback0
```

```
RouterA(config-if)# ip nat inside
```

```
RouterA(config-if)# int fa0/0
```

```
RouterA(config-if)# ip nat outside
```

## Configure PAT (NAT Overload)

- \* Configure a standard access list to define what internal traffic will be translated
- \* Link the access list to the interface to be used for PAT
- \* Define interfaces as either inside or outside

PAT router commands

```
RouterA(config)# access-list 1 permit 192.168.0.0 0.0.0.255
```

```
RouterA(config)# ip nat inside source list 1 interface fa0/0 overload
```

(Notice the "interface fa0/0" means "NAT out of this interface" and the keyword **overload** for PAT in the above command)

```
RouterA(config)# interface fa0/0
```

```
RouterA(config-if)# ip nat outside
```

```
RouterA(config-if)# interface loopback0
```

```
RouterA(config-if)# ip nat inside
```



## BASIC SWITCHING



### Hub

- It is a Physical layer device (Layer 1)
- It is Dummy Device
- It works with 0's and 1's (Bits)
- It works with broadcasting
- It works with shared bandwidth
- It has 1 Broadcast Domain and 1 Collision Domain
- Collisions are identified using Access Methods called CSMA/CD and CSMA/CA

### CSMA/CD

stands for Carrier Sense Multiple Access with Collision Detection. It refers to the means of media access, or deciding "who gets to talk" in an Ethernet network.

A more elegant term for "who gets to talk" is to refer to the "media access method", which, in this case, would be "CSMA/CD".

**Carrier Sense** means that before a station will "talk" onto an Ethernet wire, it will listen for the "carrier" that is present when another station is talking. If another station is talking, this station will wait until there is no carrier present.

**Multiple Access** refers to the fact that when a station is done transmitting it is allowed to immediately make another access to the medium (a 'multiple' access). This is as opposed to a Token-Ring network where a station is required to perform other tasks inbetween accessing the medium (like releasing a token or sometimes releasing a management frame).

**Collision Detection** refers to the ability of an Ethernet adapter to detect the resulting "collision" of electrical signals and react appropriately. In a normally operating Ethernet network, it will sometimes occur that two stations simultaneously detect no carrier and begin to talk. In this case the two electrical signals will interfere with each other and result in a collision; an event which is detected by the Collision Detection circuitry in the transmitting network interface cards.

### Switch



- It is Datalink layer device (Layer 2)
- Its is An Intelligent device

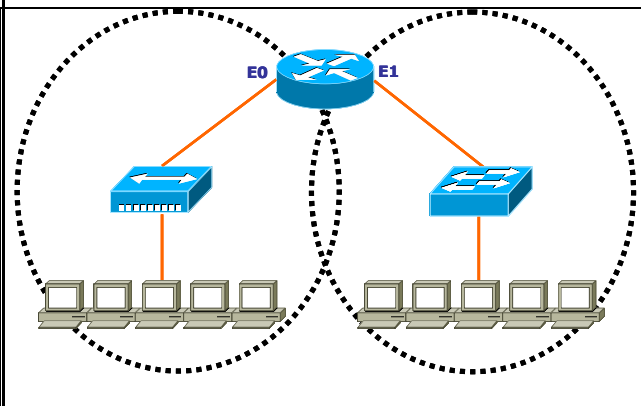


- It works with Physical addresses (i.e. MAC addresses)
- It works with fixed bandwidth
- It works with Flooding and Unicast
- It has 1 Broadcast domain and Number of Collision domains depends upon the number of ports.
- It maintains a MAC address table

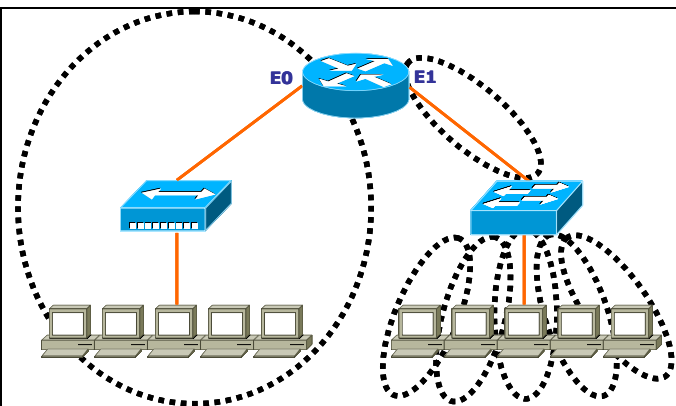
### Broadcast Domain & Collision Domain

- **Broadcast Domain**  
Set of all devices that receive broadcast frames originating from any device within the set.
- **Collision domain**  
In Ethernet, the network area within which frames that have collided are propagated is called a collision domain.
- A collision domain is a network segment with two or more devices sharing the same bandwidth.

#### Broadcast Domains



#### Collision Domains



### Types of Switches

- **Manageable switches**  
On a Manageable switch, an IP address can be assigned and configurations can be made. It has a console port .
- **Unmanageable switches**  
On an Unmanageable switch, configurations cannot be made, an IP address cannot be assigned as there is no console port.

### Cisco's Hierarchical Design Model

Cisco divided the Switches into 3 Layers

#### 1. Access Layer Switches

Switches Series : 1900 & 2900

#### 2. Distribution Layer Switches

Switches Series : 3000 & 5000

#### 3. Core Layer Switches

Switches Series : 7000, 8000 & 10,000

**Access Layer Switch****Catalyst 1900****Catalyst 2900****Distribution Layer Switch****3550 switch****Core Layer Switches**



## Switching Mode

Three types of Switching Mode :

- **Store & Forward**
  - A Default switching method for distribution layer switches.
  - Latency : High
  - Error Checking : Yes
- **Fragment Free**
  - It is also referred to as Modified Cut-Through
  - A Default Switching method for access layer switches.
  - Latency : Medium
  - Error Checking : On 64 bytes of Frame
- **Cut through**
  - A Default switching method for the core layer switches
  - Latency : Low
  - Error Checking : No

Latency is the total time taken for a Frame to pass through the Switch. Latency depends on the switching mode and the hardware capabilities of the Switch.

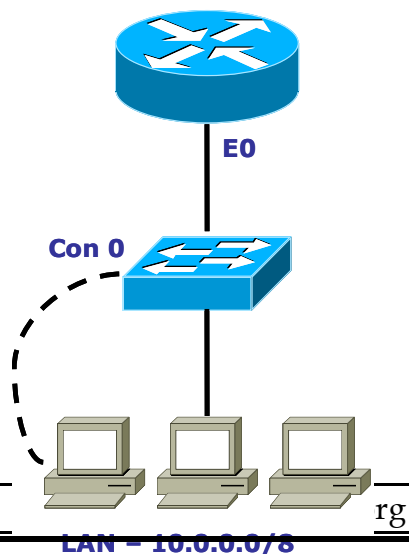
## Console Connectivity

- Connect a rollover cable to the Switch console port (RJ-45 connector).
- Connect the other end of the rollover cable to the RJ-45 to DB-9 adapter
- Attach the female DB-9 adapter to a PC Serial Port.
- Open emulation software on the PC.

## Emulation Software

IN WINDOWS

- Start ◇ Programs ◇ Accessories ◇ Communications ◇ HyperTerminal ◇ HyperTerminal.



- Give the Connection Name & Select Any Icon
- Select Serial (Com) Port where Switch is Connected.
- In Port Settings ◊ Click on Restore Defaults

IN LINUX

- # minicom -s

### **INITIAL CONFIGURATION OF A SWITCH:**

Connect one end of console cable to console port of switch and other end of cable to your computer's com port.

Now open Hyper terminal and power on the switch.

Would you like to enter into initial configuration dialog (yes/no): no

2950>en

2950#config terminal

#### **TO assign telnet Password**

2950(config) # line vty 0 4

2950(config-line) # login

2950(config-line) # password <password>

#### **TO assign Console Password**

2950(config) # line con 0

2950(config-line) # login

2950(config-line) # password <password>

#### **TO assign Enable Password**

2950(config) #enable secret < password>

2950(config) #enable password < password>

2950(config) #exit

switch# Show mac-address-table ( to see the entries of the MAC table)

switch# Show interface status

#### **To assign IP to a Switch**

switch(config)# Interface Vlan 1

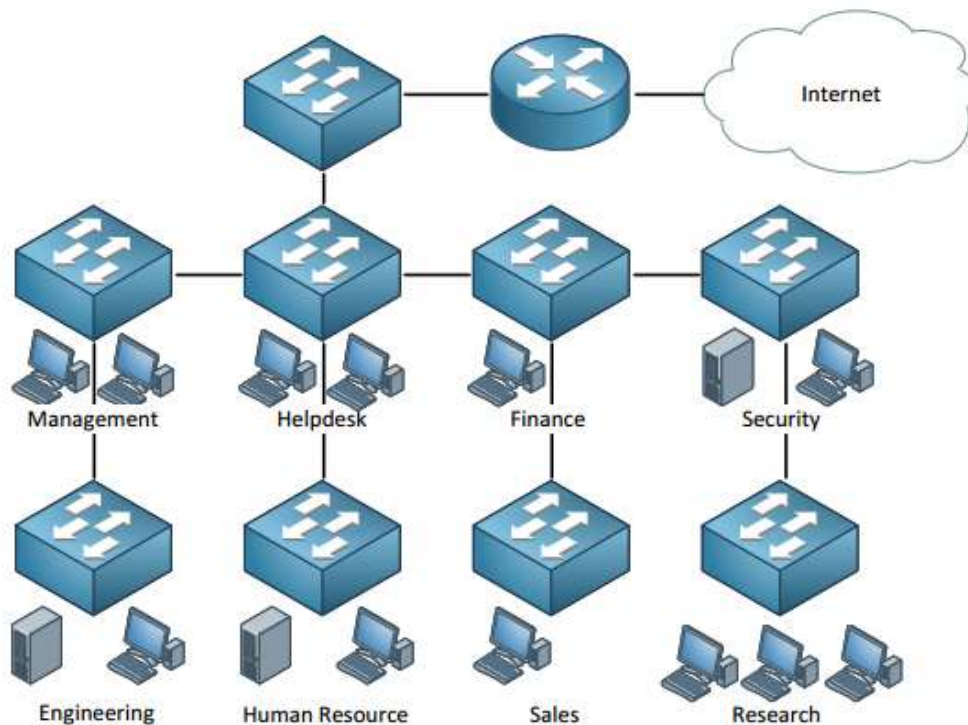
switch(config-if)# ip address <ip> <mask>

switch(config-if)# no shutdown

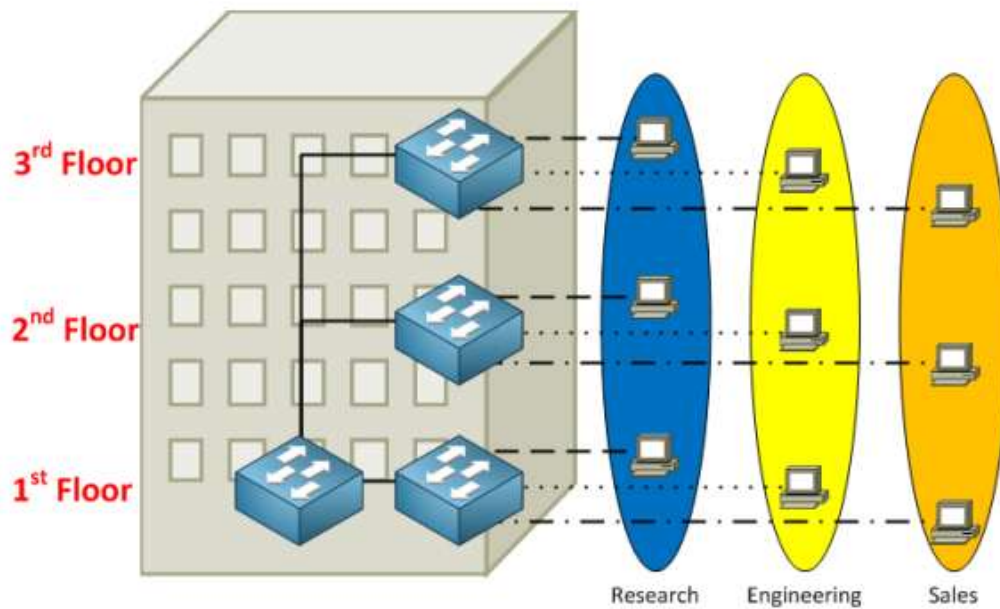
#### **To assign Default Gateway to a Switch**

switch(config)#ip default-gateway 192.168.20.1

## Virtual LAN



- A Layer 2 Security
- Divides a Single Broadcast domain into Multiple Broadcast domains.
- By default all ports of the switch are in VLAN1 . This VLAN1 is known as Administrative VLAN or Management VLAN
- VLAN can be created from 2 – 1001
- Can be Configured on a Manageable switch only
- 2 Types of VLAN Configuration
  - Static VLAN
  - Dynamic VLAN
- By default, routers allow broadcasts only within the originating network, but switches forward broadcasts to all segments.
- The reason it's called a flat network is because it's one Broadcast domain , not because its design is physically flat. (Flat Network Structure)
- Network adds, moves, and changes are achieved by configuring a port into the appropriate VLAN.
- A group of users needing high security can be put into a VLAN so that no users outside of the VLAN can communicate with them.
- As a logical grouping of users by function, VLANs can be considered independent from their physical or geographic locations.
- VLANs can enhance network security.
- VLANs increase the number of broadcast domains while decreasing their size.



### Static VLAN

- Static VLAN's are based on port numbers
- Need to manually assign a port on a switch to a VLAN
- Also called Port-Based VLANs
- It can be a member of single VLAN and not multiple VLAN's

### Static VLAN On 2900 series Switch

- **Creation of VLAN:-**  

