NETWORK KINGS®

CCNA VERSION 2

www.nwkings.com

Atul Sharma

Network Specialist

10 years of Industry experience with implementation and support of network technologies. A highly experienced and talented Network Specialist, with expertise in Troubleshooting and Optimising Networks, coupled with extensive knowledge of Service Provider Network & LAN. "Worked with Apple, Juniper Networks, TCS & Aricent." 10 years of Industry experience with implementation and support of network technologies. A highly experienced and talented Network Specialist, with expertise in Troubleshooting and Optimising Networks, coupled with extensive knowledge of Service Provider Network & LAN. "Worked with Apple, Juniper Networks, TCS & Aricent.” Juniper Networks, TCS & Aricent." 10 years of Industry experience with implementation and support of network technologies. A highly experienced and talented Network Specialist, with expertise in Troubleshooting and Optimising Networks, coupled with extensive knowledge of Service Provider Network & LAN. "Worked with Apple, Juniper Networks, TCS & Aricent.”

CCNA

Cisco Certified Network Associate

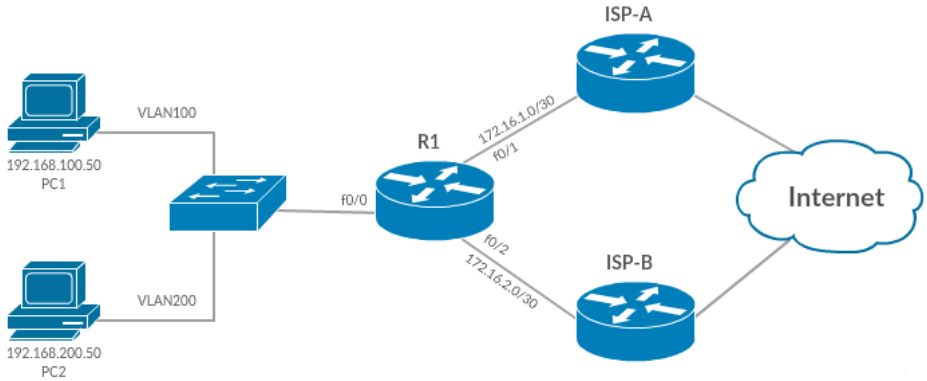
Congratulations! you've probably already decided to go for your Cisco certification. If you want to succeed as a technical person in the networking industry, you need to know Cisco. Cisco has a ridiculously high market share in the router and switch marketplace, with more than an 80 percent share in some markets. In many geographies and markets around the world, networking equals Cisco. If you want to be taken seriously as a network engineer, Cisco certification makes perfect sense.

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 .

Important Websites:
Video Lessons : www.nwkings.com

Official Website: www.networkkings.org
Download packet tracer
Register in netcad account : https://goo.gl/pWbLFU

Gns3 (First make account and download)
https://www.gns3.com/software



Basics of Networking

What is a network?
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 two computers at your home sharing files and a printer between connected devices is called as networking.

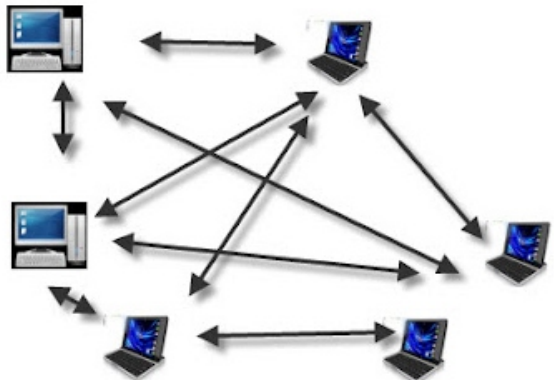
Some of the components that make up a network:
Personal Computers (PC): These are the endpoints of your network, sending and receiving data. Interconnections: These are components that make sure data can travel from one device to another, you need to think about:

Network Interface Card (NIC):
NIC stands for Network Interface Card. It is a small circuit board (chip) on the motherboard of PC. NIC connects a computer to the internet. On NIC, there is a RJ-45 port. NIC has a MAC address (physical address) that is assigned by manufacturer.

Media Cables and connectors : network cables, perhaps wireless,

Connectors: the plug you plug in your network card , RJ 45 is commond for ethernet cable , RJ 11 connector for landline telephones.

What is a host?
A host can be a computer, a laptop, a mobile, an internet printer or any other device that uses IP address to go to the internet.



What is a topology?

Topology simply defines how hosts are connected in a particular network.
There are many different topologies- star topology, ring topology, bus topology, mesh topology and hybrid topology (mixture of all).
In modern networks star, mesh and
hybrid topologies are most commonly used.

The Difference Between Unicast, Multicast and Broadcast Messages

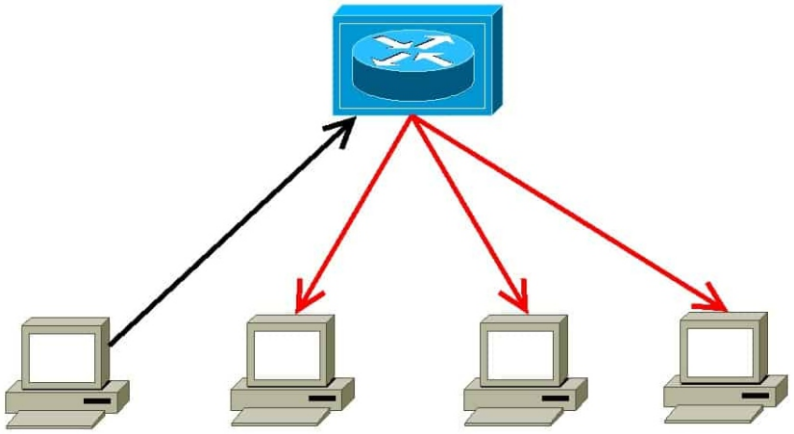
Unicast: Unicast means message is sent to only one host. In unicast mode, there is one sender and one receiver.

Multicast: Multicast term is used when there is 1 sender and 2 or more than two receivers. Multicast is also known as one-to-many.

Broadcast: Broadcast means one-to-all. We use term broadcast when 1 sender sends information to all other hosts which are present in the network.

Network Devices :
Routers: Routers interconnect networks and choose the best path to each network Destination, router makes its routing table for best path.

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



What is hub?

Hub is a LAN device. It works on layer 1 (physical layer). Hub is used in LAN network to connect host together. Now hubs are completely obsolete from the market. There are two main reasons behind this-

1. Hub had less number of ports. As, the network size is increasing day by day, we need to connect more devices in a LAN, so we need a device that has large number of ports.

2. Hub was a dummy device; simply broadcast the frame, more likely repeater.

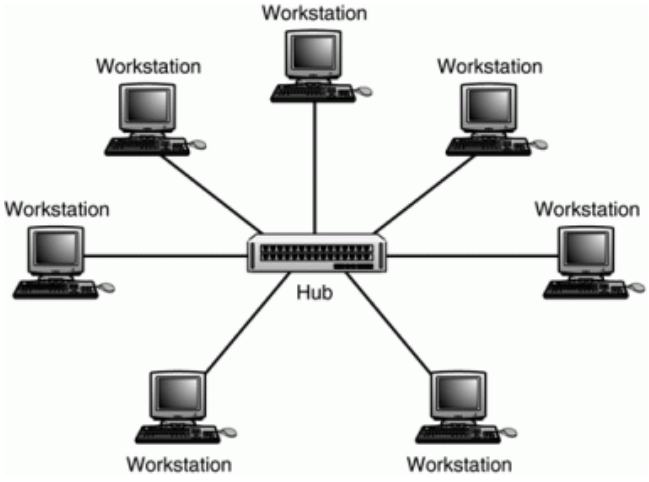
What is bridge?

Bridge is a network hardware device that used to connect the hubs together.

What is Switch?

Switch is a layer 2 device (data link layer). Switch is the advanced version of hub, so sometime called as intelligent hub. Switch is used to connect hosts in the LAN network. The basic function of a switch is to forward the frame. Switches maintain an ARP table that contains MAC address and port number. So, unlike hub switch doesn't broadcast every time, it receives the frame then check the table and then forward the frame. Switch broadcast the frame only when ARP table is blank. Now days, multi-switches are also available in the market. Multi-switch works on both layer 2 and layer 3. You can use multi-switch as a router as well as a layer 2 switch.

Vendors: Cisco, Juniper Networks, Huawei, HP, Dlink, tplink.



HUB

- Known as Dummy Device.
- 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 :-
  1. Manageble switch
  2. Unmanageable switch
- Its is a Layer 2 Device

What is Gateway?

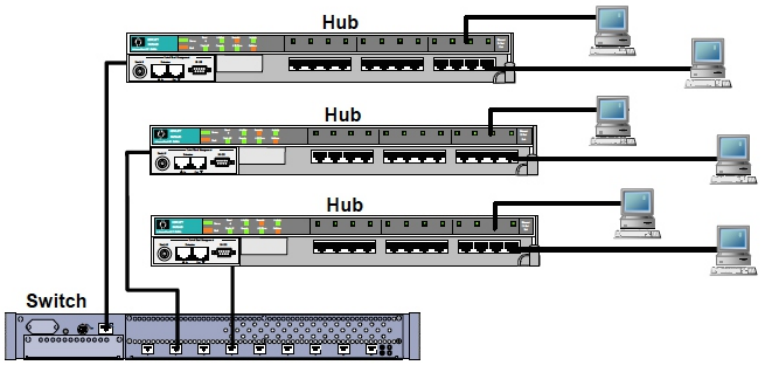
Gateway is the entrance/exit point of a LAN network. Gateway is basically a router. Like in our home, there is a main gate through which we enter/exit. Similar way, gateway is that router through which outside traffic comes inside the LAN network and inside traffic goes outside the network.

What is modem?

Modem stands for modulation and demodulation. Modem performs both modulations as well as demodulation depends on the requirement. At receiver side, it performs demodulation, convert analog signal (electrical signal) into binary form (10011011000011). At sender side, it performs modulation and converts digital signal into analog signal, just opposite of demodulation.

What is a repeater?

Repeater is a layer 1 device. Repeater is used to reproduce the original strength of the signal. For example, when a signal travels a long distance, signal strength fades away. In that situation we need a repeater in the midway to recover the original signal strength.



What is Access point(AP)?

In traditional networks, our LAN network is wired one. I mean all devices are connected together through wired connection. But, now the scenario is different, LAN networks have both type of hosts wired host and wireless host. To connect wireless devices to wired network, we use access points.

In other words, we can say access points are used to merge wireless network into existing wired network to achieve proper utilisation of resources. Sometimes APs are used to extend the signal range (works as range-extender).

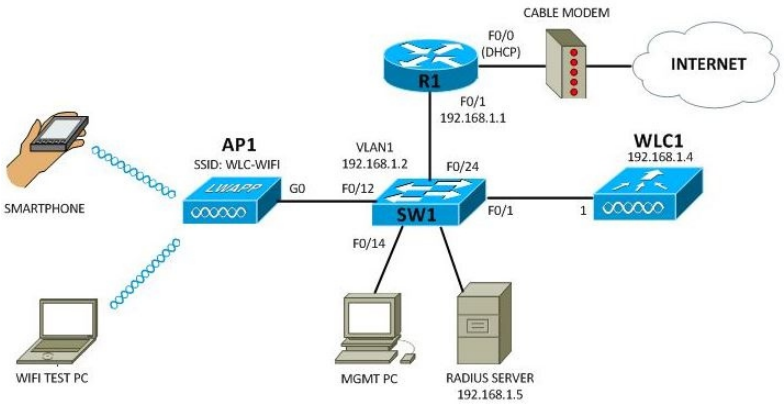
What is WLC?

WLC stands for wireless link controller. It is used to manage the Access points.

Some Cmd commands for CCNA !

1. ping :- packet internet gopher
it works on ICMP protocol
For verification the other device is reachble to me or not ??

2. ipconfig :- to check the ip address of a computer
3. ipconfig /all :- to check the ip address + mac address
4. getmac :- to check the mac address of a computer
5. netstat :- to check the session's
6. nslookup :- to check the all servers of a website
7. arp -a :- to check arp table
8. arp –d :- to delete arp table (run as administrator)
9. To check public ip
Visit :- www.whatismyipaddress.com to check your public ip



How 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
4.Assign Ip address

MAC Address vs IP Address

- 48 bit MAC address

-Layer 2
-Used to get packet from one interface to another within the same LAN/subnet (Ethernet, token ring...)
-Flat
-Unique
- No change when moving

- 32-bit IP address

-Network layer
-Used to get packet to destination IP subnet
- Hierarchical
- Change when moving

- Depeing on IP subnet to which node is attached

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.

Ethernet Frame

IPv4 Addressing
IP Header: Explanation
Version: This field tells the IP version – IPv4 or Ipv6.

Header Length: This field tells the header length. Most of time, you will see header length is 5. Here, 5 is representing total number of rows in header. If this value is 6, options field is also present in the header, but this will be very rare.

Type of Service (TOS): This is 8 bits field. This TOS field is used to prioritize the traffic. For example, In a company there is an important meeting is going on, so we don't want any interruption in the meeting, so in this case we set higher priority by using TOS.

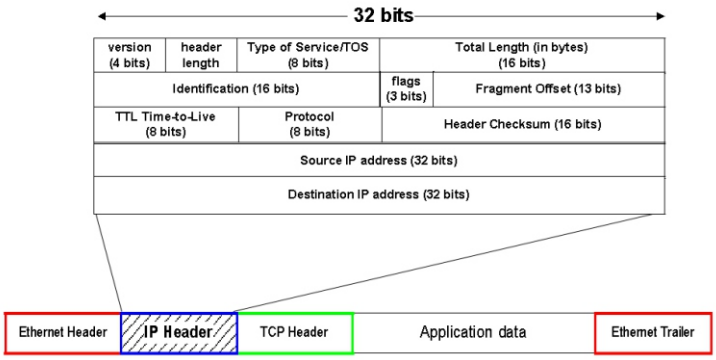
Total Length: Total length represents the length of header and data both.
Total length = Data + IP header

Identification Field: When a packet is large, normally packet is divided into parts before sending, these parts is known as fragment. To collect these fragments at receiver side, an identification field is added. Fragments that belong to same packet have same identification value.