```
Switch # vlan database
Switch(vlan)# vlan <vlan id> name <vlan name>
Switch(vlan)# exit
```
- **Assigning port in VLAN:-**  

```
Switch#config t
Switch(config)# int fastethernet <int no>
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan <vlan id>
```
- **Verify using**  

```
Switch # show vlan
```

### VLAN Creation – 1900 Series

```
Switch(config)# vlan <no>
Switch(config-Vlan)# name <name>
Switch(config-Vlan)# Exit
```

#### Assigning ports in Vlan

```
Switch(config)# interface <interface type> <interface no.>
Switch(config-if)# switchport mode access
```

*Switch(config-if)# switchport access Vlan <no>*

**The range command** (Assigning multiple ports at same time)

The range command, you can use on switches to help you configure multiple ports at the same time

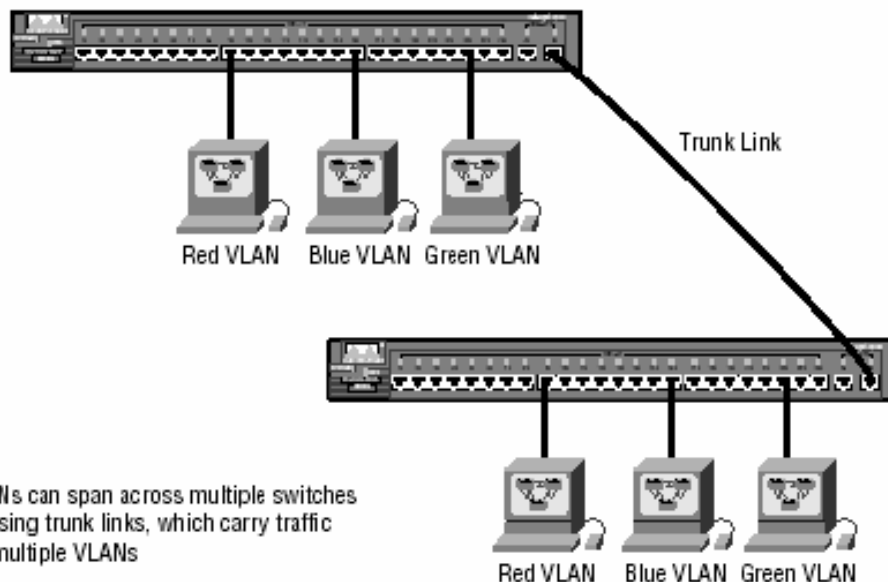
*Switch(config)# int range fastEthernet 0/1 - 12*

## Dynamic VLAN

- Dynamic VLAN's are based on the MAC address of a PC
- Switch automatically assigns the port to a VLAN
- Each port can be a member of multiple VLAN's
- For Dynamic VLAN configuration, a software called VMPS( VLAN Membership Policy Server) is needed

## Types of links/ports

- **Access links**
  - This type of link is only part of one VLAN, and it's referred to as the native VLAN of the port.
  - Any device attached to an access link is unaware of a VLAN membership—the device just assumes it's part of a broadcast domain, but it has no understanding of the physical network.
  - Switches remove any VLAN information from the frame before it's sent to an accesslink device.
- **Trunk links**
  - Trunks can carry multiple VLANs.
  - A trunk link is a 100- or 1000Mbps point-to-point link between two switches, between a switch and router, or between a switch and server. These carry the traffic of multiple VLANs—from 1 to 1005 at a time.
  - Trunking allows you to make a single port part of multiple VLANs at the same time.

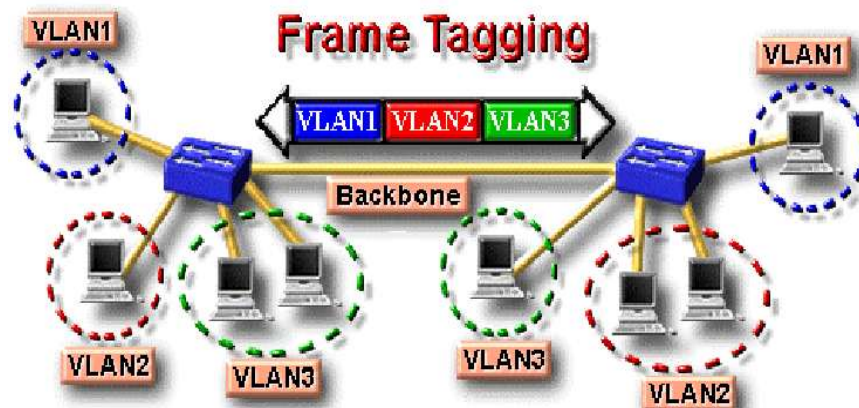


VLANs can span across multiple switches by using trunk links, which carry traffic for multiple VLANs



### VLAN Identification Methods (Frame Tagging)

- VLAN identification is what switches use to keep track of all those frames
- It's how switches identify which frames belong to which VLANs, and there's more than one trunking method :
  - **Inter-Switch Link (ISL)**
  - **IEEE 802.1Q**



<b>ISL</b>	<b>IEEE 802.1Q</b>
<ul style="list-style-type: none"> <li>• It's a Cisco proprietary</li> <li>• It adds 30 bytes to the header</li> <li>• All VLAN traffic is tagged</li> <li>• It works with Ethernet, Token ring, FDDI</li> <li>• Frame is not modified</li> </ul>	<ul style="list-style-type: none"> <li>• Created by the IEEE as a standard method or frame tagging.</li> <li>• Open standard, we can use on different vendors switches.</li> <li>• It works only on Ethernet</li> <li>• Unlike ISL , 802.1q does not encapsulate the frame . It modifies the existing Ethernet frame to include the VLAN ID</li> <li>• Only 4 Byte tag will add to original frame.</li> </ul>

### Trunking Configuration – 2900 Series

```
Switch(config)# interface <interface type> <interface no.>
Switch(config-if)# switchport trunk allowed vlan {<vlan no.>|all}
Switch(config-if)# switchport trunk encapsulation dot1q/ISL
```



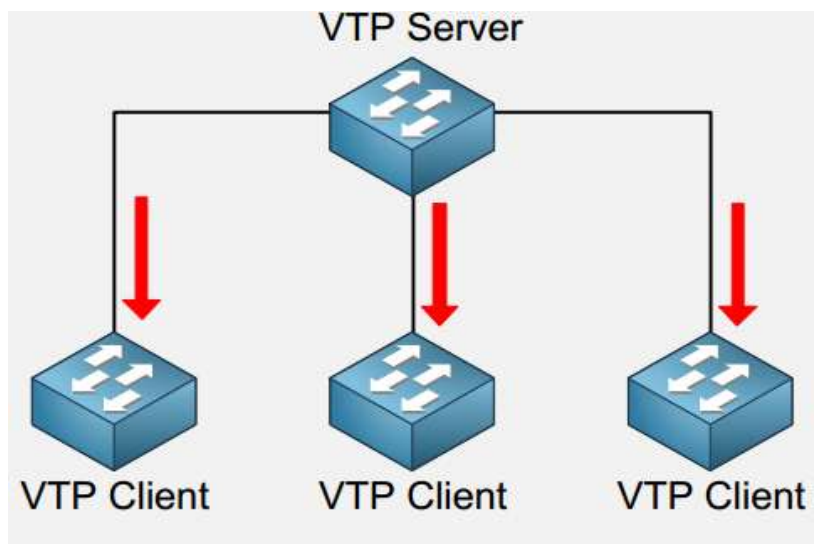
## VTP - Virtual LAN Trunking Protocol

- VTP is a CISCO proprietary protocol
- used to share the VLAN configurations with multiple switches and to maintain consistency throughout that network.
- Information will be passed only if switches connected with FastEthernet or higher ports.
- VTP allows an administrator to add, delete, and rename VLANs-information that is then propagated to all other switches in the VTP domain.
- **Note:** Switches Should be configure with same Domain. Domain are not Case sensitive.

### VTP Modes

VTP Mode are of three types :

- **Server Mode**
  - A Switch configured in Server mode can Add , Modify and Delete VLAN's
  - A Default VTP mode for all switches
- **Client Mode**
  - A switch configured in Client mode cannot Add , Modify and Delete its VLAN configurations
  - Doesn't store its VLAN configuration information in the NVRAM. Instead , learns it from the server every time it boots up
- **Transparent Mode**
  - A switch configured in a Transparent Mode can Add , Modify and Delete VLAN configurations.
  - Changes in one transparent switch will not affect any other switch.



### Benefits of VLAN Trunking Protocol (VTP)

- Consistent VLAN configuration across all switches in the network
- Accurate tracking and monitoring of VLANs
- Dynamic reporting of added VLANs to all switches in the VTP domain
- Plug-and-Play VLAN adding

### VTP Pruning

- Preserves bandwidth by configuring it to reduce the amount of broadcasts, multicasts, and unicast packets.
- VTP pruning only sends broadcasts to trunk links that truly must have the information.
- Enabling pruning on a VTP server, enables it for the entire domain.
- By default, VLANs 2 through 1005 are pruning-eligible, but VLAN 1 can never prune because it's an administrative VLAN.

### VTP Configuration – 2950 Series

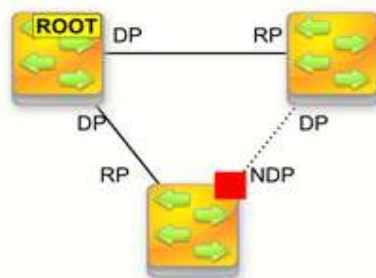
```
Switch(config)# VTP Domain <Name>
Switch(config)# VTP Password <password>
Switch(config)# VTP Mode <server/client/transparent>
Switch(config)# VTP pruning
```

### VTP Configuration – 1900 Series

```
Switch#VLAN Database
Switch(VLAN)# VTP Domain <Name>
Switch(VLAN)# VTP Password <password>
Switch(VLAN)# VTP Mode <server/client/transparent>
Switch(VLAN)# VTP pruning
```

## Spanning Tree Protocol

### STP Terminology



#### STP Port Roles:

- Root Port (Forward upstream)
- Designated Port (Forward downstream)
- Non-Designated Port (Block)

#### STP Port States:

- Disabled
- Blocking (20 sec. MAX\_AGE)
- Listening (15 sec. FORWARD\_DELAY)
- Learning (15 sec. FORWARD\_DELAY)
- Forwarding

- Spanning Tree Protocol (STP) uses Spanning Tree Algorithm to avoid the Switching loops in layer-2 devices (bridges or switches).
- STP works when multiple switches are used with redundant links avoiding Broadcast Storms, Multiple Frame Copies & Database instability.
- First Developed By DEC
- STP is a open standard (IEEE 802.1D)
- STP is enabled by default on all Cisco Catalyst switches

### STP Terminology

- **BPDUs**
  - All switches exchange information through what is called as Bridge Protocol Data Units (BPDUs)
  - BPDUs contain a lot of information to help the switches determine the topology and any loops that result from that topology.
  - BPDUs are sent every 2 sec
- **Bridge ID**

- Each switch has a unique identifier called a Bridge ID or Switch ID
- Bridge ID = Priority + MAC address of the switch
- When a switch advertises a BPDU , they place their switch id in these BPDUs.
- **Root Bridge**
  - The bridge with the Best (Lowest) ID.
  - Out of all the switches in the network , one is elected as a root bridge that becomes the focal point in the network.
- **Non-Root bridge**
  - All Switches other than the Root Bridge are Non-Root Bridges
- **Designated port**
  - Either a port On a root bridge or a port that has been determined as having the best (lower) cost.
  - A designated port will always in Forward Mode
- **Root port**
  - The link directly connected to the root bridge, or the shortest path to the root bridge.
  - Priority and Alternatives if Config occurred.
    - Root port with the least cost (Speed) connecting to the root bridge.
    - The bridge with the Best (Lowest) Switch ID.
    - Lowest Physical Port Number.
  - Only One root port will Be in Bridge or switch.
- **Non Designated port**
  - All the Port or ports which are blocked by STP to avoid switching loop.
  - A Non Designated port Will Always in Blocked Mode.

### STP port states

- Blocking - 20 Sec Or No Limits.
- Listening - 15 Sec.
- Learning - 15 Sec.
- Forwarding - No Limits.
- Disable - No Limits.

### Switch - Port States

- **Blocking** : Won't forward frames; listens to BPDUs. All ports are in blocking state by default when the switch is powered up.
- **Listening** : Listens to BPDUs to make sure no loops occur on the network before passing data frames.
- **Learning** : Learns MAC addresses and builds a filter table but does not forward frames.
- **Forwarding** : Sends and receives all data on the bridged port.

### Typical Costs of Different Ethernet Networks

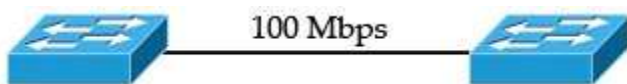
Speed New	IEEE Cost	Original IEEE Cost
-----------	-----------	--------------------

10Gbps	2	1
1Gbps	4	1
100Mbps	19	10
10Mbps	100	100

## EtherChannel

EtherChannel is the technology which is used to combine several physical links between switches or routers into one logical connection and treat them as a single link. Let's take an example to see the benefits of this technology:

Suppose your company has two switches connecting with each other via a FastEthernet link (100Mbps):



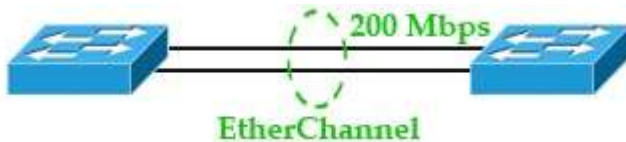
Your company is growing and you need to transfer more than 100 Mbps between these switches. If you only connect other links between the two switches it will not work because Spanning-tree protocol (STP) will block redundant links to prevent a loop:



To extend the capacity of the link you have two ways:

- + Buy two 1000Mbps (1Gbps) interfaces
- + Use EtherChannel technology to bundle them into a bigger link

The first solution is expensive with the new hardware installed on the two switches. By using EtherChannel you only need some more unused ports on your switches:



EtherChannel bundles the physical links into one logical link with the combined bandwidth and it is awesome! STP sees this link as a single link so STP will not block any links! EtherChannel also does load balancing among the links in the channel automatically. If a link within the EtherChannel bundle fails, traffic previously carried over the failed link is carried over the remaining links within the EtherChannel. If one of the links in the channel fails but at least one of the links is up, the logical link (EtherChannel link) remains up.

EtherChannel also works well for router connections:



When an EtherChannel is created, a logical interface will be created on the switches or routers representing for that EtherChannel. You can configure this logical interface in the way you want. For example, assign access/trunk mode on switches or assign IP address for the logical interface on routers...

Note: A maximum of 8 Fast Ethernet or 8 Gigabit Ethernet ports can be grouped together when forming an EtherChannel.

There are three mechanisms you can choose to configure EtherChannel:

- + Port Aggregation Protocol (PAgP)
- + Link Aggregation Protocol (LACP)
- + Static ("On")

**LACP is the IEEE Standard** (IEEE 802.3ad) and is the most common dynamic ether-channel protocol, whereas **PAgP is a Cisco proprietary** protocol and works only between supported vendors and Cisco devices. All ports in an EtherChannel must use the same protocol; you cannot run two protocols on two ends. In other words, PAgP and LACP are not compatible so both ends of a channel must use the same protocol.

The Static Persistence (or "on" mode) bundles the links unconditionally and no negotiation protocol is used. In this mode, neither PAgP nor LACP packets are sent or received.

([http://www.cisco.com/en/US/tech/tk389/tk213/technologies\\_tech\\_note09186a0080094714.shtml](http://www.cisco.com/en/US/tech/tk389/tk213/technologies_tech_note09186a0080094714.shtml))

Next we will learn more about the three EtherChannel mechanisms above.

### Port Aggregation Protocol (PAgP)

PAgP dynamically negotiates the formation of a channel. There are two PAgP modes:

<b>Auto</b>	Responds to PAgP messages but does not aggressively negotiate a PAgP EtherChannel. A channel is formed only if the port on the other end is set to Desirable. This is the default mode.
<b>Desirable</b>	Port actively negotiates channeling status with the interface on the other end of the link. A channel is formed if the other side is Auto or Desirable.

The table below lists if an EtherChannel will be formed or not for PAgP:

<b>PAgP</b>	<b>Desirable</b>	<b>Auto</b>
<b>Desirable</b>	Yes	Yes
<b>Auto</b>	Yes	<b>No</b>

### Link Aggregation Protocol (LACP)

LACP also dynamically negotiates the formation of a channel. There are two LACP modes:

<b>Passive</b>	Responds to LACP messages but does not aggressively negotiate a LACP EtherChannel. A channel is formed only if the other end is set to Active
<b>Active</b>	Port actively negotiates channeling with the interface on the other end of the link. A channel is formed if the other side is Passive or Active

The table below lists if an EtherChannel will be formed or not for LACP:

LACP	Active	Passive
Active	Yes	Yes
Passive	Yes	<b>No</b>

In general, **Auto** mode in PAgP is the same as **Passive** mode in LACP and **Desirable** mode is same as **Active** mode.

Auto = Passive

Desirable = Active

### Static ("On")

In this mode, no negotiation is needed. The interfaces become members of the EtherChannel immediately. When using this mode make sure the other end must use this mode too because they will not check if port parameters match. Otherwise the EtherChannel would not come up and may cause some troubles (like loop...).

(<http://packetlife.net/blog/2010/jan/18/etherchannel-considerations/>)

Note: All interfaces in an EtherChannel must be configured identically to form an EtherChannel. Specific settings that must be identical include:

- + Speed settings
- + Duplex settings
- + STP settings
- + VLAN membership (for access ports)
- + Native VLAN (for trunk ports)
- + Allowed VLANs (for trunk ports)
- + Trunking Encapsulation (ISL or 802.1Q, for trunk ports)

### EtherChannel Configuration

To assign and configure an EtherChannel interface to an EtherChannel group, use the **channel-group** command in interface mode:

**channel-group** *number* **mode** { active | on | {auto [non-silent]} | {desirable [non-silent]} | passive }

For example we will create channel-group number 1:

#### Switch(config-if)#channel-group 1 mode ?

**active** Enable LACP unconditionally

**auto** Enable PAgP only if a PAgP device is detected

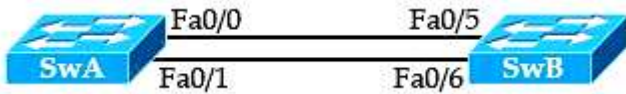
**desirable** Enable PAgP unconditionally

**on** Enable Etherchannel only

**passive** Enable LACP only if a LACP device is detected

If a port-channel interface has not been created before using this command, it will be created automatically and you will see this line: "Creating a port-channel interface Port-channel 1".

In this example, we will create an EtherChannel via LACP between SwA & SwB with the topology shown below:



SwA Configuration	SwB Configuration
<pre>//Assign EtherChannel group 1 to fa0/0 and fa0/1 and set Active mode on them SwA(config)#interface range fa0/0 – 1 SwA(config-if-range)#channel-group 1 mode active <b>Creating a port-channel interface Port- channel 1</b> //Next configure the representing port-channel interface as trunk SwA(config)#interface port-channel 1 SwA(config-if)#switchport trunk encapsulation dot1q SwA(config-if)#switchport mode trunk</pre>	<pre>//Assign EtherChannel group 2 to fa0/5 and fa0/6 and set Passive mode on them SwB(config)#interface range fa0/5 – 6 SwB(config-if-range)#channel-group 2 mode passive <b>Creating a port-channel interface Port- channel 2</b> //Next configure the representing port-channel interface as trunk SwB(config)#interface port-channel 2 SwB(config-if)#switchport trunk encapsulation dot1q SwB(config-if)#switchport mode trunk</pre>

That is all the configuration for the EtherChannel to work well on both switches. We can verify with the "show etherchannel <port-channel number> port-channel" or "show etherchannel summary" command.

## Telnet

### To remotely access the device

pc -----telnet-----switch/router

```
switch/router#configure terminal
switch/router(config)#line vty 0 1 (2 lines)
```

### When we can give vty 0 15 ( it means 16 lines )

```
switch/router(config-line)#password cisco
switch/router(config-line)#login
switch/router(config-line)#exit
```

```
switch/router(config)#enable password cisco
```

```
switch# show users      (To check the status of vty ( virtual terminal) lines)
```

## SSH

**To remotely access the device , it creates encrypted session**

Step 1. As a requirement to generate an RSA general-usage key you'll need to change the hostname to a hostname other than the default "Router" hostname. In this case, you can use R1 as shown below;

```
Router>enable
```

```
Password:
```

```
Router#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#hostname R1
```

```
R1(config)#ip domain-name ccies.in
```

```
R1(config)#crypto key generate rsa modulus 2048
```

```
R1(config)#
```

. Configure the transport input protocol on the VTY lines to accept only SSH by executing the transport input ssh under the vty line configuration mode as shown below;

```
R1(config)#line vty 0 4
```

```
R1(config-line)#transport input ssh
```

Step 6. Verify your SSH configuration by using the Cisco IOS SSH client and SSH to the routers loopback interface 10.1.1.1

```
R1(config-line)#end
```

```
R1#ssh -l john 10.1.1.1
```

```
Password:
```

```
R1#ssh -l john 10.1.1.1
```



Password:

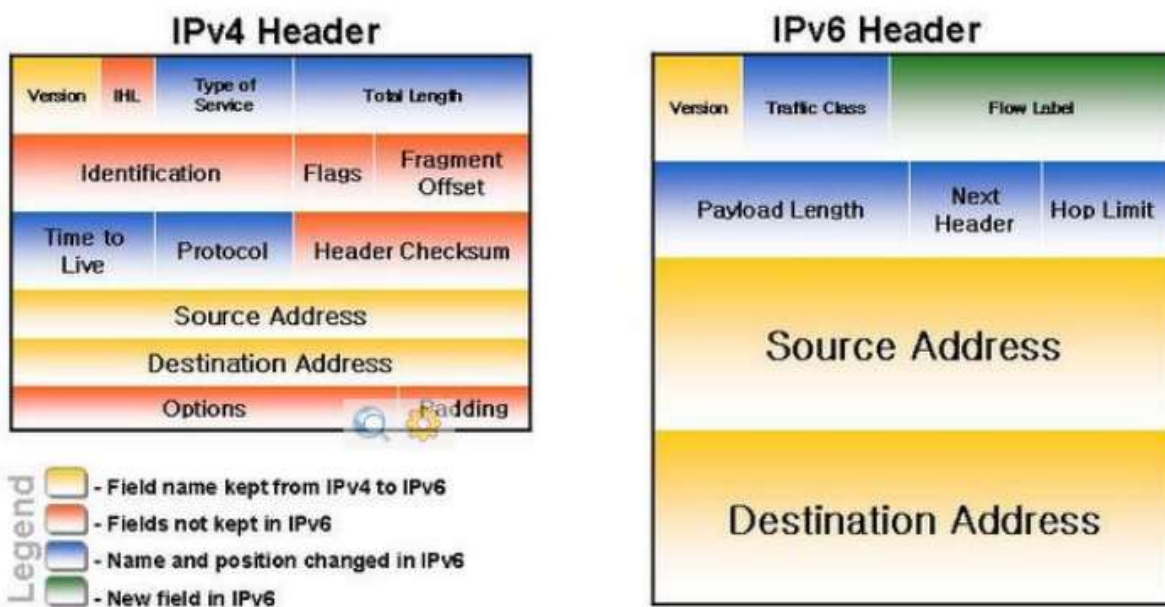
R1#show ssh