Flags: This field has 3 bits; combination of these 3 bits represent 3 different actions. Mainly different combinations of flags tell packet is fragmented or not.

0	000	Resend
1	001	No Fragmentation
2	010	Fragmentation

Mainly, packets are fragmented when size is greater than 1500bytes (header+data). Because Maximum Transmission Unit (MTU) = 1500 bytes.



Fragment Offset: This field is used to indicate the position of the fragments in the packet. It tells the sequence number in which fragments are arranged to reassemble the original packet.
Fragment offset value is very useful in recollecting the fragments at receiver side, because many times fragments are appeared in random manner.

Time to Live: By default, TTL value is 64. A user can set it manually up to 255. TTL value is used to avoid layer 3 infinite loops, when TTL = 0 (zero), packet is dropped. TTL value is decremented as it traverses the router in the path. For example- let suppose initial TTL value is 64. To reach to a destination, there are 4 routers in the path, so TTL value is decremented by 1 every time, as it will pass the router, and in last TTL value will be 60. You can also calculate Hop counts by using TTL value.
Hop counts = Initial TTL- final TTL

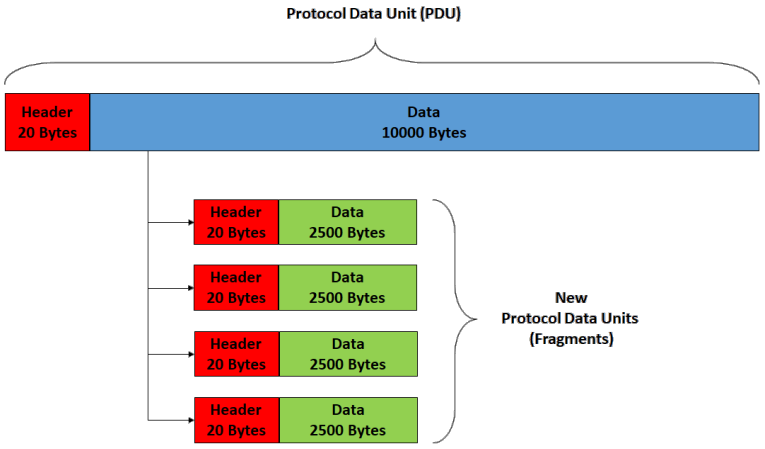
Protocol Number: This field represents the protocol number.

Header Checksum: This is responsible for checking errors, it only checks the header error, if any error is present in the header, it drops the packet.

Source IP address: This field represents the IP address of sender. This is 32 bits field.

Destination IP address: This field represents the IP address of destination. This is also 32 bits field.

Note: Source IP and destination IP address field never change, these remain same, doesn't matter where you check.



What is the size of IP header?

It is very simple to calculate. Just look at the IP header once, now notice each row is 32 bits in length and there are total 5 rows. So, 5×32 = 160 bits.

As, we know 1 byte = 8 bits, so 160 ÷ 8 = 20 bytes.

So, IP header size is 20 bytes (160 bits).

IP Addressing

• IP Address is Logical Address. It is a Network Layer address (Layer 3), IPv4 addresses are 32-bit numbers that are typically displayed in dotted decimal notation. A 32-bit address contains two primary parts: the network prefix and the host number.

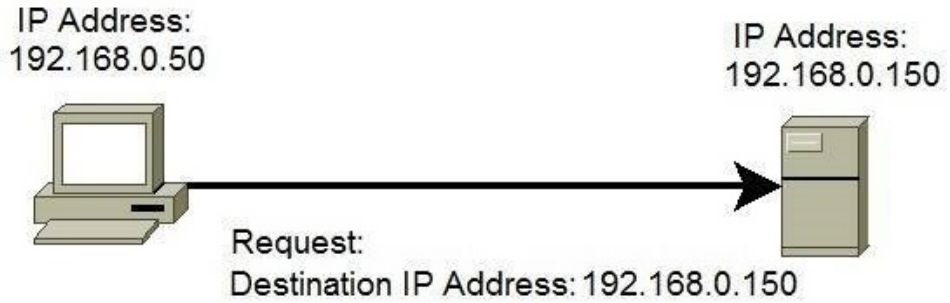
· All hosts within a single network share the same network address. Each host also has an address that uniquely identifies it. Depending on the scope of the network and the type of device, the address is either globally or locally unique

· IP addresses are assigned by a central numbering authority called the Internet Assigned Numbers Authority (IANA).

2 Types of IP Address

1. IPv4 address (32 bits address)
2. IPv6 Address (128 bits address)

Note: Here v stands for version. So, we can expand like that IP version 4 and IP version 6.



How I can check IP address of my computer (for windows)?

1st method

1. Go to the desktop, now type cmd in the window search bar and hit enter button.
2. After that command prompt screen will be open.
3. Look carefully, there will be a cursor blinking, now just type ipconfig and hit enter.

2nd method

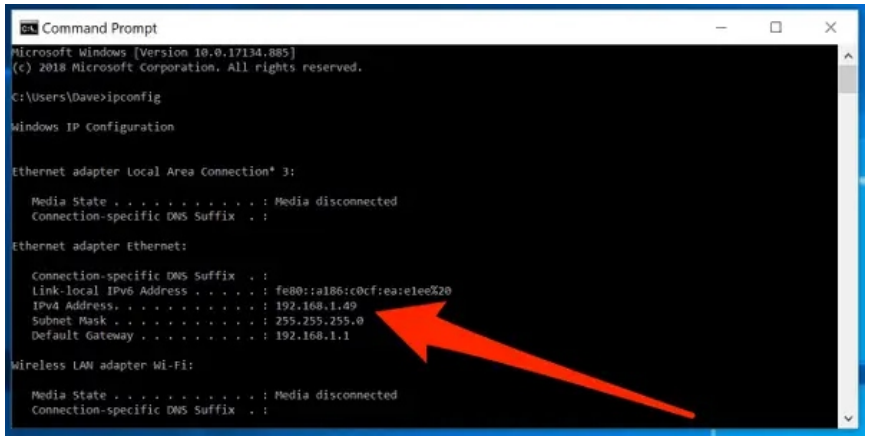
1. Go to the desktop, now type “ncpa.cpl” in the window search bar and hit enter.
2. Now a dialog box will appear on your screen to shows network connection.
3. Click on the network from which you are connected, then a dialog box will appear.
4. In this dialog box, there is a detail option, click on that.
5. Now you able to see the IP address of your computer.

What are the classes of IPv4 Addresses?

IPv4 Addresses are divided into 5 Classes, These are divided by IANA :- Internet Assigned Number authority.

1. Class A (1-126)
2. Class B (128-191)
3. Class C (192-223)
4. Class D (224-240)
5. Class E (241-239)

Class	First Octe	First Octet Rang	Prefix length	Subnet Mask	Network Bit	Host Bits
A	0XXXXXXX	0-127 (1126)	/8	225.0.0.0	8	24
B	10XXXXXX	128191	/16	255.255.0.0	16	16
C	110XXXXX	192223	/24	255.255.255.	24	8
D	1110XXXX	224239				
E	1111XXXX	240255				



How to recognize the IP address class?

By looking at the first octet, you can recognize the class of an IP address.

For Class A: The first octet in binary form is 0XXXXXXX. First bit of class A always will be zero. Here X could be a zero or one (not fixed).

In decimal notation, first octet always will be lies in the range of 1 - 126. And rest lie in the range of 0-255.

For Class B: The first binary octet is 10xxxxxx. So, you can see for Class B first 2 bits of first octet always will be 10.

Decimal Octet range: 128-191

For Class C: First binary octet always will be 110xxxxx.

Decimal Octet range is 192-223.

For Class D: First binary octet always will be 1110xxxx.

For Class E: First binary octet always will be 1111xxxx.

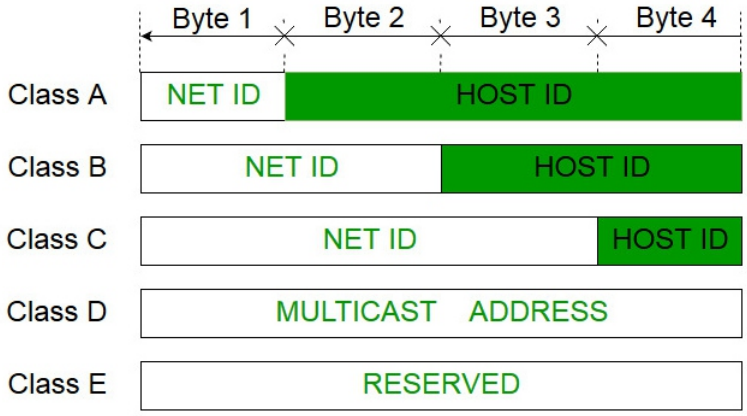
Although, Class D and Class E address will not used in configuration.

What is APIPA Address?

APIPA stands for Automatically Private IP Address Assignment. When DHCP server fails, automatically an IP address is generated and this address is called as APIPA address. APIPA assigns a class B address, range from 169.254.0.0 to 169.254.255.255.

Static IP: Static IP is not a type of IP, it's a terminology. When an IP address is manually configured in a host then it is called as static IP.

Dynamic IP: When an IP address is configured through DHCP then it is called as dynamic IP.



Private IP Address : Private IP are used inside the LAN network only. Sometime also known as LAN addresses. Private IP is uniquely defined in a LAN network. It means inside a LAN network, you can't assign same IP to 2 different host. Although, you can assign same IP address in 2 different LAN networks. There are certain addresses in each class that are reserved for Private Networks.

Class	**A10.0.0.0**	**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**

Public IP address: Public IP is provided by internet service provider (ISP). Public IP is globally unique. A host without public IP can't go to the internet. So, whenever a host sitting in our LAN network, want to go on internet, first router performs NAT to convert private into public IP then it forwards the request to the internet.

Subnet Mask: It is an address used to identify the network and host portion of the ip address.

Class A	**N.H.H.H**	**255.0.0.0**
Class B	**N.N.H.H**	**255.255.0.0**
Class C	**N.N.N.H**	**255.255.255.0**

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

How to Calculate Subnet Mask?
It is a very easy process, once you will learn the method then you will calculate for any prefix length.
Replace all the network bits by 1 and all the host bits by 0.

PRIVATE IP	PUBLIC IP
• Used with the LAN or within the organization • Not recognized on internet • Given by the administrator • Unique within the network or organization • Free • Unregistered IP	• Used on public network (INTERNET) • Recognized on internet • Given by the service provider (from IANA) • Globally unique • Pay to service provider (or IANA) • • Registered

Now we will do 1 problem to understand this in more clear way-

1. 192.168.1.0/24 – (Class C address with prefix length 24. As I told you earlier prefix length represents network bits. So, here we have 24 network bits and 8 host bits.)

2. First perform binary to decimal conversion.

192 . 168 . 1 . 0

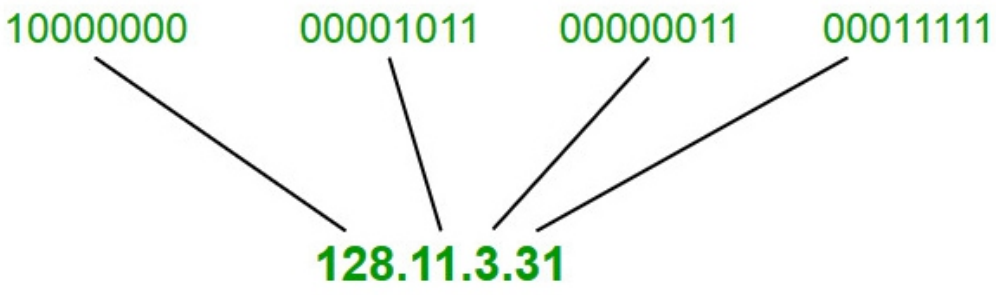
11000000.10100000.00000001.00000000

3. Now replace all network bits by 1 and all host bit by 0.

11111111.11111111.11111111.00000000

4. Now again perform binary to decimal conversion and here we have

255.255.255.0



Subnetting

Subnetting:

It is the process of dividing a Single Network into Multiple Networks. A subnet or subnetwork is a part of larger network.

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 >= requirement**

Requirement of Networks ? **2^n >= requirement**

What is Supernetting or CIDR?

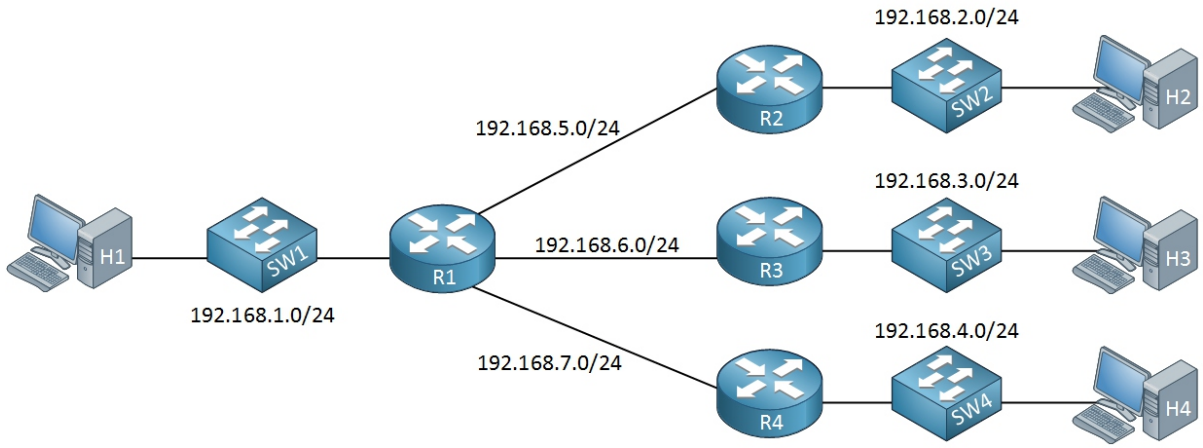
Classless Inter-Domain Routing (CIDR) merges or combines network addresses of same class into one single address to reduce the size of the routing table.