```

Connection Version Mode Encryption Hmac      State      Username
0          1.99  IN  aes128-cbc hmac-sha1  Session started  john
0          1.99  OUT aes128-cbc hmac-sha1  Session started  john
%No SSHv1 server connections running.

```

## IPV6



**IPv4 released in 1980 , 32 bit** therefore support  $2^{32}$  (4,294,967,296) addresses

**IPv6 released in 1999 , 128 bit** (approximately 340 [undecillion](#) or  $3.4 \times 10^{38}$ ) addresses

**340,282,366,920,938,463,463,374,607,431,768,211,456**

### IPv6 Address Types

Address Type	Description
Unicast	One to One (Global, Link local, Site local)

	+ An address destined for a single interface.
Multicast	One to Many + An address for a set of interfaces + Delivered to a group of interfaces identified by that address. + Replaces IPv4 "broadcast"
Anycast	One to Nearest (Allocated from Unicast) + Delivered to the closest interface as determined by the IGP

**2001:0000:0000:0012:0000:0000:1234:56ab**

### The Benefits and Uses of IPv6

- IPv6 also allows multiple addresses for hosts and networks.
- IPv6 uses multicast traffic. it dont have broadcast

**Unicast: - one to one**

**Multicast: - one to many**

**Anycast: - one to closest**

2001:0db8:3c4d:0012:**0000:0000**:1234:56ab      **\_\_\_\_\_8 groups \_\_\_\_1 group = 16 bit\_\_4 hexadecimal**

**Not easy to remember:- we have 2 rules**

#### 1. Eliminate the consecutive zero's:- represent with double :: ( colon's)

2001:0000:0000:0012:**0000:0000**:1234:56ab  
 2001:0000:0000:0012::**1234:56ab**  
 2001:0:0:12::**1234:56ab**

## 2 Eliminate the Leading zeros

2001:0000:0000:0012:**0000:0000**:1234:56ab  
 2001:0000:0000:0012::1234:56ab  
 2001:0:0:12::1234:56ab

### Example:

2001:0000:0000:0012:0000:0000:1234:56ab

2001:0:0:12:**0 : 0**:1234:56ab

2001:: **12 :: 1234: 56ab (wrong)**

2001::12:**0:0**:1234:56ab (correct)

### Example:

2001:C:7:ABCD::1/64 is really

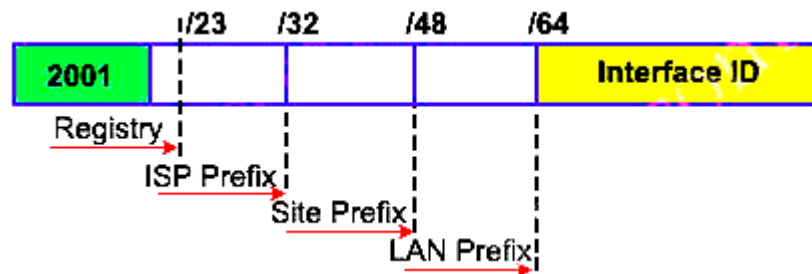
2001:000C:0007:ABCD:0000:0000:0000:0001/64

+ The first 64-bits 2001:000C:0007:ABCD is the address prefix

+ The last 64-bits 0000:0000:0000:0001 is the interface ID

+ /64 is the prefix length (/64 is well-known and also the prefix length in most cases)

The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for the assignment of IPv6 addresses. ICANN assigns a range of IP addresses to Regional Internet Registry (RIR) organizations. The size of address range assigned to the RIR may vary but with a minimum prefix of /12 and belong to the following range: 2000::/12 to 200F:FFFF:FFFF:FFFF::/64.



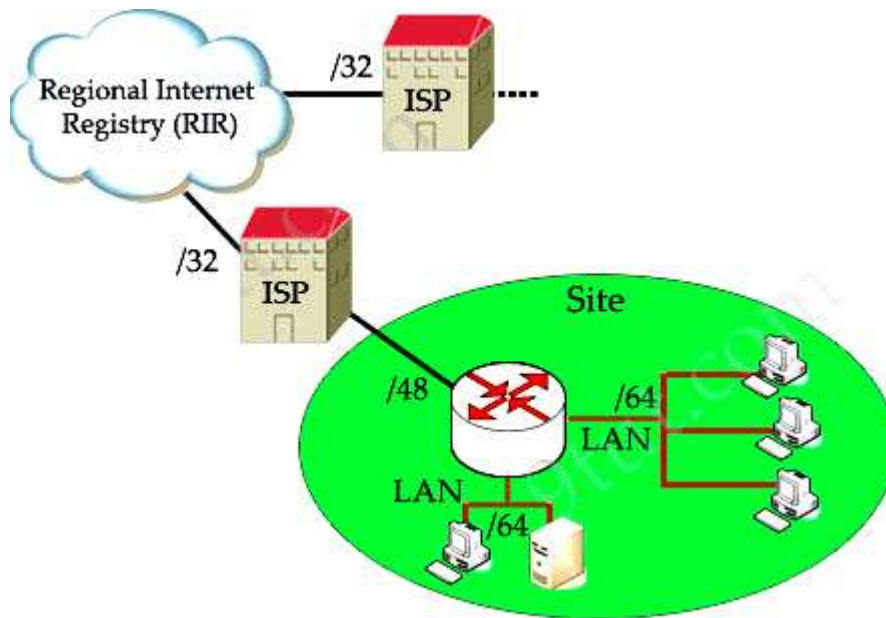
Each ISP receives a /32 and provides a /48 for each site -> every ISP can provide  $2^{(48-32)} = 65,536$  site addresses (note: each network organized by a single entity is often called a site).

Each site provides /64 for each LAN -> each site can provide  $2^{(64-48)} = 65,536$  LAN addresses for use in their private networks.

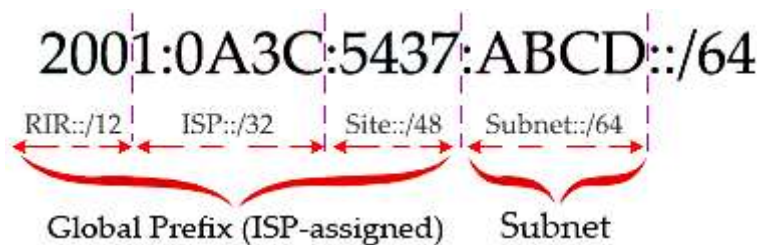
So each LAN can provide  $2^{64}$  interface addresses for hosts.

-> Global routing information is identified within the first 64-bit prefix.

Note: The number that represents the range of addresses is called a prefix



Now let's see an example of IPv6 prefix: 2001:0A3C:5437:ABCD::/64:



In this example, the RIR has been assigned a 12-bit prefix. The ISP has been assigned a 32-bit prefix and the site is assigned a 48-bit site ID. The next 16-bit is the subnet field and it can allow  $2^{16}$ , or 65536 subnets. This number is redundant for largest corporations on the world!

The 64-bit left (which is not shown the above example) is the Interface ID or host part and it is much more bigger: 64 bits or  $2^{64}$  hosts per subnet! For example, from the prefix 2001:0A3C:5437:ABCD::/64 an administrator can assign an IPv6 address 2001:0A3C:5437:ABCD:**218:34EF:AD34:98D** to a host.

### IPv6 Address Scopes

Address types have well-defined destination scopes:

IPv6 Address Scopes	Description
---------------------	-------------

<b>Link-local address</b>	<ul style="list-style-type: none"> <li>+ only used for communications within the local subnetwork (automatic address configuration, neighbor discovery, router discovery, and by many routing protocols). It is only valid on the current subnet.</li> <li>+ routers do not forward packets with link-local addresses.</li> <li>+ are allocated with the FE80::/64 prefix -&gt; can be easily recognized by the prefix FE80. Some books indicate the range of link-local address is FE80::/10, meaning the first 10 bits are fixed and link-local address can begin with FE80, FE90, FEA0 and FEB0 but in fact the next 54 bits are all 0s so you will only see the prefix FE80 for link-local address.</li> <li>+ same as 169.254.x.x in IPv4, it is assigned when a DHCP server is unavailable and no static addresses have been assigned</li> <li>+ is usually created dynamically using a link-local prefix of FE80::/10 and a 64-bit interface identifier (based on 48-bit MAC address).</li> </ul>
<b>Global unicast address</b>	<ul style="list-style-type: none"> <li>+ unicast packets sent through the public Internet</li> <li>+ globally unique throughout the Internet</li> <li>+ starts with a 2000::/3 prefix (this means any address beginning with 2 or 3). But in the future global unicast address might not have this limitation</li> </ul>
<b>Site-local address</b>	<ul style="list-style-type: none"> <li>+ allows devices in the same organization, or site, to exchange data.</li> <li>+ starts with the prefix FEC0::/10. They are analogous to IPv4's private address classes.</li> <li>+ Maybe you will be surprised because Site-local addresses are no longer supported (deprecated) by RFC 3879 so maybe you will not see it in the future.</li> </ul>

All nodes must have at least one link-local address, although each interface can have multiple addresses.

However, using them would also mean that NAT would be required and addresses would again not be end-to-end.

Site-local addresses are no longer supported (deprecated) by RFC 3879.

### Special IPv6 Addresses

Reserved Multicast Address	Description
<b>FF02::1</b>	+ All nodes on a link (link-local scope).
<b>FF02::2</b>	+ All routers on a link
<b>FF02::5</b>	+ OSPFv3 All SPF routers

<b>FF02::6</b>	+ OSPFv3 All DR routers
<b>FF02::9</b>	+ All routing information protocol (RIP) routers on a link
<b>FF02::A</b>	+ EIGRP routers
<b>FF02::1:FFxx:xxxx</b>	+ All solicited-node multicast addresses used for host auto-configuration and neighbor discovery (similar to ARP in IPv4) + The xx:xxxx is the far right 24 bits of the corresponding unicast or anycast address of the node
<b>FF05::101</b>	+ All Network Time Protocol (NTP) servers

#### Reserved IPv6 Multicast Addresses

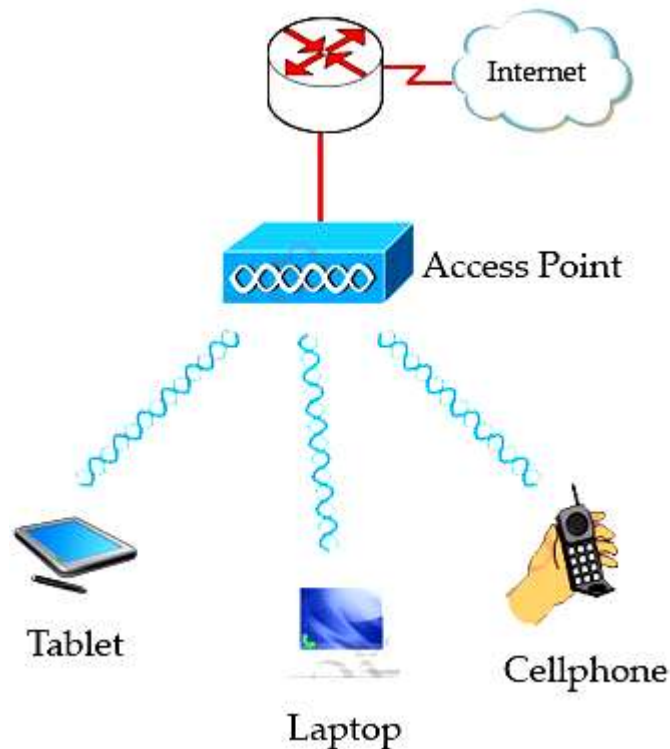
Reserved Multicast Address	Description
FF02::1	+ All nodes on a link (link-local scope).
FF02::2	+ All routers on a link
FF02::9	+ All routing information protocol (RIP) routers on a link
FF02::1:FFxx:xxxx	+ All solicited-node multicast addresses used for host auto-configuration and neighbor discovery (similar to ARP in IPv4) + The xx:xxxx is the far right 24 bits of the corresponding unicast or anycast address of the node
FF05::101	+ All Network Time Protocol (NTP) servers

## Wi-Fi



## Wi-Fi: - wireless fidelity

Wireless LAN (WLAN) is very popular nowadays. Maybe you have ever used some wireless applications on your laptop or cellphone. Wireless LANs enable users to communicate without the need of cable. Below is an example of a simple WLAN:



Each WLAN network needs a wireless Access Point (AP) to transmit and receive data from users. Unlike a wired network which operates at full-duplex (send and receive at the same time), a wireless network operates at half-duplex so sometimes an AP is referred to as a Wireless Hub.

The major difference between wired LAN and WLAN is WLAN transmits data by radiating energy waves, called radio waves, instead of transmitting electrical signals over a cable.

Also, WLAN uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) instead of CSMA/CD for media access. WLAN can't use CSMA/CD as a sending device can't transmit and receive data at the same time. CSMA/CA operates as follows:

- + Listen to ensure the media is free. If it is free, set a random time before sending data
- + When the random time has passed, listen again. If the media is free, send the data. If not, set another random time again
- + Wait for an acknowledgment that data has been sent successfully
- + If no acknowledgment is received, resend the data

### IEEE 802.11 standards:

Nowadays there are three organizations influencing WLAN standards. They are:

- + ITU-R: is responsible for allocation of the RF bands
- + IEEE: specifies how RF is modulated to transfer data
- + Wi-Fi Alliance: improves the interoperability of wireless products among vendors

But the most popular type of wireless LAN today is based on the IEEE 802.11 standard, which is known informally as Wi-Fi.

\* **802.11a:** operates in the 5.7 GHz ISM band. Maximum transmission speed is 54Mbps and approximate wireless range is 25-75 feet indoors.

\* **802.11b:** operates in the 2.4 GHz ISM band. Maximum transmission speed is 11Mbps and approximate wireless range is 100-200 feet indoors.

\* **802/11g:** operates in the 2.4 GHz ISM band. Maximum transmission speed is 54Mbps and approximate wireless range is 100-200 feet indoors.

**ISM Band:** The ISM (Industrial, Scientific and Medical) band, which is controlled by the FCC in the US, generally requires licensing for various spectrum use. To accommodate wireless LAN's, the FCC has set aside bandwidth for unlicensed use including the 2.4Ghz spectrum where many WLAN products operate.

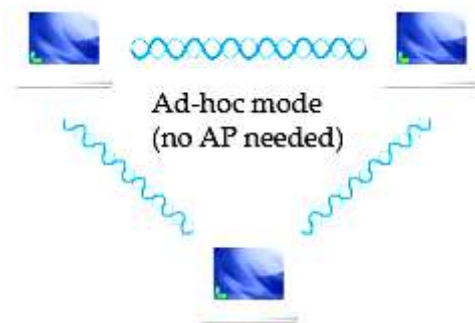
**Wi-Fi:** stands for Wireless Fidelity and is used to define any of the IEEE 802.11 wireless standards. The term Wi-Fi was created by the Wireless Ethernet Compatibility Alliance (WECA). Products certified as Wi-Fi compliant are interoperable with each other even if they are made by different manufacturers.

Access points can support several or all of the three most popular IEEE WLAN standards including 802.11a, 802.11b and 802.11g.

### WLAN Modes:

WLAN has two basic modes of operation:

\* **Ad-hoc mode:** In this mode devices send data directly to each other without an AP.

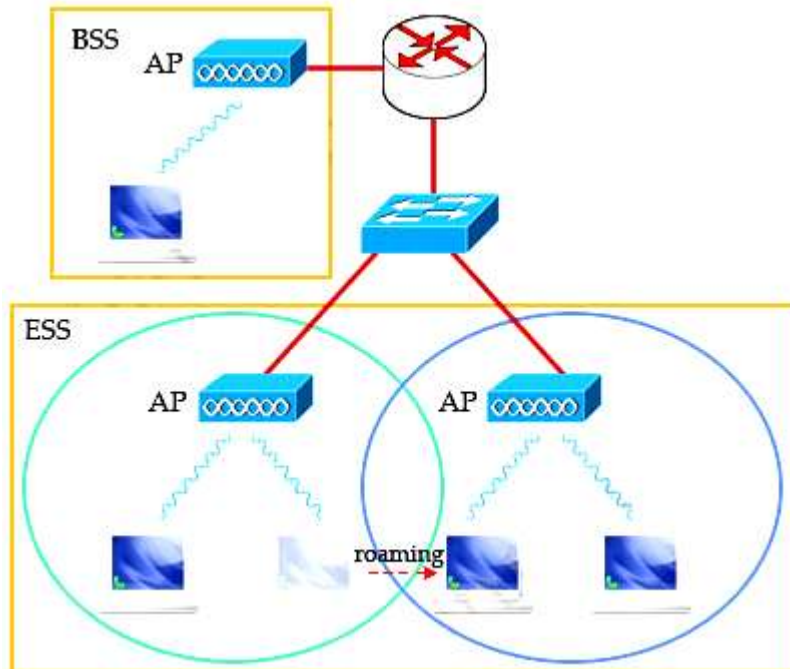


\* **Infrastructure mode:** Connect to a wired LAN, supports two modes (service sets):

+ Basic Service Set (BSS): uses only a single AP to create a WLAN

+ Extended Service Set (ESS): uses more than one AP to create a WLAN, allows roaming in a larger area than a single AP. Usually there is an overlapped area between two APs to support roaming. The overlapped area should be more than 10% (from 10% to 15%) to allow users moving between two APs without losing their connections (called roaming). The two adjacent APs should use non-overlapping channels to avoid interference. The most popular non-overlapping channels are channels 1, 6 and 11 (will be explained later).





**Roaming:** The ability to use a wireless device and be able to move from one access point's range to another without losing the connection.

When configuring ESS, each of the APs should be configured with the same Service Set Identifier (SSID) to support roaming function. SSID is the unique name shared among all devices on the same wireless network. In public places, SSID is set on the AP and broadcasts to all the wireless devices in range. SSIDs are case sensitive text strings and have a maximum length of 32 characters. SSID is also the minimum requirement for a WLAN to operate. In most Linksys APs (a product of Cisco), the default SSID is "linksys".

Encoding	Used by
<b>FHSS</b>	The original 802.11 WLAN standards used FHSS, but the current standards (802.11a, 802.11b, and 802.11g) do not
<b>DSSS</b>	802.11b
<b>OFDM</b>	802.11a, 802.11g, 802.11n

### WLAN Security Standards

Security is one of the most concerns of people deploying a WLAN so we should grasp them.

#### Wired Equivalent Privacy (WEP)

WEP is the original security protocol defined in the 802.11b standard so it is very weak comparing to newer security protocols nowadays.

WEP is based on the RC4 encryption algorithm, with a secret key of 40 bits or 104 bits being combined with a 24-bit Initialisation Vector (IV) to encrypt the data (so sometimes you will hear

"64-bit" or "128-bit" WEP key). But RC4 in WEP has been found to have weak keys and can be cracked easily within minutes so it is not popular nowadays.

The weak points of WEP is the IV is too small and the secret key is static (the same key is used for both encryption and decryption in the whole communication and never expires).

### Wi-Fi Protected Access (WPA)

In 2003, the Wi-Fi Alliance developed WPA to address WEP's weaknesses. Perhaps one of the most important improvements of WPA is the Temporal Key Integrity Protocol (TKIP) encryption, which changes the encryption key dynamically for each data transmission. While still utilizing RC4 encryption, TKIP utilizes a temporal encryption key that is regularly renewed, making it more difficult for a key to be stolen. In addition, data integrity was improved through the use of the more robust hashing mechanism, the Michael Message Integrity Check (MMIC).

In general, WPA still uses RC4 encryption which is considered an insecure algorithm so many people viewed WPA as a temporary solution for a new security standard to be released (WPA2).

### Wi-Fi Protected Access 2 (WPA2)

In 2004, the Wi-Fi Alliance updated the WPA specification by replacing the RC4 encryption algorithm with Advanced Encryption Standard-Counter with CBC-MAC (AES-CCMP), calling the new standard WPA2. AES is much stronger than the RC4 encryption but it requires modern hardware.

Standard	Key Distribution	Encryption
WEP	Static Pre-Shared	Weak
WPA	Dynamic	TKIP
WPA2	Both (Static & Dynamic)	AES

### Wireless Interference

The 2.4 GHz & 5 GHz spectrum bands are unlicensed so many applications and devices operate on it, which cause interference. Below is a quick view of the devices operating in these bands:

**+ Cordless phones:** operate on 3 frequencies, 900 MHz, 2.4 GHz, and 5 GHz. As you can realize, 2.4 GHz and 5 GHz are the frequency bands of 802.11b/g and 802.11a wireless LANs.

Most of the cordless phones nowadays operate in 2.4 GHz band and they use frequency hopping spread spectrum (FHSS) technology. As explained above, FHSS uses all frequencies in the the entire 2.4 GHz spectrum while 802.11b/g uses DSSS which operates in about 1/3 of the 2.4 GHz band (1 channel) so the use of the cordless phones can cause significant interference to your WLAN.



An example of cordless phone

**+ Bluetooth:** same as cordless phone, Bluetooth devices also operate in the 2.4 GHz band with FHSS technology. Fortunately, Bluetooth does not cause as much trouble as cordless phone because it usually transfers data in a short time (for example you copy some files from your laptop to your cellphone via Bluetooth) within short range. Moreover, from version 1.2 Bluetooth defined the adaptive frequency hopping (AFH) algorithm. This algorithm allows Bluetooth devices to periodically listen and mark channels as good, bad, or unknown so it helps reduce the interference with our WLAN.

**+ Microwaves** (mostly from oven): do not transmit data but emit high RF power and heating energy. The magnetron tubes used in the microwave ovens radiate a continuous-wave-like at frequencies close to 2.45 GHz (the center burst frequency is around 2.45 – 2.46 GHz) so they can interfere with the WLAN.

**+ Antenna:** There are a number of 2.4 GHz antennas on the market today so they can interfere with your wireless network.

**+ Metal materials** or materials that conduct electricity deflect Wi-Fi signals and create blind spots in your coverage. Some of examples are metal siding and decorative metal plates.

**+ Game controller, Digital Video Monitor, Wireless Video Camera, Wireless USB** may also operate at 2.4 GHz and cause interference too.

## WAN :- wide area network

A WAN is a data communications network that operates beyond the geographic scope of a LAN.

### 1. Wireless

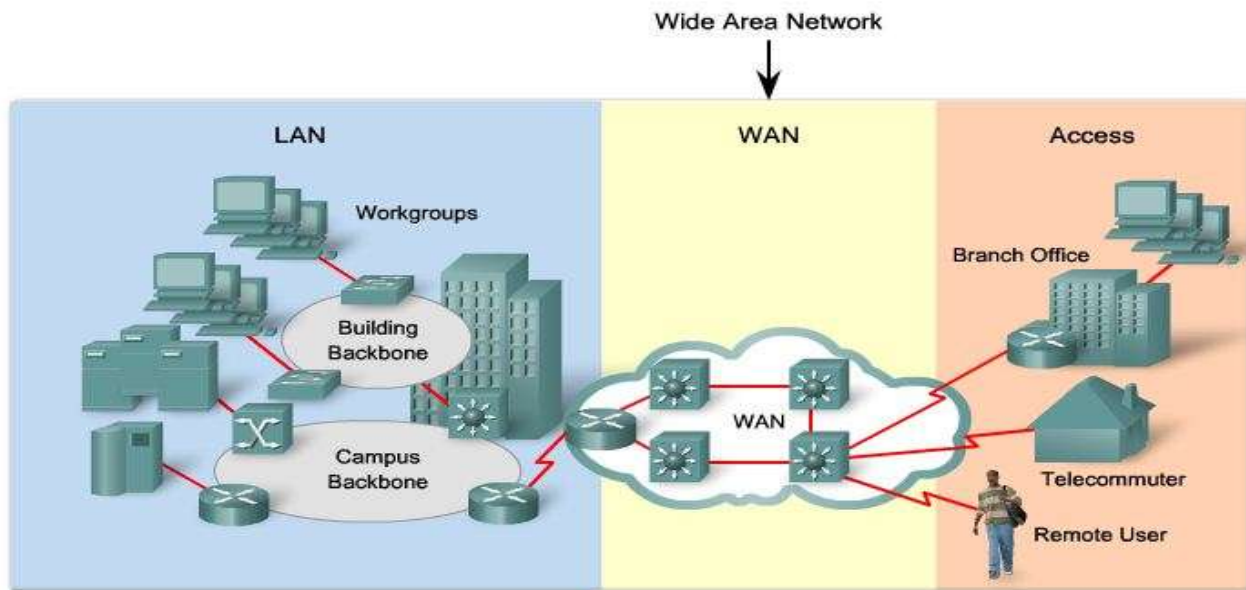
2. Satellite

3. Cables: - 1. Leased lines ---- dedicated lines

2. Circuit switching

3 . Packet switching

Option	Description	Advantages	Disadvantages	Sample protocols used
Leased line	Point-to-Point connection between two computers or Local Area Networks (LANs).	Most secure	Expensive	PPP, HDLC, SDLC, HNAS
Circuit switching	A dedicated circuit path is created between endpoints. Best example is dialup connections.	Less expensive	Call setup	PPP, ISDN
Packet switching	Devices transport packets via a shared single point-to-point or point-to-multipoint link across a carrier interwork. Variable length packets are transmitted over permanent virtual circuits (PVCs) or switched virtual		Shared media across link	X.25, Frame Relay



## WAN Protocols

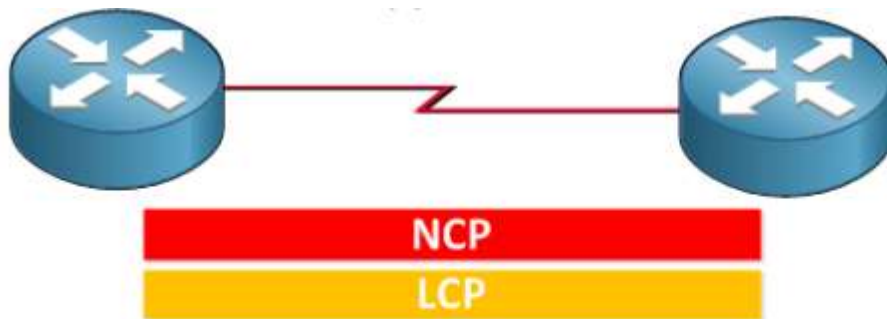
*Leased Lines uses two types of WAN encapsulation protocols:*

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

<b>HDLC</b>	<b>PPP</b>
<ul style="list-style-type: none"> <li>• Higher level data link Control protocol</li> <li>• Cisco Proprietary Layer 2 WAN Protocol</li> <li>• Doesn't support Authentication</li> <li>• Doesn't support Compression and error correction</li> </ul>	<ul style="list-style-type: none"> <li>• Point to Point Protocol</li> <li>• Standard Layer 2 WAN Protocol</li> <li>• Supports Authentication</li> <li>• Support error correction</li> </ul>

**PPP uses two Protocols**

**NCP: Network Control Protocol**  
**LCP : link Control Protocol**



NCP will make sure you can run different protocols over our PPP link like IP, IPv6 but also CDP (Cisco Discovery Protocol) and older protocols like IPX or Appletalk.

So in short if you enable PPP on both routers this is what happens:

1. LCP: Takes care of setting up the link.
2. (Optional): Authentication.
3. NCP: Makes sure we can send IP and other protocols across our PPP link.

oco

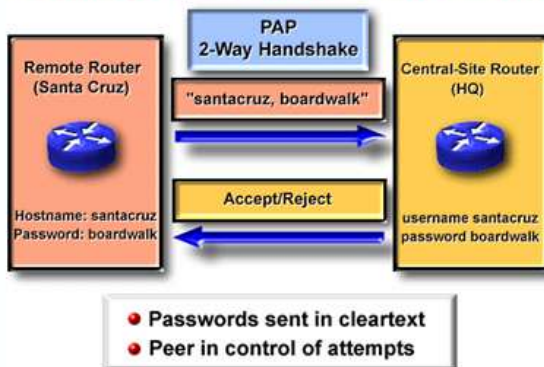
### **PPP supports two authentication protocols:**

- 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
- PAP is not a strong authentication protocol.
- Passwords are sent across the link in clear text.

### **Selecting a PPP Authentication Protocol**

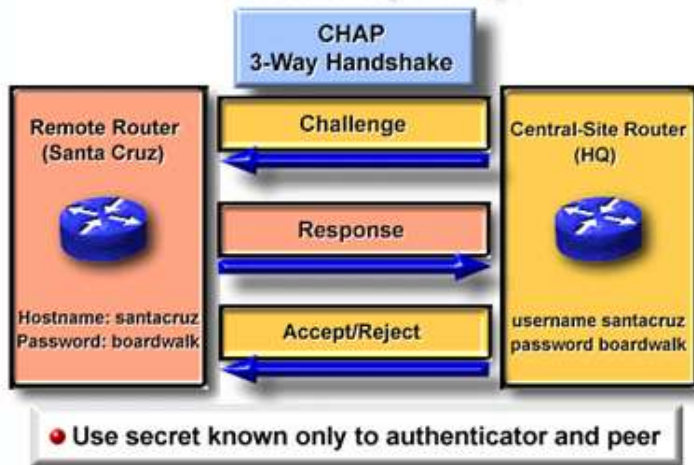


### **CHAP (Challenge Handshake Authentication Protocol)**

- 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.

### Selecting a PPP Authentication Protocol (con't.)



#### Configuration of HDLC:-

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

#### Configuration of PPP:

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

#### 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
```