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

It is implemented by ISP (internet service providers).

How to calculate available addresses and usable addresses?

This is very simple and easy calculation. To find out the total number of available addresses, first find how many host bits are there? Then use below formula to calculate total addresses



For example: Class A has 24 host bits, so total no. of available addresses = 2^{24}

Class B has 16 host bits, so total no. of available addresses = 2^{16}

Class C has 8 host bits, so total no. of available addresses = 2^{8}

Total Number of usable addresses =$2^{hostbits}$ - 2

From total addresses we subtract 2 because first address is used as network address and last address is used as broadcast address, we can't assign these two addresses to devices.

How to calculate number of subnets?

Number of subnets = 2^{x}

where x =number of borrowing bits

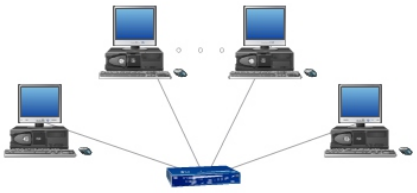
Que: How many subnets are available with the network 172.16.0.0/26?

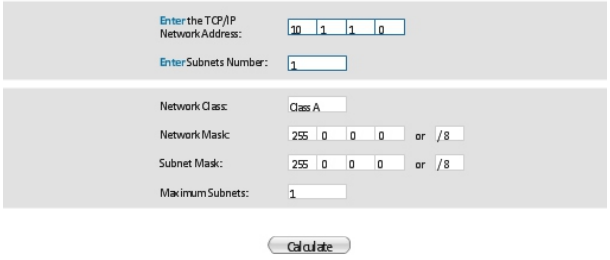
Sol. Given Address belong to class B. and for class B prefix length is 16.

But, given prefix length is 26.

So, borrowed host bits = 26-16 = 10

Now, 2^{10} =1024 subnets





Que: How many subnets are available with the network 172.16.0.0/26?

Sol. Given Address belong to class B. and for class B prefix length is 16.

But, given prefix length is 26.

So, borrowed host bits = 26-16 = 10

Now, 2^{10} =1024 subnets

Type-1. Find the subnet ID

Que-1.Which subnet does host 172.16.26.127/21 belong to?

Steps to find out the subnet ID

1. Perform decimal to binary conversion.

2. Then, convert all host bits to zero.

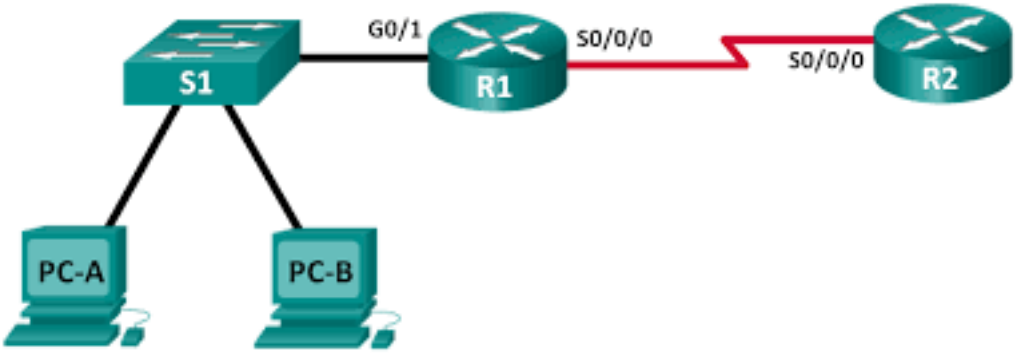
3. Now again perform the decimal conversion.

First Method:

Solution: Prefix length is 21, it means 21 network bits and rest 11 are host bits.

Step-1: 172. 16. 26. 127 (decimal Form of IP address)

10101100. 00010000. 00011010. 01111111



Step-2: Put network bits as it is and convert all host bits to zero.

10101100. 00010000. 00011000. 00000000

Step-3: Now perform binary to decimal conversion. First two octets are same put them as they are.

172. 16. 24. 0/21 is the subnet Id.

Second Method:

Sol. Here, prefix length is 21 and total bits are 32 in IPv4, so host bits are 32-21= 11

Decimal form of IP 172.16.26.127, no need to convert all 4 octets to binary form.

As you can see host bits are only 11 that lie in last 2 octets (26.127).

All bits of last octet are host bits, so you can simply put it zero without any conversion.

Now you have to only convert the third octet (26) in binary form.

Decimal form 26

Binary form 00011010, (first five bits are network bits and last 3 bits are host bits).

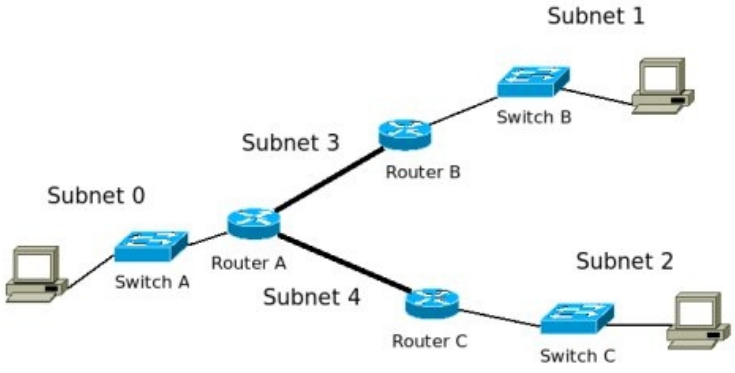
Now convert host bits to zero.

Binary form: 00011000

Equivalent decimal form: 24

Now subnet id is 172.16.24.0/21

I solve this question by using two methods. To apply second method, you need to do lot of practice. Steps are same in both methods only unnecessary conversion is eliminated.



Que2. What subnet does host 192.168.5.57/27 belongs to?

Solution: Here, prefix length is 27 (network bits), rest 5 are host bits.

Step1: Perform decimal to binary conversion

192. 168. 5. 57

11000000. 10101000. 00000010. 00111001 (first 27 bits are network bits and last 5 bits are host bits).

Step2: Put network bits as they are and convert all host bits to zero.

11000000. 10101000. 00000010. 00100000

Step-3: Now perform binary to decimal conversion.

There is no changes in first three octets, put them as they are initially in decimal form.

192.168.5.32 is the subnet Id.

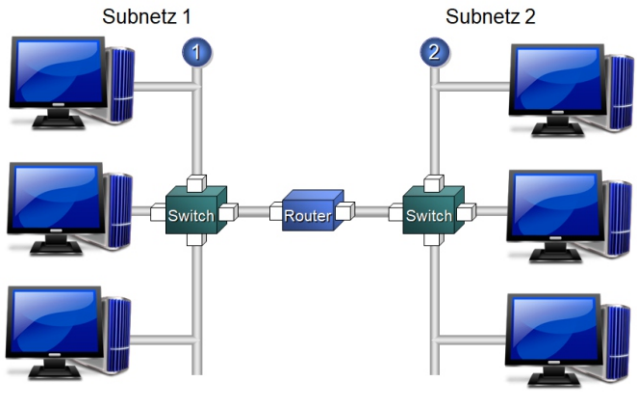
Que3. What subnet does host 192.168.29.219/29 belongs to?

Solution: Here, prefix length is 29 (network bits), rest 3 are host bits.

Step1: Perform decimal to binary conversion

192. 168. 29. 219

11000000. 10101000. 00011101. 11011011 (first 29 bits are network bits and last 3 bits are host bits).



Step2: Put network bits as it is and convert all host bits to zero.

11000000. 10101000. 00011101. 11011000

Step-3: Now perform binary to decimal conversion.

There is no changes in first three octets, put them as they are initially in decimal form.

192.168.29.216/29 is the subnet Id.

Que4: What subnet does host 172.21.111.201/20 belongs to?

Solution: Here, prefix length is 20 (network bits), rest 12 are host bits.

Step1: Perform decimal to binary conversion

172. 21. 111. 201

10101100. 00010101. 01101111. 11001001 (first 20 bits are network bits and last 12 bits are host bits)

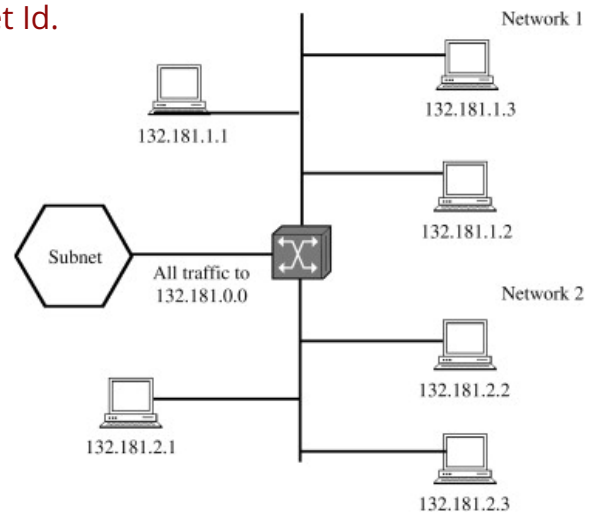
Step2: Put network bits as it is and convert all host bits to zero.

10101100. 00010101. 01100000. 00000000

Step-3: Now perform binary to decimal conversion.

There is no changes in first two octets, put them as they are initially in decimal form.

172.21.96.0/20 is the subnet Id.



Type-2 Find the prefix length

Que1. You have been given the 172.16.0.0/16 network. You are asked to create 80 subnets for your company's various LANs. What prefix length should you use?

Solution: Total no. of subnets = 2^x

80 = 2^x

2^6 = 64 and 2^7 = 128 (64 is less than 80 so, here x = 7, borrowed bits from host bits).
Hence, prefix length = network bits + borrowed host bits

= 16 + 7, prefix length = 23

Que2. You have been given the 172.18.0.0/16 network. Your company requires 250 subnets with the same number of hosts per subnet. What prefix length you should use?

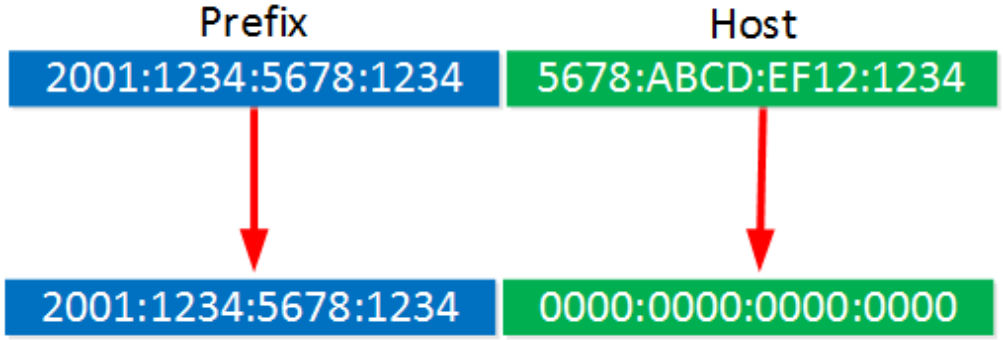
Solution: Total no. of subnets = 2^x

250 = 2^x

2^7 = 128 and 2^8 = 256 (128 is less than 250 so, here x = 8, borrowed bits from host bits).
Hence, prefix length = network bits + borrowed host bits

Total number of available addresses = $2^{hostbits}$

= 16 + 8prefix length = 24



How to calculate network address and broadcast address?

To find the network address, all host bits are converted into 0 (zero).
To find the broadcast address, all host bits are converted into 1 (one).

Que1. PC1 has an IP address of 10.217.182.223/11. Find out-

1. Network address
2. Broadcast address
3. First usable address
4. Last usable address
5. Number of host addresses

Solution: 1. First perform decimal to binary conversion

Decimal form of IP: 10 .217 .182 .223

Binary form: 00001010 .11011001 .10110110 .11011111

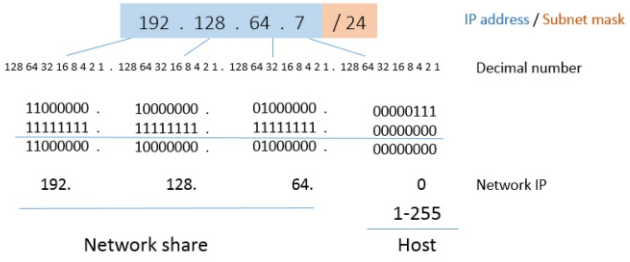
Now to find the network address convert all host bits into 0 (zero). As given IP has prefix length 11. It means 11 network bits and remaining (32-11 = 21) bits are host bits.

00001010 .11000000 .00000000 . 00000000

Now again perform binary to decimal conversion

10 .192 .0 .0

Network address = 10.192.0.0/11



2. To find broadcast address convert all host bits to 1 (one).

Decimal form of IP: 10 .217 .182 .223

Binary form: 00001010 .11011001 .10110110 .11011111

Convert all host bits to 1

00001010 .11011111 .11111111 .11111111

Now perform binary to decimal conversion:

10 .223 .255 .255Broadcast address = 10.223.255.255/11

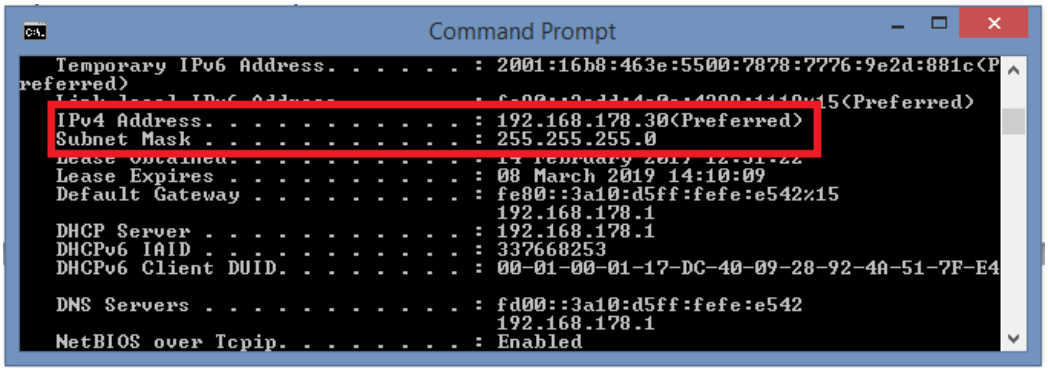
3. Find First usable address: The first address after the network address is known as first usable address.

Network address = 10.192.0.0/11

So, first usable address is 10.192.0.1/11

4. Find last usable address: The address just before the the broadcast address is known as last usable address.

Broadcast address = 10.223.255.255/11
So, last usable address is 10.223.255.254/11



5. Total Number of host addresses = $2^{hostbits}$

Here, host bits are 21

So, total host addresses are = 2^{21}

Que- Represent /24 in decimal dotted form (subnet mask). Or what will be decimal dotted representation of /24?

Sometime this type of questions are directly asked by interviewer. I remember recently I gave 1 interview in which interviewer asked what will be the decimal dotted representation of /28?

So, now the thing is how to solve this type of question? Let me explain this.For /24, many of you know the decimal dotted representation. But here I will tell you the step-by-step procedure, so that you can calculate subnet mask(decimal dotted representation) for any prefix length.

In IPv4, total bits are 32. **/ value** represent number of network bits. So, in /24, we have 24 network bits and 8 host bits.

To calculate decimal dotted form, assign 1 (one) to all network bits and 0 (zero) to all host bits.

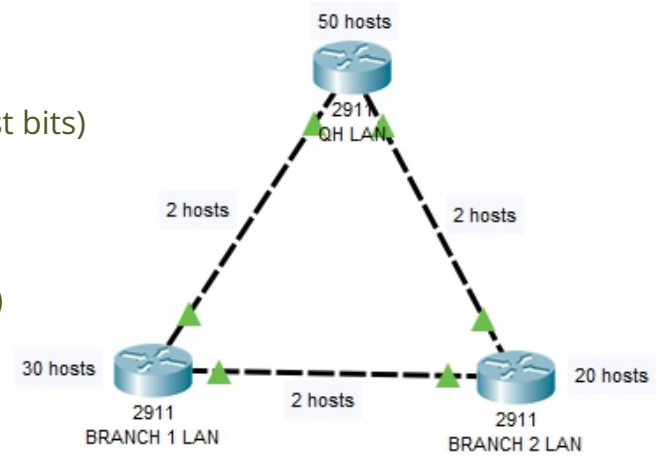
For /24

11111111. 11111111. 11111111. 11110000
255.255.255.0 (decimal dotted form).

For /28 (28 network bits and remaining 4 are host bits)

11111111. 11111111. 11111111. 11110000

255.255.255.240 (Decimal dotted representation)



Prefix Value (/ value)	Network bits	Host bits	Binary form (assign 1 to network bits and 0 to host b	Decimal dotted representation (subnet mask)
/24	24	8	11111111. 11111111. 11111111. 00000000	255.255.255.0
/25	25	7	11111111. 11111111. 11111111. 10000000	255.255.255.128
/26	26	6	11111111. 11111111. 11111111. 11000000	255.255.255.192
/27	27	5	11111111. 11111111. 11111111.11100000	255.255.255.224
/28	28	4	11111111. 11111111. 11111111. 11110000	255.255.255.240
/29	29	3	11111111. 11111111. 11111111. 11111000	255.255.255.248
/30	30	2	11111111. 11111111. 11111111. 11111100	255.255.255.252
/31	31	1	11111111. 11111111. 11111111. 11111110	255.255.255.254
/32	32	0	11111111. 11111111. 11111111. 11111111	255.255.255.255

$2^1 = 2$	$2^{10} = 1024$
$2^2 = 4$	$2^{11} = 2048$
$2^3 = 8$	$2^{12} = 4096$
$2^4 = 16$	$2^{13} = 8192$
$2^5 = 32$	$2^{14} = 16384$
$2^6 = 64$	$2^{15} = 32768$
$2^7 = 128$	$2^{16} = 65536$
$2^8 = 256$	$2^{17} = 131072$
$2^9 = 512$	

FLSM : Example-- 1

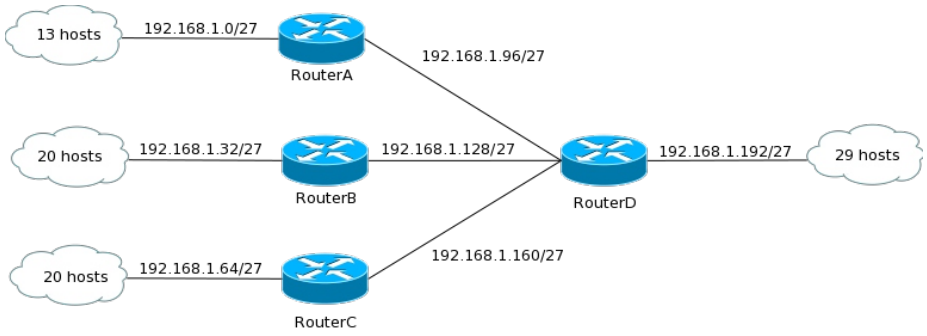
Req = 40 hosts using C-class address network 192.168.1.0/24

1. $2^h - 2 >= req$
   $2^6 - 2 >= 40$
   $64 - 2 >= 40$
   $62 >= 40$

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

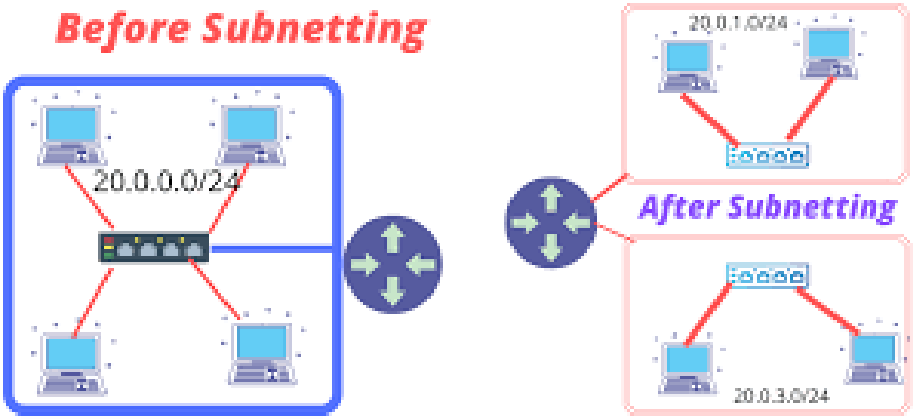
FLSM : Example-- 2

1.Req = 500 hosts using B-class address network 172.16.0.0/16
2^h - 2 >= req
2^9 – 2 >= 500
512 – 2 >= 500
510 >= 500

2.Host bits required **(h)= 9**
3. **Converted network Bits** (n) = Total. H. Bits -- req. H. Bits
= 16 --- 9 = **7 (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 >= req

2^{11} – 2 >= 2000

2048 – 2 >= 2000

2046 >= 2000

2.Host bits required (h)= 11

3.Converted network Bits (n) = Total. H. Bits -- req. H. Bits

= 24 --- 11 = **13 (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 = 2n = 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

...

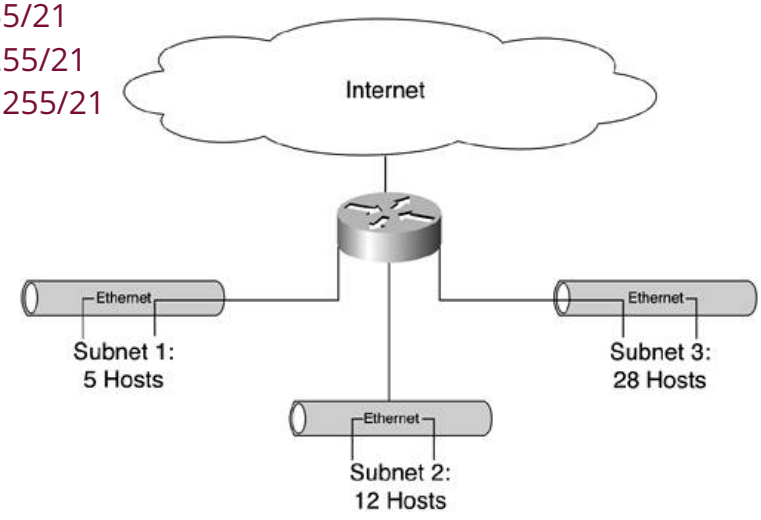
...

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

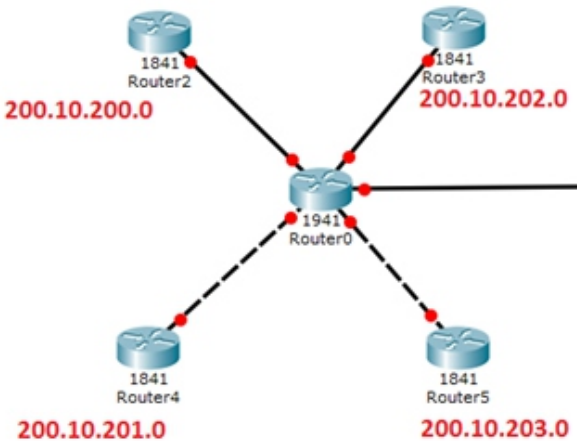
10.255.8.0/21 --- 10.0.15.255/21

10.255.16.0/21 --- 10.0.23.255/21

....

...

10.255.248.0/21 ... 10.255.255.255/21



Network ID	Subnet Mask	Interface
200.10.200.0	255.255.255.0	a
200.10.201.0	255.255.255.0	a
200.10.202.0	255.255.255.0	a
200.10.203.0	255.255.255.0	a

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.

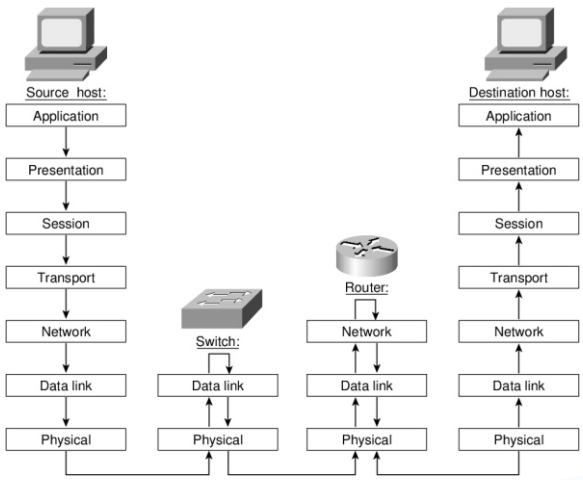
All People Seem To Need Data Processing
Physical Layer: This layer describes stuff like voltage levels, timing, physical data rates, physical connectors and so on. Everything you can “touch” since it’s physical.

Total number of available addresses = $2^{hostbits}$
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.

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.

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.

- TCP lives here; it’s a protocol which send data in a reliable way.
- 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.



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.

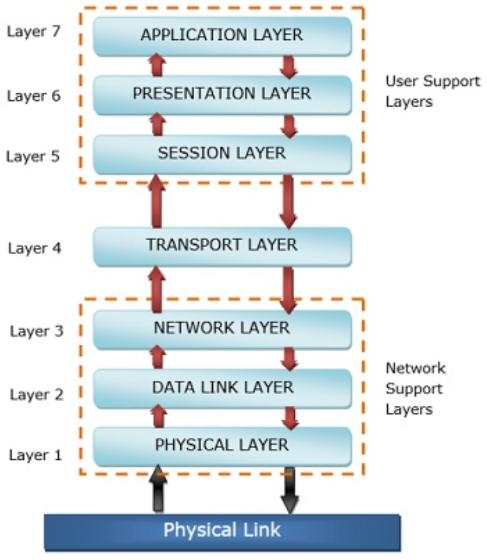
Port Numbers

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[1]	DNS
67	UDP	DHCP Server
68	UDP	DHCP Client
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
514	UDP	Syslog

[1] DNS uses both UDP and TCP in different instances. It uses port 53 for both TCP and UDP.



The major functions described at the Transport Layer are..

- 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

Transmission Control Protocol	User Datagram Protocol
• Connection Oriented • Reliable communication(with Ack's) • Slower data Transportation • Protocol No is 6 • Eg: HTTP, FTP, SMTP	• Connection Less • Unreliable communication (no Ack's) • Faster data Transportation • Protocol No is 17 • Eg: DNS, D HCP, TFTP

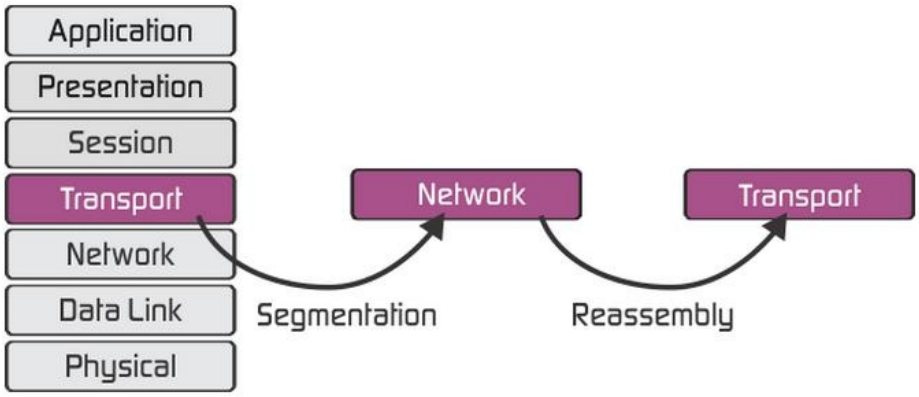
Network Layer

- 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..