<b>DCE</b>	<b>DTE</b>
<ul style="list-style-type: none"> <li>• <i>Data Communication Equipment</i></li> <li>• <i>Generate clocking (i.e. Speed).</i></li> <li>• <i>Example of DCE device in Leased line setup : V.35 &amp; G.703 Modem &amp; Exchange (Modem &amp; MUX)</i></li> <li>• <i>Example of DCE device in Dial up setup : Dialup Modem</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Data Termination Equipment</i></li> <li>• <i>Accept clocking (i.e. Speed).</i></li> <li>• <i>Example of DTE device in Leased line setup : Router</i></li> <li>• <i>Example of DTE device in Dial up setup : Computer</i></li> </ul>

**Router # show controllers (s0/0 or s0/1)**

*(To know whether the cable connected to the serial interface is DCE or DTE)*



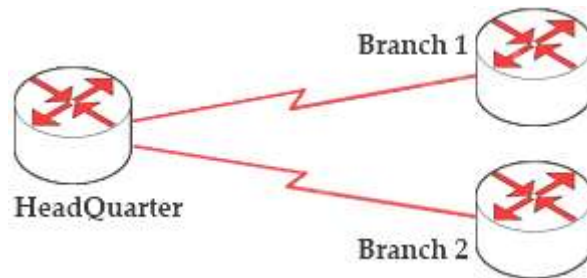
**V.35 Back to Back Cable**



## Frame relay:-

### Why do we need Frame Relay?

Let's take a simple example. Suppose you are working in a big company and your company has just expanded to two new locations. The main site is connected to two branch offices, named Branch 1 & Branch 2 and your boss wants these two branches can communicate with the main site. The most simple solution is to connect them directly (called a leased line) as shown below:



To connect to these two branches, the main site router, HeadQuarter, requires two serial interfaces which a router can provide. But what happens when the company expands to 10 branches, 50 branches? For each point-to-point line, HeadQuarter needs a separate physical serial interface (and maybe a separate CSU/DSU if it is not integrated into the WAN card). As you can imagine, it will need many routers with many interfaces and lots of rack space for the routers and CSU/DSUs. Maybe we should use another solution for this problem? Luckily, Frame Relay can do it!

By using Frame Relay we only need one serial interface at the HeadQuarter to connect to all branches. This is also true when we expand to 10 or 50 branches. Moreover, the cost is much lesser than using leased-lines.



Frame Relay is a high-performance WAN protocol that operates at the physical and data link layers of the OSI reference model. It offers lower-cost data transfer when compared to typical point-to-point applications, by using virtual connections within the frame relay network and by combining those connections into a single physical connection at each location. Frame relay providers use a frame relay switch to route the data on each virtual circuit to the appropriate destination.

Maybe these terminologies of Frame Relay are difficult to understand so we will explain them in more detail in this article.

### DCE & DTE

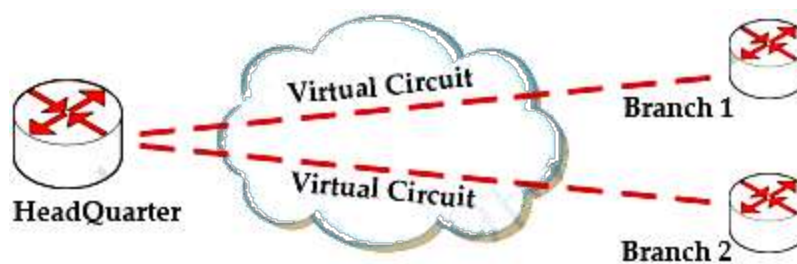
The first concept in Frame Relay you must grasp is about DTE & DCE:

- + Data terminal equipment (DTE), which is actually the user device and the logical Frame-relay end-system
- + Data communication equipment (DCE, also called data circuit-terminating equipment), which consists of modem and packet switch

In general, the routers are considered DTE, and the Frame Relay switches are DCE. The purpose of DCE equipment is to provide clocking and switching services in a network. In our example, HeadQuarter, Branch 1 & Branch 2 are DTEs while Frame Relay switches are DCEs.

### Virtual Circuits

The logical connection through the Frame Relay network between two DTEs is called a virtual circuit (VC). The term "virtual" here means that the two DTEs are not connected directly but through a network. For example, the HeadQuarter & Branch 1 (or Branch 2) can communicate with each other as if they were directly connected but in fact they are connected through a Frame Relay network with many Frame Relay switches between them.



There are two types of VCs

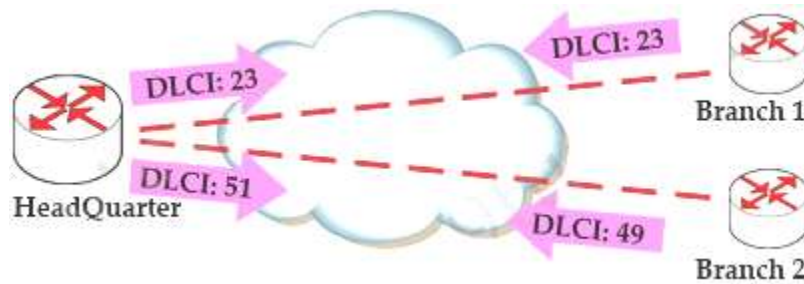
- + **switched virtual circuits (SVCs)**: are temporary connections that are only used when there is sporadic data transfer between DTE devices across the Frame Relay network. SVC is set up dynamically when needed. SVC connections require call setup and termination for each connection.
- + **permanent virtual circuits (PVCs)**: A predefined VC. A PVC can be equated to a leased line in concept.

Nowadays most service providers offer PVC service only to save additional costs for signaling and billing procedures.

### DLCI

Although the above picture shows two VCs from the HeadQuarter but do you remember that the HeadQuarter only has only one serial interface? So how can it know which branch it should send the frame to?

Frame-relay uses data-link connection identifiers (DLCIs) to build up logical circuits. The identifiers have local meaning only, that means that their values are unique per router, but not necessarily in the other routers. For example, there is only one DLCI of 23 representing for the connection from HeadQuarter to Branch 1 and only one DLCI of 51 from HeadQuarter to Branch 2. Branch 1 can use the same DLCI of 23 to represent the connection from it to HeadQuarter. Of course it can use other DLCIs as well because DLCIs are just local significant.

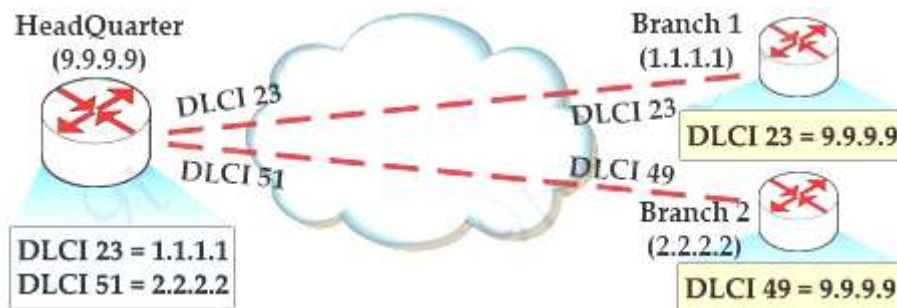


By including a DLCI number in the Frame Relay header, HeadQuarter can communicate with both Branch 1 and Branch 2 over the same physical circuit.

DLCI values typically are assigned by the Frame Relay service provider (for example, the telephone company). In Frame Relay, DLCI is a 10-bit field.

Before DLCI can be used to route traffic, it must be associated with the IP address of its remote router. For example, suppose that:

- + HeadQuarter's IP address is 9.9.9.9
- + Branch 1's IP address is 1.1.1.1
- + Branch 2's IP address is 2.2.2.2



Then the HeadQuarter will need to map Branch 1 IP address to DLCI 23 & map Branch 2 IP address to DLCI 51. After that it can encapsulate data inside a Frame Relay frame with an appropriate DLCI number and send to the destination. The mapping of DLCIs to Layer 3 addresses can be handled manually or dynamically.

**\* Manually (static):** the administrators can statically assign a DLCI to the remote IP address by the following statement:

```
Router(config-if)#frame-relay map protocol dlci [broadcast]
```

For example HeadQuarter can assign DLCIs of 23 & 51 to Branch 1 & Branch 2 with these commands:

```
HeadQuarter(config-if)#frame-relay map ip 1.1.1.1 23 broadcast
```

```
HeadQuarter(config-if)#frame-relay map ip 2.2.2.2 51 broadcast
```

We should use the "broadcast" keyword here because by default split-horizon will prevent routing updates from being sent back on the same interface it received. For example, if Branch 1 sends an update to HeadQuarter then HeadQuarter can't send that update to Branch 2 because they are received and sent on the same interface. By using the "broadcast" keyword, we are telling the HeadQuarter to send a copy of any broadcast or multicast packet received on that interface to the virtual circuit specified by the DLCI value in the

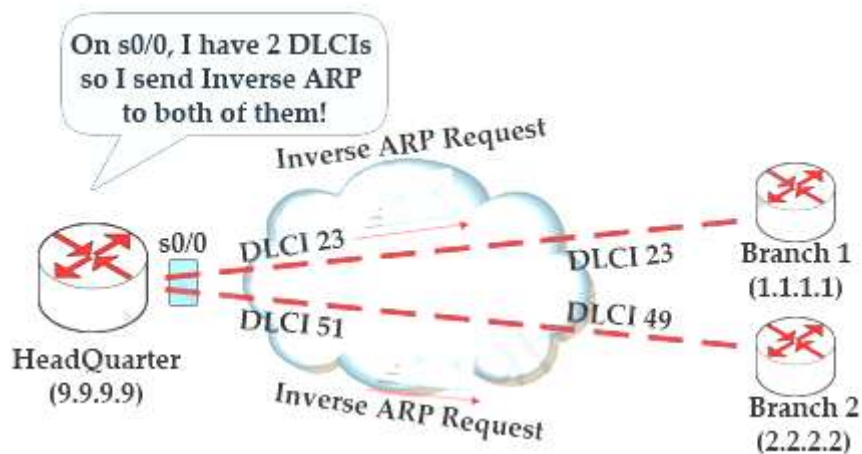
"frame-relay map" statement. In fact the copied packet will be sent via unicast (not broadcast) so sometimes it is called "pseudo-broadcast".

Note: "frame-relay interface-dlci" command can be used to statically assign (bind) a DLCI number to a physical interface.

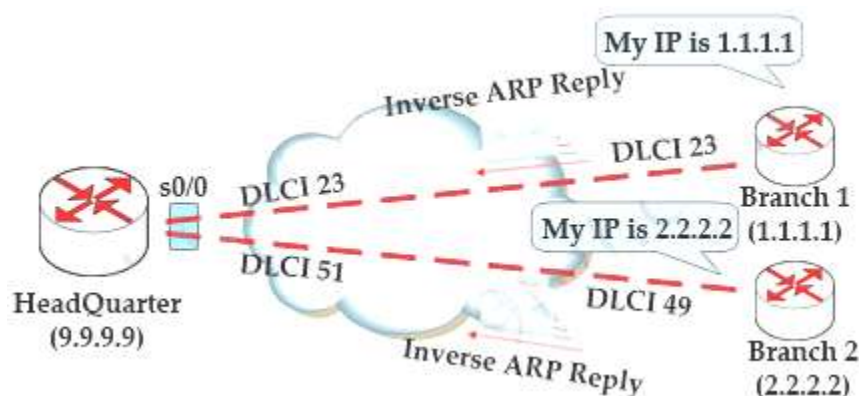
Note: In fact, we need to run a routing protocol (like OSPF, EIGRP or RIP...) to make different networks see each other

**\* Dynamic:** the router can send an **Inverse ARP Request** to the other end of the PVC for its Layer 3 address. In short, Inverse ARP will attempt to learn its neighboring devices IP addresses and automatically create a dynamic map table. By default, physical interfaces have Inverse ARP enabled.

We will take an example of how Inverse ARP works with the topology above. At the beginning, all routers are not configured with static mapping and HeadQuarter has not learned the IP addresses of Branch 1 & 2 yet. It only has 2 DLCI values on s0/0 interface (23 & 51). Now it needs to find out who are attached to these DLCIs so it sends an Inverse ARP Request on s0/0 interface. Notice that the router will send Inverse ARP Request out on every DLCI associated with the interface.



In the Inverse ARP Request, HeadQuarter also includes its IP 9.9.9.9. When Branch 1 & 2 receive this request, they send back an Inverse ARP Reply with their own IP addresses.



Now all the routers have a pair of DLCI & IP address of the router at the other end so data can be forwarded to the right destination.

In this example you can see that each router has a DLCI first (Layer 2) and it needs to find out the IP address (Layer 3). This process is opposite of the ARP process (ARP translates Layer 3 address to Layer 2 address) so it is called Inverse ARP.

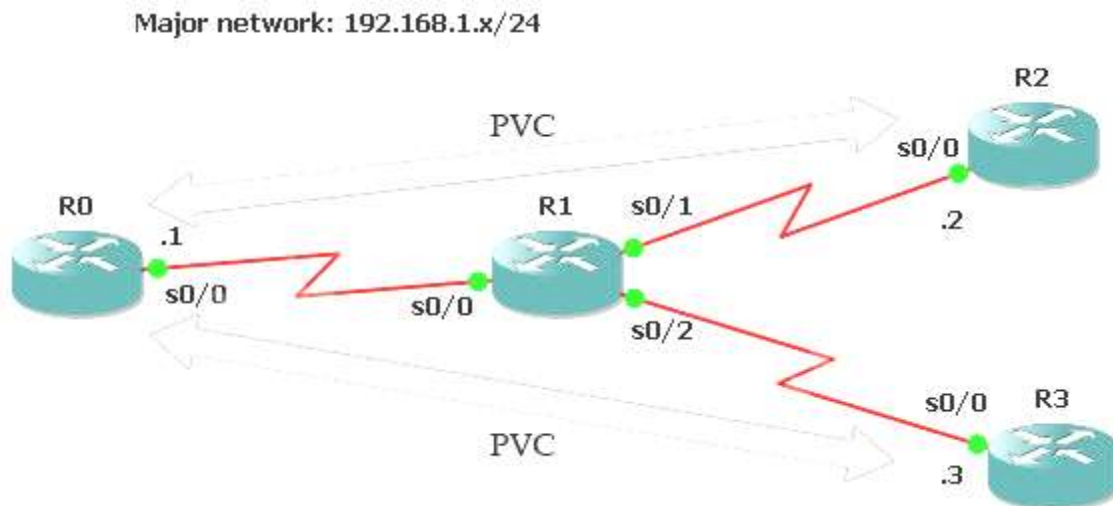
After the Inverse ARP process completes, we can use the "show frame-relay map" to check. The word "dynamic" indicates the mapping was learned through Inverse ARP (the output below is not related to the above topology):

```
R2#show frame-relay map
Serial0/0 <up>: ip 192.168.1.1 dlci 201(0xC9,0x3090), dynamic,
                broadcast,, status defined, active
R2#
```

By default, routers send Inverse ARP messages on all active DLCIs every 60 seconds.

Another thing you should notice is when you supply a static map (via "frame-relay map" command), Inverse ARP is automatically disabled for the specified protocol on the specified DLCI.

First we create 4 routers and link them as follows:



### Configure IP addresses

First we will assign IP addresses for all relevant interfaces. Notice that R1 will be Frame-Relay switch in this lab so its interfaces don't need IP addresses.

On R0:

```
R0#configure terminal
R0(config)#interface s0/0
R0(config-if)#ip address 192.168.1.1 255.255.255.0
R0(config-if)#no shutdown
```

On R2:

```
R2#configure terminal
R2(config)#interface s0/0
```

```
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shutdown
```

On R3:

```
R3#configure terminal
R3(config)#interface s0/0
R3(config-if)#ip address 192.168.1.3 255.255.255.0
R3(config-if)#no shutdown
```

### **Configure Frame-Relay (using Inverse ARP)**

To configure Frame-Relay on R0, R2 and R3 we need to enable Frame-Relay encapsulation and specify a type of LMI (ansi – in this case). Notice that Inverse ARP is enabled by default on Cisco routers so we don't need to type anything to activate it.

```
R0,R2,R3(config)#interface s0/0
R0,R2,R3(config-if)#encapsulation frame-relay
R0,R2,R3(config-if)#frame-relay lmi-type ansi
```

### **Configure R1 as a Frame-Relay switch**

In this lab R1 will be configured as a Frame-relay switch so no IP address is required.

Turn on Frame-Relay switching feature on R1:

```
R1(config)#frame-relay switching
```

On each interface we must specify how the frame will be proceeded. In practical, the Frame-Relay switch (R1) is placed at the ISP side so its interfaces should be set to DCE.

```
R1(config)# interface s0/0
R1(config-if)#encapsulation frame-relay
R1(config-if)#frame-relay lmi-type ansi
R1(config-if)#frame-relay intf-type dce //This command specifies the interface to handle LMI
like a Frame Relay DCE device.
R1(config-if)#clock rate 64000
R1(config-if)#frame-relay route 102 interface Serial0/1 201 (will be explained later)
R1(config-if)#frame-relay route 103 interface Serial0/2 301
```

The command **frame-relay route 102 interface Serial0/1 201** means frame-relay traffic come to R1 which has a DLCI of 102 will be sent to interface Serial0/1 with a DLCI of 201.

Note: Data link connection identifiers (DLCIs) are numbers that refer to paths through the Frame Relay network. They are only locally significant.

Continue configuring s0/1 & s0/2 interfaces (same as s0/0)

```
R1(config)# interface s0/1
R1(config-if)#encapsulation frame-relay
R1(config-if)#frame-relay lmi-type ansi
```



```

R1(config-if)#frame-relay intf-type dce
R1(config-if)#clock rate 64000
R1(config-if)#frame-relay route 201 interface Serial0/0 102

R1(config)# interface s0/2
R1(config-if)#encapsulation frame-relay
R1(config-if)#frame-relay lmi-type ansi
R1(config-if)#frame-relay intf-type dce
R1(config-if)#clock rate 64000
R1(config-if)#frame-relay route 301 interface Serial0/0 103

```

Use the **show frame-relay map** command to display the current map entries for static and dynamic routes

**R0#show frame-relay map**

```

R0#show frame-relay map
Serial0/0 (up): ip 192.168.1.2 dlci 102(0x66,0x1860), dynamic,
                broadcast,, status defined, active
Serial0/0 (up): ip 192.168.1.3 dlci 103(0x67,0x1870), dynamic,
                broadcast,, status defined, active
R0#

```

By default, Cisco uses Inverse ARP to map remote IP address of the PVC with the DLCI of the local interface as we can see here. From the output above we learn that DLCI 102 is set on Serial0/0 of R0 and mapped with 192.168.1.2. The status of this connection is "dynamic" and "active", which means it is operating correctly.

The outputs of this command on other routers are shown below:

```

R2#show frame-relay map
Serial0/0 (up): ip 192.168.1.1 dlci 201(0xC9,0x3090), dynamic,
                broadcast,, status defined, active
R2#

```

```

R3#show frame-relay map
Serial0/0 (up): ip 192.168.1.1 dlci 301(0x12D,0x48D0), dynamic,
                broadcast,, status defined, active
R3#

```

Notice that you will only see the "map" at two ends. If we issue this command on Frame-Relay switch (R1 is this case) it will show nothing.

The **show frame-relay pvc** command is used to display the status of all configured connections, traffic statistics, BECN and FECN packets received by the router.

```

R0#show frame-relay pvc
PVC Statistics for interface Serial0/0 (Frame Relay DTE)

Local          Active      Inactive      Deleted      Static
Switched       2          0             0            0
Unused         0          0             0            0

DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0

  input pkts 2          output pkts 1          in bytes 68
  out bytes 34          dropped pkts 0          in pkts dropped 0
  out pkts dropped 0      out bytes dropped 0
  in FECN pkts 0          in BECN pkts 0          out FECN pkts 0
  out BECN pkts 0          in DE pkts 0            out DE pkts 0
  out bcast pkts 1        out bcast bytes 34
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:04:09, last time pvc status changed 00:03:59

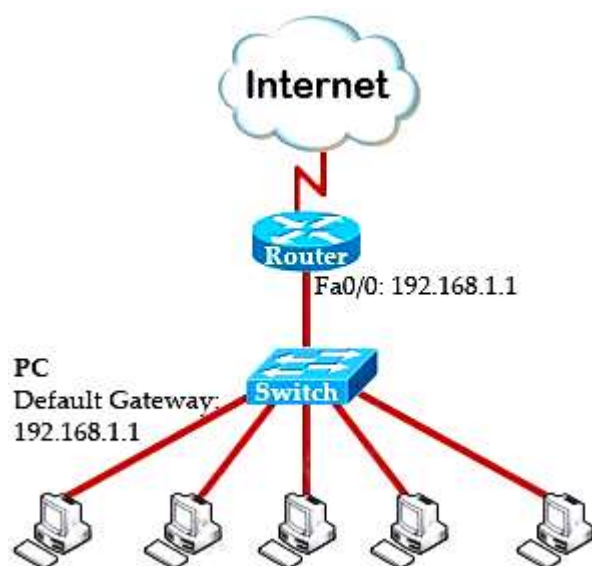
DLCI = 103, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0

  input pkts 1          output pkts 1          in bytes 34
  out bytes 34          dropped pkts 0          in pkts dropped 0
  out pkts dropped 0      out bytes dropped 0
  in FECN pkts 0          in BECN pkts 0          out FECN pkts 0
  out BECN pkts 0          in DE pkts 0            out DE pkts 0
  out bcast pkts 1        out bcast bytes 34
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:04:19, last time pvc status changed 00:04:09
R0#

```

## HSRP, VRRP and GLBP Protocols

Most of the company in the world has a connection to the Internet. The picture below shows a most simple topology of such a company:

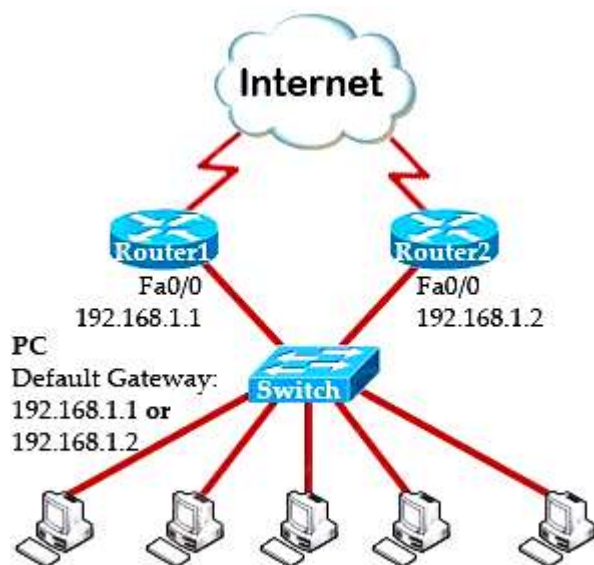




To make above topology work we need to:

- + Configure IP addresses on two interfaces of the Router. Suppose the IP address of Fa0/0 interface (the interface connecting to the switch) is 192.168.1.1.
- + Assign the IP addresses, default gateways and DNS servers on all PCs. In this case we have to set the default gateways to Fa0/0 interface (with the IP address 192.168.1.1) of the router. This can be done manually or automatically via DHCP.

After some time, your boss wants to implement some redundant methods so that even the Router fails, all PCs can still access the Internet without any manual configuration at that time. So we need one more router to connect to the Internet as the topology below:



But now we have a problem: There is only one default gateway on each host, so if Router1 is down and we want to access the Internet via Router2, we have to change the default gateway (to 192.168.1.2). Also, when Router1 comes back we have to manually change back to the IP address on Router1. And no one can access to the Internet in the time of changing the default gateway. HSRP can solve all these problems!