Data-link Layer

It is responsible for end-to-end delivery of data between the devices on a Network segment. 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.

Physical Layer

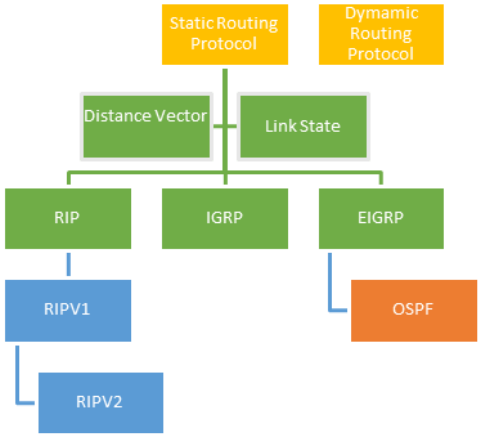
- It deals with physical transmission of Binary data on the given media (copper, Fiber, wireless..).
- It also deals with electrical, Mechanical and functional specifications of the devices, media.. etc
- The major functions described at this layer are..

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

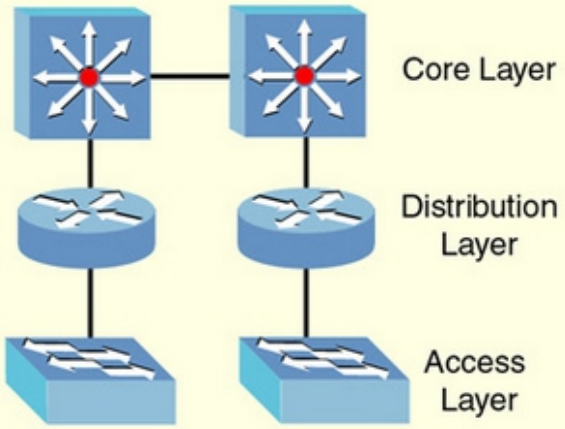
Devices works at physical layer are Hub, Modems, Repeater, Transmission Media

The Cisco Three-Layer Hierarchical Model:

1- Core Layer: Uses multi-layer switches.
Functions: Switches traffic as fast as possible using high speed technology (i.e. FDDI, Fast-Ethernet/Gigabit-Ethernet, ATM).

2- Distribution Layer: (also called *Workgroup layer.*) Uses routers.
Functions: Routes between LANs and VLANs. Provides Security (i.e. *Access List, Packet Filtering, Queuing, Route Redistribution*) and broadcasts control.

3- Access Layer: (also called *Desktop Layer.*) Uses switches.
Functions: Provides access to the network. Breaks collision domains.



INTRODUCTION TO ROUTERS

Wht is a Router ?

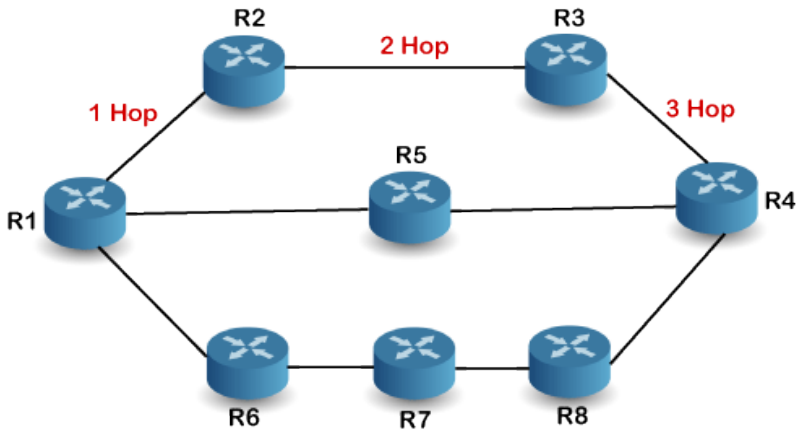
- Router is a device which makes communication possible between two or more different networks present in different geographical locations.
  - It is an internetworking device used to connect two or more different networks
  - It works on layer 3 i.e. network layer.
- It does two basic things:-
  - Select the best path from the routing table.
  - Forward the packet on that path

Which Routers to buy ?

Many companies are manufacturing Router :

- Cisco
- Juniper
- huawei

But Cisco is having Monopoly in the market of Routers



Router Classification

FIXED ROUTER	MODULAR ROUTER
• Fixed router (Non Upgradable cannot add and remove the Ethernet or serial interfaces) • Access Layer Routers are example of Fixed Router except 1600 and 1700 series	• Modular router (Upgradable can add and remove interfaces as per the requirement) • Distribution and Core Layer Routers example of Modular Router

Branch

Gain highly secure connectivity, machine learning, and cloud-managed security.

ISR 4000 Series (updated)

ISR 1000 Series (updated)

ISR 900 Series (new)

ISR 800 Series

Meraki MX

WAN aggregation

Get performance and security for WAN, Internet, and machine-to-machine (M2M) interconnectivity.

NCS 5000 Series

NCS 5500 Series

ASR 1000 Series

Edge

Grow density and resiliency with programmability for a scalable network edge.

ASR 9000 Series

ASR 1000 Series

Service provider core

Address today's needs and scale for future ones with strong ROI.

NCS 6000 Series

NCS 5500 Series

ASR 9000 Series

Industrial

Deliver enterprise-class features in rugged and harsh environments.

900 Series Industrial (new)

800 Series Industrial ISR

2000 Series Connected Grid Routers

1000 Series Connected Grid

Virtual

Get multitenant network services for public, private, or provider-hosted clouds.

IOS XRv 9000

CSR 1000v

Meraki vMX100

Small Business Routers

Get advanced capabilities and security features at an affordable price.

ISR 4221

ISR 1000 Series

ISR 900 Series (new)

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

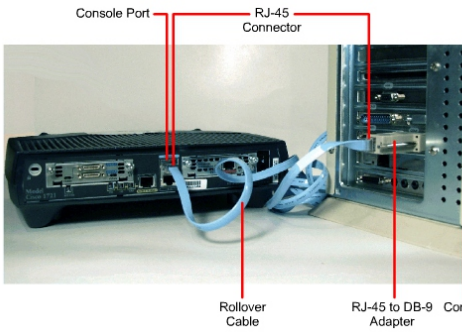
- It is known as Local Administrative Port
- It is generally used for Initial Configuration, Password Recovery and Local Administration of the Router. It is RJ45 Port
- **IMP :** It is the most delicate port on the Router. So make less use of the Console Port.

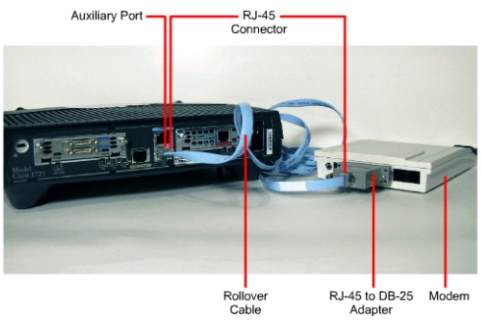
Console Connectivity

- 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

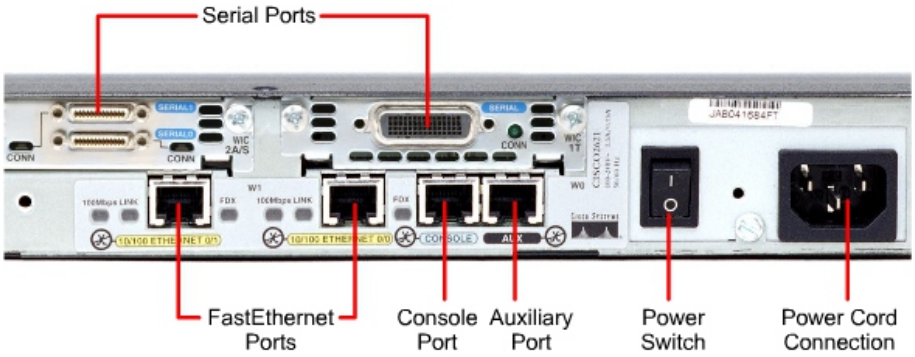
Auxiliary Port

- 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



Networking Software Systems

IOS

- Integrates technology, business services, and hardware support
- Reduces operational spending
- Optimizes return on investment
- Improves business productivity

IOS XE

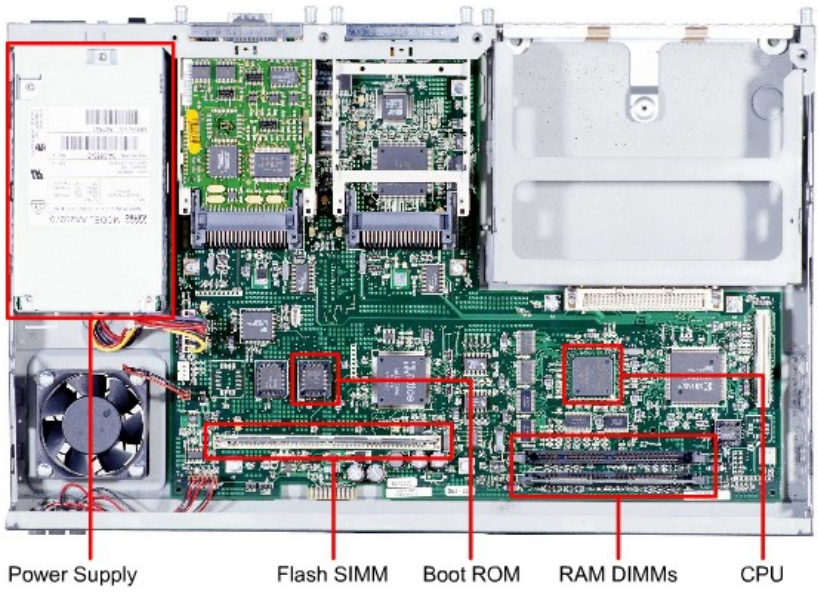
- Supports next-generation platforms
- Runs as a single daemon within a modern Linux operating system
- Separates the data plane and control plane
- Improved services integration

IOS XR

- Focuses on the needs of service providers
- Designed for the dynamic network usage requirements of services
- Flexible programmability for dynamic reconfiguration

NX-OS

- Open, modular and programmable for an agile data center infrastructure
- Optimized for both physical and virtual data center deployments
- Highly reliable continuous system operation, optimizing uptime



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.

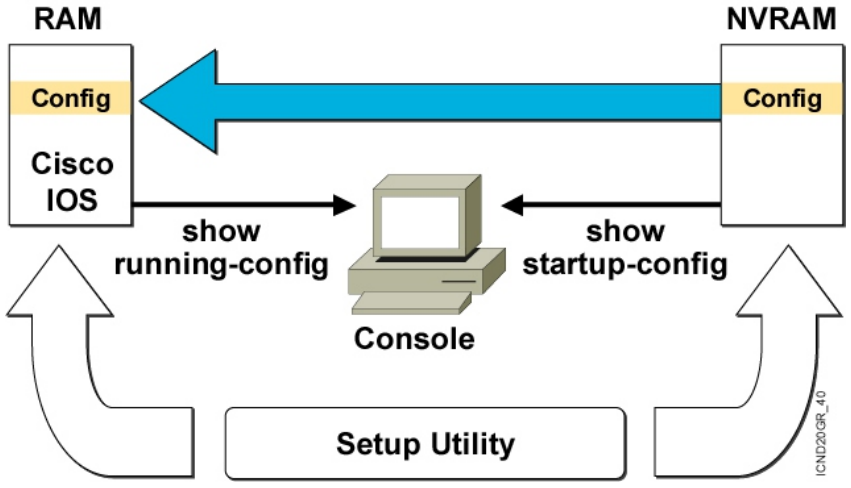
- **NVRAM -** Non volatile RAM, similar to Hard Disk It is also known as Permanent Storage or Startup Configuration. Generally size of NVRAM is 32 KB.

- **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



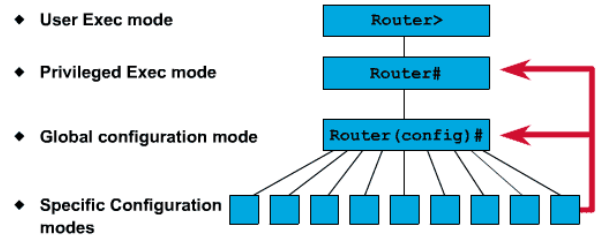
MODES OF A ROUTER:-

- 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.

Overview of Router Modes



Configuration Mode	Prompt
Interface	`Router(config-if)#`
Subinterface	`Router(config-subif)#`
Controller	`Router(config-controller)#`
Map-list	`Router(config-map-list)#`
Map-class	`Router(config-map-class)#`
Line	`Router(config-line)#`
Router	`Router(config-router)#`
IPX-router	`Router(config-ipx-router)#`
Route-map	`Router(config-route-map)#`

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:

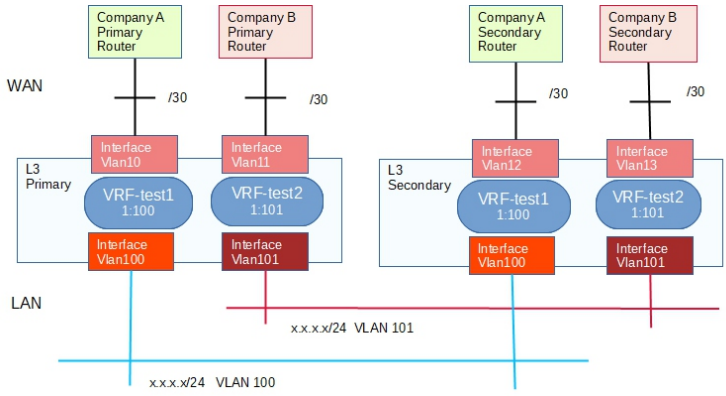
Router(config) #

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 enable password:

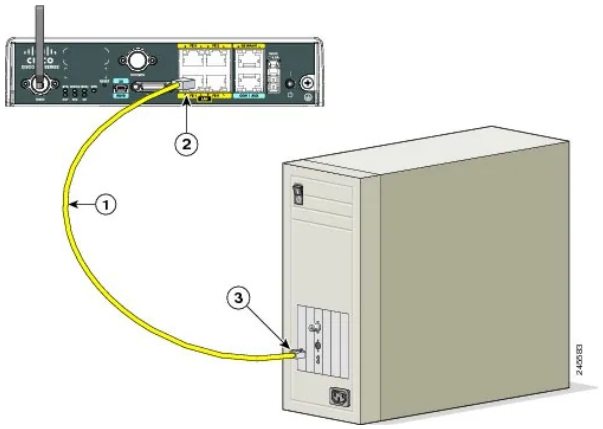
Router(config) # enable secret <password> (To encrypt the password)
Router(config) # enable password <password>

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



Basic Show Commands

Router#show running-config

Router#show flash

Router#show ip protocols

Use this command to view the status of the current layer 3 routed protocols running on your router

Router#show version

This command will give you critical information, such as: router platform type, operating system revision, operating system last boot time and file location, amount of memory, number of interfaces, and configuration register

Router#show clock
***1:46:13.169 UTC Mon Nov 1 2009**

Will show you Routers clock

Router#show hosts

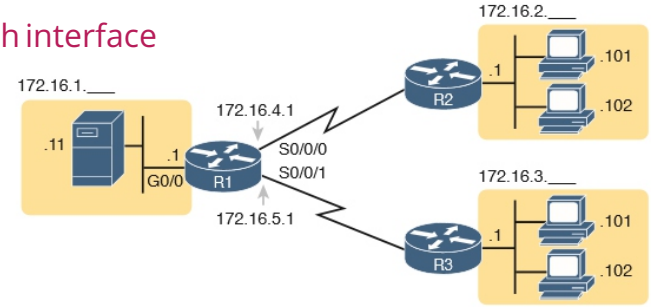
will display a cached list of hosts and all of their interfaces IP addresses

Router#show users

Will show a list of all users who are connected to the router

Router#show interfaces

will give you detailed information about each interface



Router#show protocols

will show the global and interface-specific status of any layer 3 protocols

Router#show ip interface brief

This command will show brief descriptions about interface. This command mostly used in troubleshooting.

There may be three possible conditions of status.

UP: - interface is up and operational

DOWN: - physical link is detected but there is some problem in configurations.

Administratively down: - port is disable by shutdown command (Default mode of any port on router.)

R1#show ip route

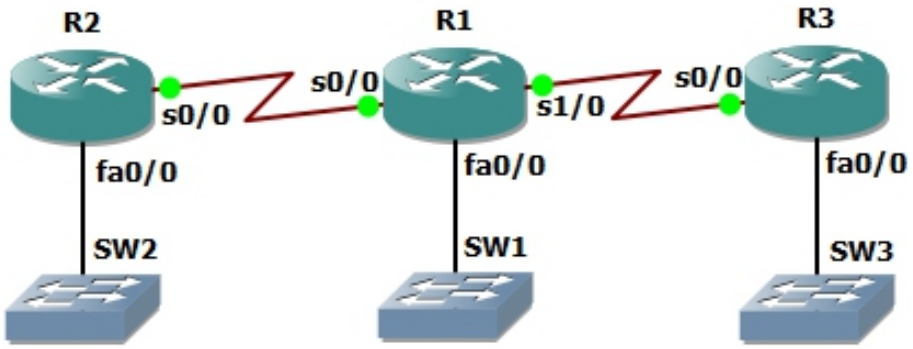
This command will give a detail about known route. Router will not forward packet if route is not shown here for that packet. Router's routing decision is made by this routing table.

R1#show controllers serial 0/0/0

Most common use of this command is to find out whether the port is DCE end or DTE. If the port is DCE end then clock rate and bandwidth command will require. As you can see in output that port is DCE.

R1#show ip protocols

Use this command to know about running routing protocols.

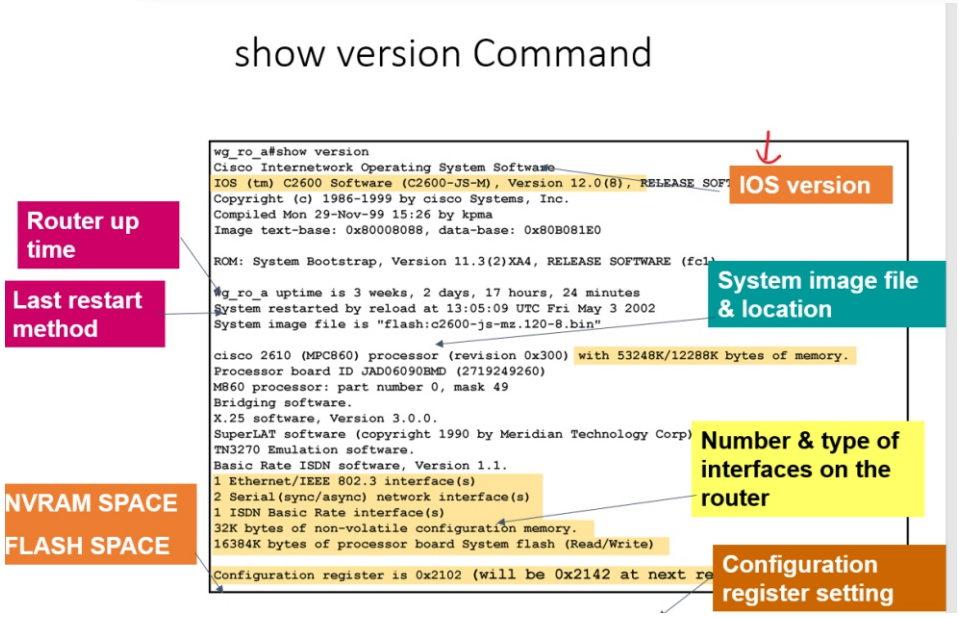


How to configure a new router or a switch.

Show ip int brief : Ip address, Interface is up or down

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

Show version: Hardware & software information.



Show flash : To check the IOS File in flash memory.

```
Router#show flash:

System flash directory:
File  Length    Name/status
  3   33591768 c1900-universalk9-mz.SPA.151-4.M4.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

To change the **hostname**:
Router>enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#**hostname Delhi-Gw1**
Delhi-Gw1(config)#

To check the current configuration:
Delhi-Gw1#**show running-config** (Ram)

To check the Startup configuration:
Delhi-Gw1#**show startup-config** (NVRAM)

To save the configuration:
Delhi-Gw1#**write**
Building configuration...
[OK]

To reload the Router:
Delhi -Gw1#**reload**
Proceed with reload? [confirm]

To check the routing table:
Delhi -Gw1#**show ip route**

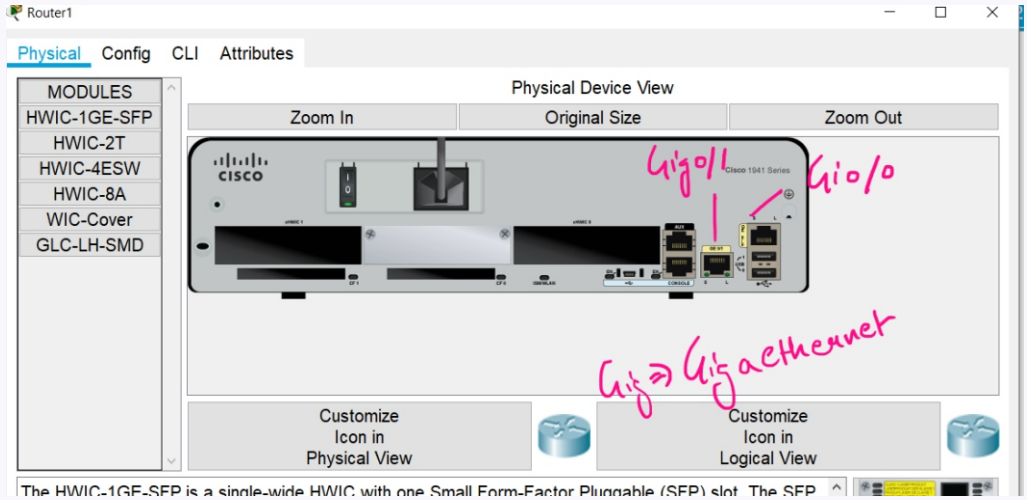
Note: To select the best path, router makes a routing table.

```
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
       ia - IS-IS inter area, * - candidate default, U - per-user static ro
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
C       10.1.3.0/24 is directly connected, FastEthernet0/1
S       10.1.0.0/16 [1/0] via 10.1.3.1
C       10.1.4.0/24 is directly connected, FastEthernet0/0
S       10.200.1.1/32 [1/0] via 10.1.3.1
S       10.200.1.4/32 [1/0] via 10.1.4.1
```

To Check the interfaces/ports status and Ip address.

```
Pune-Gw1#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1     unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES NVRAM  administratively down down
Pune-Gw1#
```

Router has two ports Gig0/0 and Gig0/1



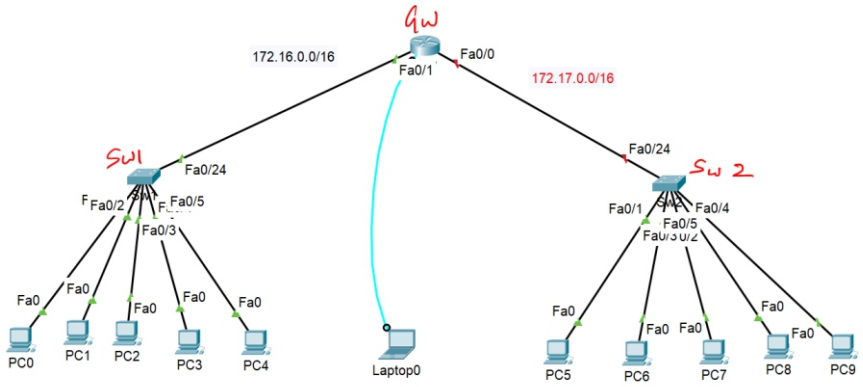
LAB#1 : Connect two different Networks.

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



Router>enable
Router#configure terminal

Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 172.16.0.2 255.255.0.0
Router(config-if)#no shutdown
Router(config-if)#end

Show ip interface brief: Interface IP address and status
Show ip route : Its shows the routing table.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        172.16.0.1      YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
Router#
Router#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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

C    172.16.0.0/16 is directly connected, FastEthernet0/1
```

Error : IF you will try to assign the same network on another interface.
Router(config)#interface fa0/0
Router(config-if)#ip address 172.16.0.1 255.255.0.0
% 172.16.0.0 overlaps with FastEthernet0/1

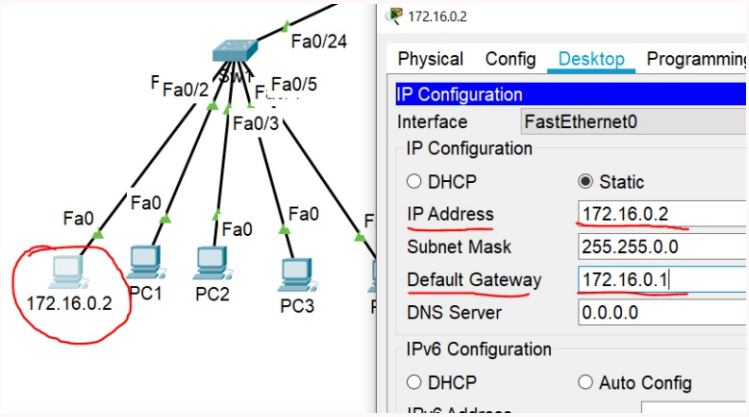
Assign always a different network on different interface.
Router(config)#interface fa0/0
Router(config-if)#ip address 172.17.0.1 255.255.0.0
Router(config-if)#no shutdown

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        172.17.0.1      YES manual up                    up
FastEthernet0/1        172.16.0.1      YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
Router#
Router#
Router#
Router#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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