### *Difference between HSRP, VRRP and GLBP Protocols*

PROTOCOL FEATURES	HSRP	VRRP	GLBP
<b>Scope</b>	Cisco Proprietary	IEEE standard	Cisco proprietary
<b>Standard</b>	RFC2281	RFC3768	none
<b>OSI Layer</b>	Layer-3	Layer-3	Layer-2

<b>Load Balancing</b>	No	No	Yes
<b>Multicast Group IP address</b>	224.0.0.2 in version 1 224.0.0.102 in version 2	224.0.0.18	224.0.0.102
<b>Transport Port Number</b>	UDP 1985	UDP 112	UDP 3222
<b>Timers</b>	Hello – 3 sec	Advertisement – 1 sec	Hello – 3sec
	Hold – 10 sec	Master down time = 3*Advertisement Time + Skew TimeSkew Time = (256- Priority)/256	Hold – 10sec
<b>Election</b>	Active Router: 1.Highest Priority 2. Highest IP address (Tiebreaker)	Master Router: (*) 1-Highest Priority 2-Highest IP (Tiebreaker)	Active Virtual Gateway: 1-Highest Priority 2-Highest IP (Tiebreaker)
<b>Router Role</b>	-One Active Router, one Standby Router-one or more listening Routers	- One Active Router-One or More Backup Routers	- One AVG (Active Virtual Gateway)- up to 4 AVF Routers on the group (Active Virtual Forwarder) passing traffic.- up to 1024 virtual Routers (GLBP groups) per physical interface.
<b>Preempt</b>	If Active Router(Highest Priority) is down and up again, Preempt should be configured to become a Active Router again	By default Preempt is ON in VRRP, If Active Router is down and up again, It will automatically become a Master Router	If Active Router(Highest Priority) is down and up again, Preempt should be configured to become a Active Router again.
<b>Group Virtual Mac Address</b>	0000.0c07.acxx	0000.5e00.01xx	0007.b4xx.xxxx
<b>IPV6 SUPPORT</b>	<b>YES</b>	<b>NO</b>	<b>YES</b>

## SYSLOG

**Syslog** is a standard for [computer message logging](#). It permits separation of the software that generates messages from the system that stores them and the software that reports and analyzes them.

Syslog can be used for computer system management and security auditing as well as generalized informational, analysis, and debugging messages. It is supported by a wide variety of devices (like printers and routers) and

receivers across multiple platforms. Because of this, syslog can be used to integrate log data from many different types of systems into a central repository.

Level	Keyword	Description
0	emergencies	System is unusable
1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist
6	informational	Informational messages
7	debugging	Debugging messages

The highest level is level 0 (emergencies). The lowest level is level 7. If you specify a level with the "logging console *level*" command, that level and all the higher levels will be displayed. For example, by using the "logging console warnings" command, all the logging of emergencies, alerts, critical, errors, warnings will be displayed.

## SNMP

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

The SNMP framework has three parts:

- + An SNMP manager
- + An SNMP agent
- + A Management Information Base (MIB)

The SNMP manager is the system used to control and monitor the activities of network hosts using SNMP. The most common managing system is called a Network Management System (NMS). The term NMS can be applied to either a dedicated device used for network management, or the applications used on such a device. A variety of network management applications are available for use with SNMP. These features range from simple command-line applications to feature-rich graphical user interfaces (such as the CiscoWorks2000 line of products).

The SNMP agent is the software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. The agent and MIB reside on the routing device (router, access server, or switch). To enable the SNMP agent on a Cisco routing device, you must define the relationship between the manager and the agent.

The Management Information Base (MIB) is a virtual information storage area for network management information, which consists of collections of managed objects

Cisco IOS software supports the following versions of SNMP:

- + SNMPv1 – The Simple Network Management Protocol: A Full Internet Standard, defined in RFC 1157. (RFC 1157 replaces the earlier versions that were published as RFC 1067 and RFC 1098.) Security is based on community strings.
- + SNMPv2c – The community-string based Administrative Framework for SNMPv2. SNMPv2c (the “c” stands for “community”) is an Experimental Internet Protocol defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 Classic), and uses the community-based security model of SNMPv1.
- + SNMPv3 – Version 3 of SNMP. SNMPv3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are as follows:
  - Message integrity: Ensuring that a packet has not been tampered with in transit.
  - Authentication: Determining that the message is from a valid source.
  - Encryption: Scrambling the contents of a packet prevent it from being learned by an unauthorized source.

## NetFlow

Rapid growth of IP networks has created interest in new business applications and services. These new services have resulted in increases in demand for network bandwidth, performance, and predictable quality of service as well as VoIP, multimedia and security oriented network services. Simultaneously, the need has emerged for measurement technology to support this growth by efficiently providing the information required to record network and application resource utilization. Cisco's IOS NetFlow provides solutions for each of these challenges.

NetFlow traditionally enables several key customer applications including:

- + **Network Monitoring** – NetFlow data enables extensive near real time network monitoring capabilities. Flow-based analysis techniques may be utilized to visualize traffic patterns associated with individual routers and switches as well as on a network-wide basis (providing aggregate traffic or application based views) to provide proactive problem detection, efficient troubleshooting, and rapid problem resolution.
- + **Application Monitoring and Profiling** – NetFlow data enables network managers to gain a detailed, time-based, view of application usage over the network. This information is used to plan,

understand new services, and allocate network and application resources (e.g. Web server sizing and VoIP deployment) to responsively meet customer demands.

+ **User Monitoring and Profiling** – NetFlow data enables network engineers to gain detailed understanding of customer/user utilization of network and application resources. This information may then be utilized to efficiently plan and allocate access, backbone and application resources as well as to detect and resolve potential security and policy violations.

+ **Network Planning** – NetFlow can be used to capture data over a long period of time producing the opportunity to track and anticipate network growth and plan upgrades to increase the number of routing devices, ports, or higher- bandwidth interfaces. NetFlow services data optimizes network planning including peering, backbone upgrade planning, and routing policy planning. NetFlow helps to minimize the total cost of network operations while maximizing network performance, capacity, and reliability. NetFlow detects unwanted WAN traffic, validates bandwidth and Quality of Service (QOS) and allows the analysis of new network applications. NetFlow will give you valuable information to reduce the cost of operating your network.

+ **Security Analysis** – NetFlow identifies and classifies DDOS attacks, viruses and worms in real-time. Changes in network behavior indicate anomalies that are clearly demonstrated in NetFlow data. The data is also a valuable forensic tool to understand and replay the history of security incidents.

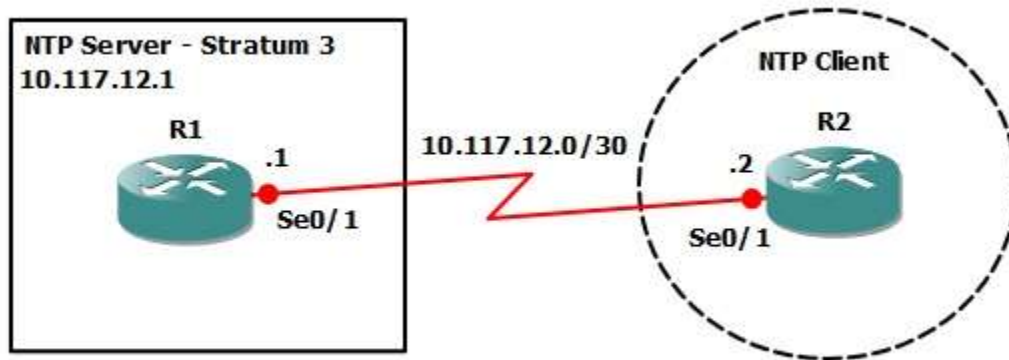
+ **Accounting/Billing** – NetFlow data provides fine-grained metering (e.g. flow data includes details such as IP addresses, packet and byte counts, timestamps, type-of-service and application ports, etc.) for highly flexible and detailed resource utilization accounting. Service providers may utilize the information for billing based on time-of-day, bandwidth usage, application usage, quality of service, etc. Enterprise customers may utilize the information for departmental charge-back or cost allocation for resource utilization

## NTP

Network Time Protocol (NTP) is a vital service not only for Cisco devices but almost every network device. Any computer-based device needs to be accurately synchronised with a reliable time source such as an NTP server.

When it comes to Cisco routers, obtaining the correct time is extremely important because a variety of services depend on it. The logging service shows each log entry with the date and time - very critical if you're trying to track a specific incident or troubleshoot a problem.

Generally, most Cisco routers have two clocks (most people are unaware of this!): a battery-powered hardware clock, referenced as the 'calendar' in the IOS CLI, and a software clock, referenced as the 'clock' in the IOS CLI.



## Lab Instruction

**Objective 1.** – Configure the time and date on R1 as 17:00:00 Jan 1, 2005 to ensure the configured time is different then the actual time to demonstrate NTP.

*R1#clock set 00:00:00 1 jan 2010*

**Objective 2.** – Configure R2 to use the NTP server located at 10.117.12.1.

*R2#configure terminal*

*Enter configuration commands, one per line. End with CNTL/Z.*

*R2(config)#ntp server 10.117.12.1*

*R2(config)#end*

*R2#*

**Objective 3.** – Verity that R2 has obtained the correct time and date from R1 via NTP by viewing the NTP associations and the local clock.

*R2#show ntp associations*

```

address      ref clock   st when poll reach delay offset disp
*~10.117.12.1  127.127.7.1  3  58  64  7   5.1 -0.93 3875.2
* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured

```

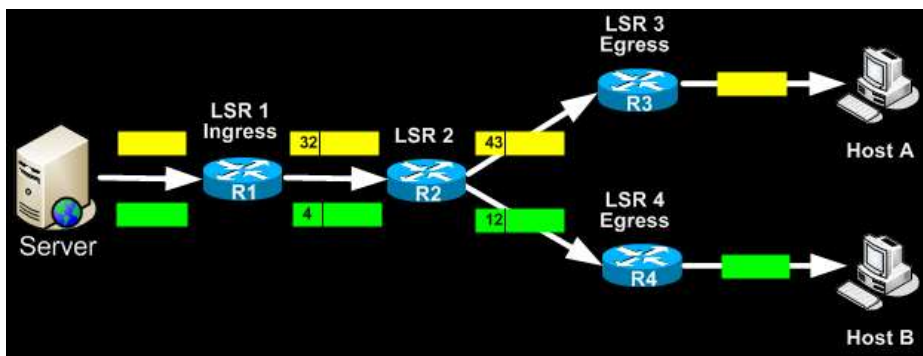
*R2#show clock*

*00:05:18.467 UTC Fri Jan 1 2010*

As shown above by the **show ntp associations** command you'll see that the server 10.117.12.1 is the master (sync'd) server as denoted by the \*. Once viewing the clock you can confirm that the time has indeed been synchronized via NTP.

## WHAT ARE MPLS NETWORKS?

Multi-Protocol Label Switching (MPLS) networks are the next-generation of networks designed to allow customers create end-to-end circuits across any type of transport medium using any available WAN technology. Until recent years, customers with the need to connect remote offices in locations across the country were restricted to the limited WAN options service providers offered, usually Frame Relay or T1/E1 dedicated links. The problem with these WAN technologies is that they are usually very expensive and complex to manage, but also not very flexible, making them a headache for both the end customer and service provider. Worst of all, as the distance between the customer's end points increased, so did the monthly bill.



### HOW MPLS NETWORKS WORK

MPLS works by tagging the traffic entering the MPLS network. An identifier (label) is used to help distinguish

the Label Switched Path (LSP) to be used to route the packet to its correct destination. Once the best LSP is identified by the router, the packet is forwarded to the next-hop router. A different label is used for every hop and the label is selected by the router (or switch) that is performing the forwarding operation.

Take for example the below diagram. It shows a simple MPLS network example where the central server is sending packets to two remote hosts.

The Ingress router (LSR1) accepts the packets from the server and selects the best LSP based on their destination IP Address. It then selects an initial label (local significance) for each packet and then forwards the packets using MPLS. When Router2 receives the packets, it uses these labels to identify the LSPs from which it selects the next hops (R3 & R4) and labels (43 & 12). At the end of the path, the egress routers (R3 & R4) remove the final label and send the packet out to the local network.

One of the great advantages offered by MPLS networks is the built-in Quality of Service mechanisms. MPLS service providers usually offer an end-to-end QoS policy to ensure their

customer MPLS networks have guaranteed QoS through the MPLS network backbone. This allows delay-sensitive services such as VoIP to be implemented with guaranteed bandwidth between the endpoints.

There really is no limitation to the type of services that can be run over a MPLS network. The QoS mechanisms and prioritisation services, allow the quick and effective forwarding of traffic between customer endpoints.

## MPLS VPN BASICS

MPLS VPNs combine the power of MPLS and the Border Gateway Protocol (BGP) routing protocol. MPLS is used to forward packets over the provider's network backbone and BGP is used for distributing routes over the backbone.

A MPLS VPN is compromised of the following equipment:

**Customer Edge (CE) routers.** These are placed at the customer site and are usually owned by the customer. Some service providers also supply the CE equipment for a small rental fee.

**Provider Edge (PE) routers.** These are the provider's edge routers to which the CE routers connect to. The PE routers are always owned by the service provider

**Provider (P) routers.** These routers are commonly referred to as 'transit routers' and are located in the service provider's core network