C    172.16.0.0/16 is directly connected, FastEthernet0/1
C    172.17.0.0/16 is directly connected, FastEthernet0/0
```

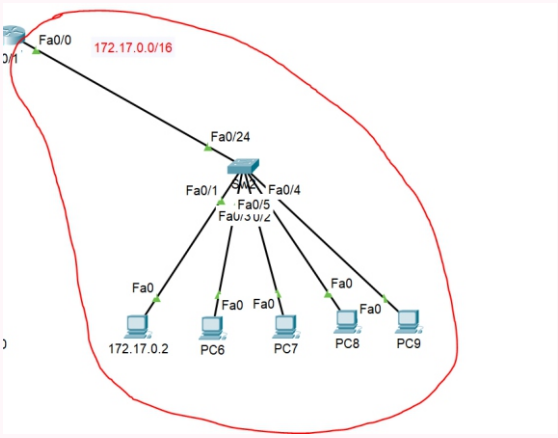
In short, router has learned both the networks from both the interfaces.

Now, both the routers can communicate between each other.

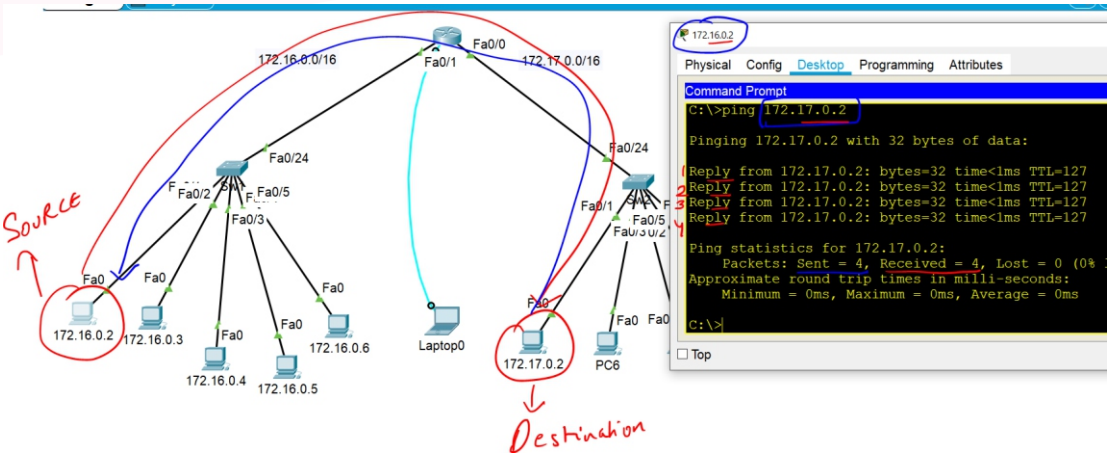
Assign IP in all the computers.



Router Gateway and Lan Network Should be in same network.



Ping Results,



ROUTING

- Routing is the process of selecting a best path for forwarding the packets. In a network, there are many routes for source to destination. But we want a best path, where less traffic congestion and packets are delivered fast.
- Routing table consist of only the best routes for every destinations.
- In below diagram, you can see there are 3 routes for source to destination, different color arrow signs are representing different routes. So, before forwarding a packet router first check its routing table for best path and then forward the packet.

Types of Routing

1. Static Routing

2. Default Routing

3. Dynamic Routing

Static Routing:

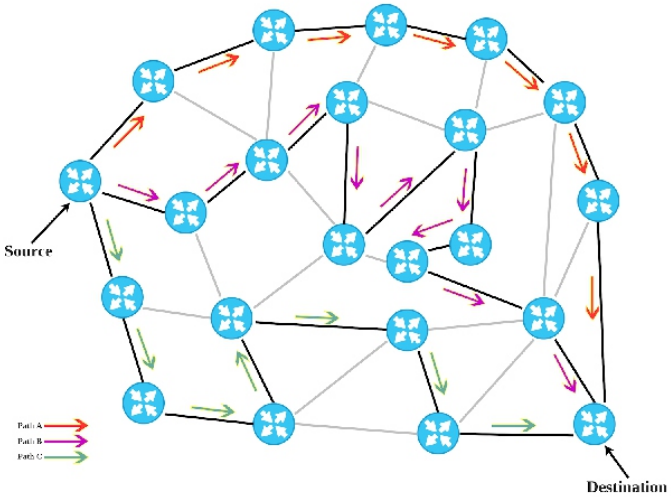
In static routing, routes are configured manually by administrator. The routes, which are configured by static routing are permanent routes. These routes will not changed until changed by manual configuration.

To configure static routing, we require network ID, subnet mask and next-hop address.

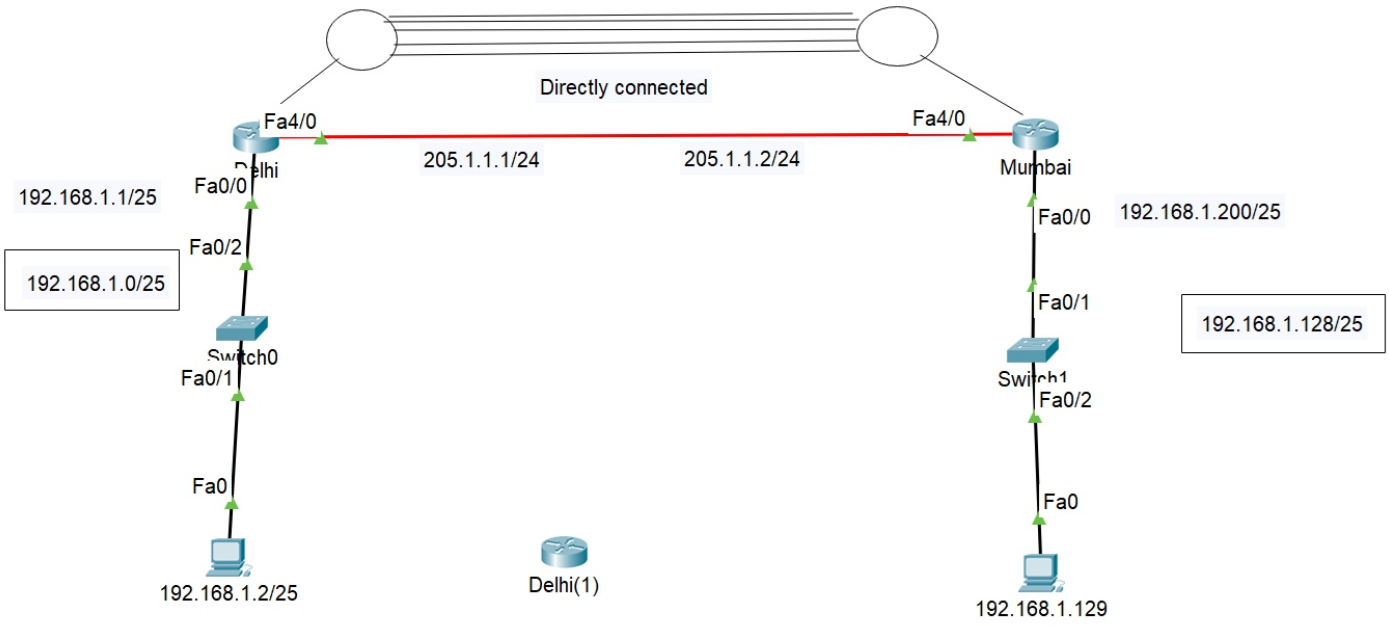
Static routing is used for small organizations within a network of 10-15 routers. Static routes are fast and secure. AD value of static route is 1.

Disadvantages :-

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



Lab 2 # Configuring Static Route



Delhi 192.168.1.0 - Nwid 192.168.1.127 - Broadcast Id	Mumbai 192.168.1.128 - Nwid 192.168.1.255 - Broadcast Id
Delhi conf t hostname delhi int fa0/0 ip address 192.168.1.1 255.255.255.128 no shutdown int fa4/0 ip address 205.1.1.1 255.255.255.0 no shutdown **ip route 192.168.1.128 255.255.255.128 205.1.1.2**	Mumbai conf t hostname Mumbai int fa0/0 ip address 192.168.1.200 255.255.255.128 no shutdown int fa4/0 ip address 205.1.1.2 255.255.255.0 no shutdown **ip route 192.168.1.0 255.255.255.128 205.1.1.1**

Default Routing

Default route is configured only when destination is unknown. Like static route, it is also configured manually. Default routing path is least preferred path. When there is no entry for the destination network in a routing table, the router will forward the packet to its default route. Default routes help in reducing the size of your routing table.

Configuring Default Route : There are 2 ways to configure default routing

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

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

Note: In default routing, destination network id and destination subnet mask field are 0.0.0.0 (unknown destination).

Lab 3 # Default Routing

A loopback interface is a logical, virtual interface in a Cisco Router. A loopback interface is not a physical interface like Fast Ethernet interface or Gigabit Ethernet interface. A loopback interface has many uses.

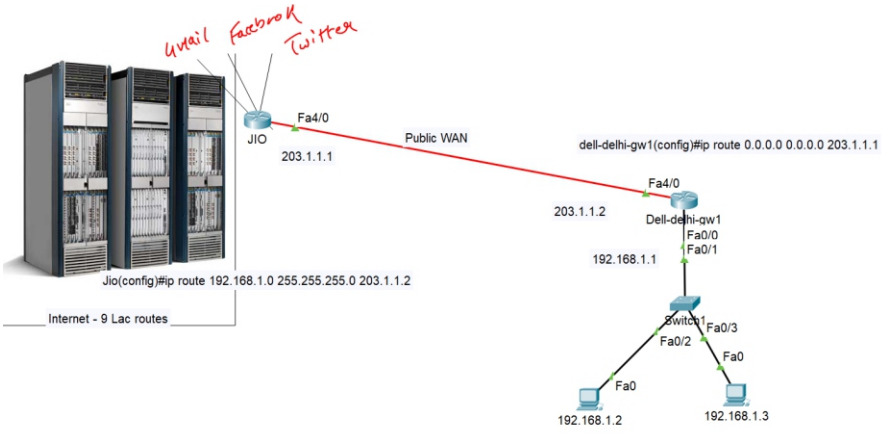
To make a LAB Internet Router – we make loopbacks on router

You can make as many loopbacks :

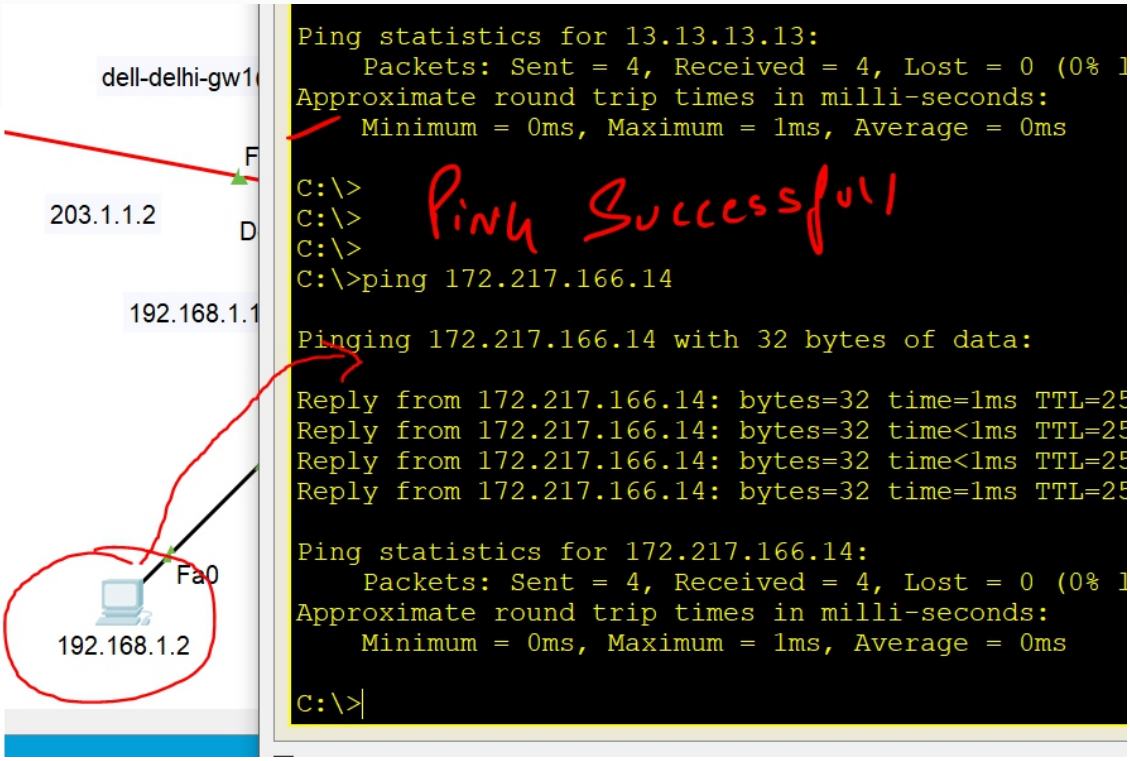
The Loopback Range :

Router(config)#interface loopback ?

<0-2147483647> Loopback interface number



Jio conf terminal int fa4/0 ip address 203.1.1.1 255.255.255.0 no shutdown **int loopback 0** ip address **172.217.166.14** 255.255.255.0 description google.com **int loopback 1** ip address **31.13.79.35** 255.0.0.0 description facebook.com **int loopback 2** ip address **104.244.42.193** 255.0.0.0 description twitter.com int loopback 3 ip address 13.13.13.13 255.0.0.0 description nwkings.com **Static Route for Dell company** Jio(config)#ip route 192.168.1.0 255.255.255.0 203.1.1.2	Dell-delhi-gw1 conf terminal hostname dell-delhi-gw1 int fa4/0 ip address 203.1.1.2 255.255.255.0 no shutdown int fa0/0 ip address 192.168.1.1 255.255.255.0 no shutdown **Default route** dell-delhi-gw1(config)#ip route 0.0.0.0 0.0.0.0 203.1.1.1



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)

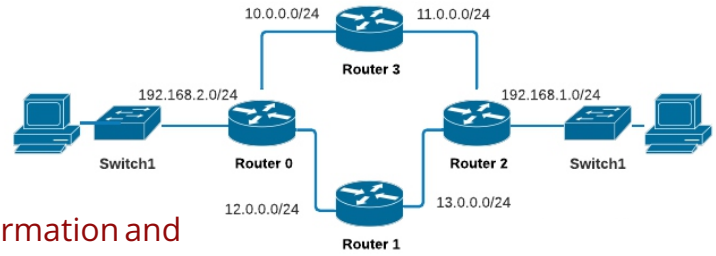
4) Serial is down, line protocol is down (Serial interface on the remote router has to be configured)

Dynamic Routing

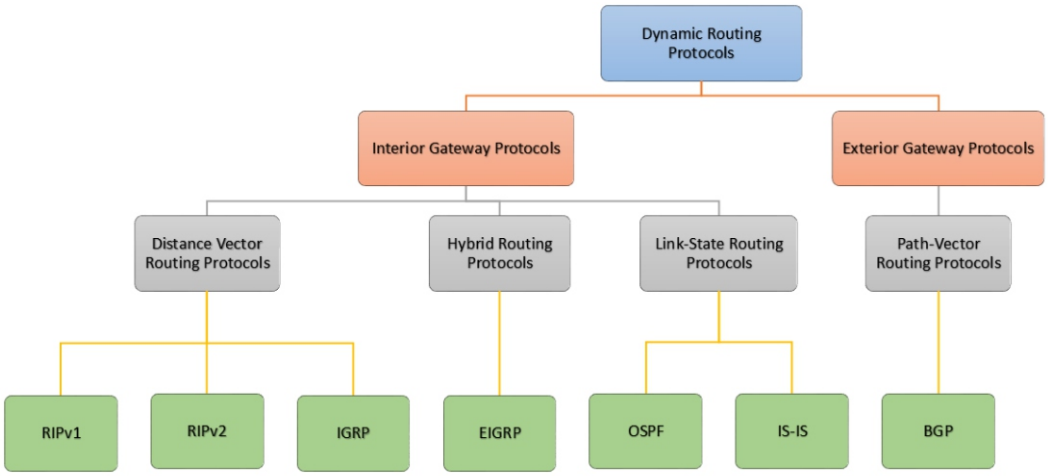
In dynamic routing, we configure a dynamic routing protocol that learns routes automatically and also updates the routing table dynamically when changes are happened in the network. For internal gateway routing, we use OSPF, EIGRP, IS-IS and for external gateway routing BGP is used.

Advantages of Dynamic over static :

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



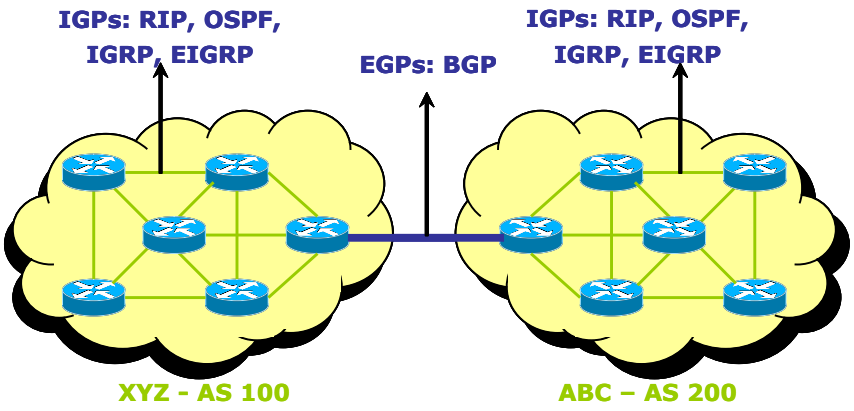
Types of Dynamic Routing Protocols



Routing Protocol Classification

IGP	EGP
• Interior Gateway Protocol • Routing protocols used within an autonomous system • Routers inside same Autonomous boundary need an IGP. • RIP, IGRP, EIGRP, OSPF, IS -IS	• Exterior Gateway Protocol • Routing protocol used between differ ent autonomous systems • Routers in different AS need an EGP • Border Gateway Protocol is extensively used as EGP

In short, IGPs are used inside the same autonomous system(AS) and EGPs are used between different AS.You can see in below, there are two AS named as XYZ-AS 100 and ABC-AS 200. Inside both AS, interior gateway protocols (OSPF, RIP, EIGRP) are used. And to connect these two AS exterior gateway protocol (BGP) is used.



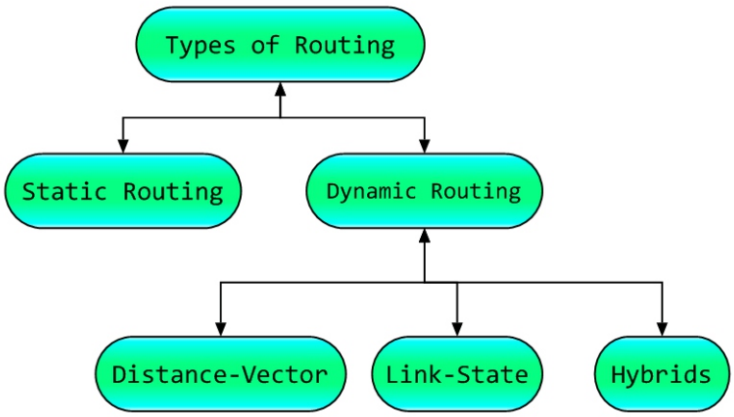
- Distance Vector Protocol
- Link State Protocol
- Hybrid Protocol

Distance Vector Protocol	Link State Protocol	Hybrid Protocol
• Works with Bellman Ford algorithm • Periodic updates • Classful routing protocol • Full Routing tables are exchanged • Updates are through broadcast • Example: RIP 1, RIP 2, IGRP	• Works with Dijkstra algorithm • Link state updates • Classless routing protocol • Missing routes are exchanged • Updates are through multicast • Example : OSPF, ISIS	• Also called as Advance Distance vector Protocol • Works with DUAL algorithm • Link state updates • Classless routing protocol • Missing routes are exchanged • Updates are through multicast • Example : EIGRP

Administrative Distance

AD stands for administrative distance. When router learns two different paths for same destination by using different protocols. In that situation to decide which is the best path, router first checks AD value. The path that has lower AD value, is considered as the best path. AD values are predefined.

- Rating of the Trustworthiness of a routing information source.
- The Number is between 0 and 255
- The higher the value, the lower the trust.



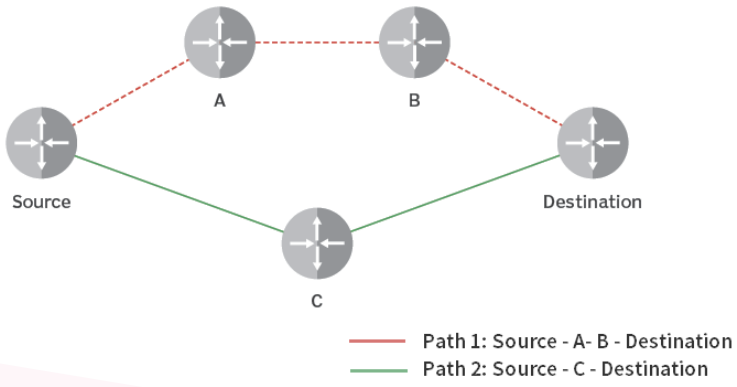
Routing Protoc	AD valu
Connected Rou	0
Static Route	1
RIP	120
IS-IS	115
OSPF	110
EIGRP	90
External EIGRP	170
BGP	20
Internal BGP	200
Unknown	255

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

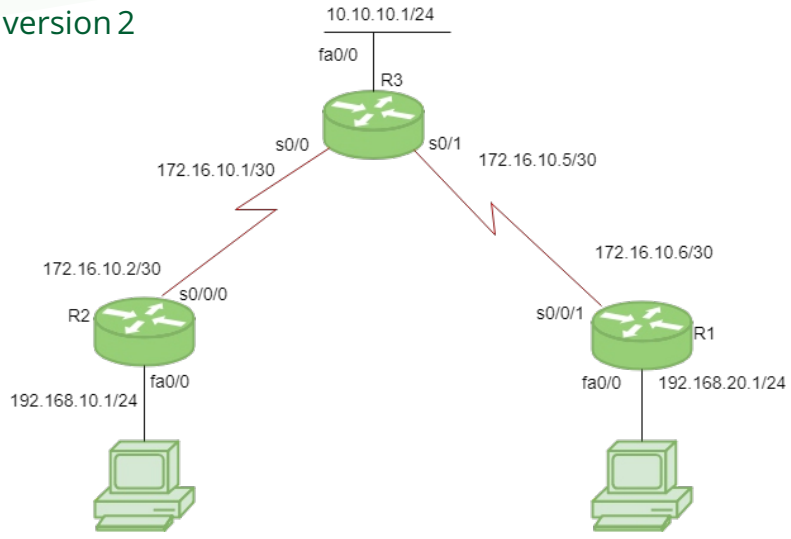
- Bandwidth utilization is very high as broadcast for every 30 second
- Works only on hop count
- Not scalable as hop count is only 15
- Slow convergence

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



LAB Practical RIP

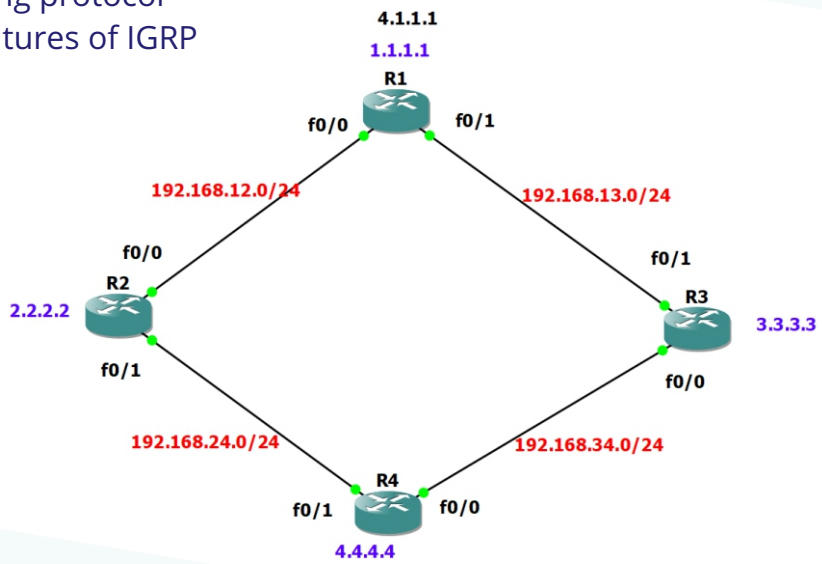
conf t hostname R1 int f0/0 ip address 192.168.12.1 255.255.255.0 no shutdown int f0/1 ip address 192.168.13.1 255.255.255.0 no shutdown int loopback 0 ip address 1.1.1.1 255.255.255.255 int loopback 1 ip address 4.1.1.1 255.255.255.255 **Router rip** **version 2** **no auto-summary** **network 192.168.12.0** **network 192.168.13.0** **network 1.1.1.1**	conf t hostname R2 int f0/0 ip address 192.168.12.2 255.255.255.0 no shutdown int f0/1 ip address 192.168.24.2 255.255.255.0 no shutdown int loopback 0 ip address 2.2.2.2 255.255.255.255 **Router rip** **version 2** **no auto-summary** **network 192.168.12.0** **network 192.168.24.0** **network 2.2.2.2**	conf t hostname R3 int f0/0 ip address 192.168.34.3 255.255.255.0 no shutdown int f0/1 ip address 192.168.13.3 255.255.255.0 no shutdown int loopback 0 ip address 3.3.3.3 255.255.255.255 **Router rip** **version 2** **no auto-summary** **network 192.168.34.0** **network 192.168.13.0** **network 3.3.3.3**	conf t hostname R4 int f0/0 ip address 192.168.34.4 255.255.255.0 no shutdown int f0/1 ip address 192.168.24.4 255.255.255.0 no shutdown int loopback 0 ip address 4.4.4.4 255.255.255.255 **Router rip** **version 2** **no auto-summary** **network 192.168.34.0** **network 192.168.24.0** **network 4.4.4.4**

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

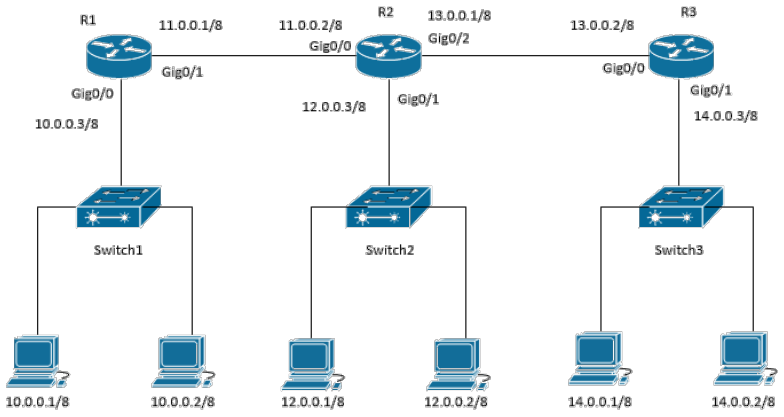
Disadvantages of EIGRP

- Works only on Cisco Routers

Configuring EIGRP

Router(config)# router eigrp <as no>

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

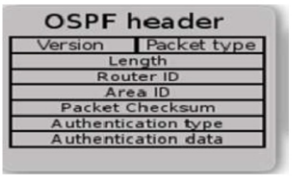


EIGRP AS 100

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 (cost=10 ^8/B.W.)
- Administrative distance is 110
- It is a classless routing protocol
- It supports VLSM and CIDR
- It supports only equal cost load balancing
- Introduces the concept of Area's to ease management and control traffic
- Provides hierarchical network design with multiple different areas
- Must have one area called as area 0
- All the areas must connect to area 0
- Scales better than Distance Vector Routing protocols.
- Supports Authentication
- Updates are sent through multicast address 224.0.0.5
- 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 periodicupdates

OSPF PACKET ENCAPSULATION



- VERSION: OSPF VERSION
- TYPE: TYPE 1/TYPE 2/TYPE 3/TYPE 4/TYPE 5
- PACKET LENGTH: LENGTH OF PROTOCOL IN BYTES
- ROUTER ID: ROUTER IDENTIFIER IN OSPF
- AREA ID : REPRESENTS THE AREA OF INTERFACE OPERATION
- CHECKSUM : USED TO CHECK THE PACKET INTEGRITY
- AuTYPE: TYPE OF OSPF PACKET AUTHENTICATION: 0/1/2
- AUTHENTICATION: USED FOR AUTHENTICATION

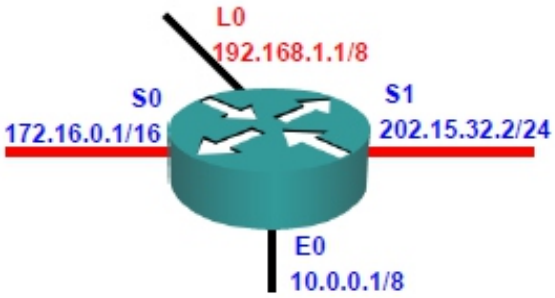
OSPF PACKET TYPES

- TYPE 1: HELLO PACKETS : USED TO DISCOVER NEIGHBORS
- TYPE 2: DATABASE DESCRIPTION : SYNCHRONIZATION BETWEEN ROUTERS
- TYPE 3: LINK STATE REQUEST :LIST OF ALL MISSING LSAs
- TYPE 4: LINK STATE UPDATE: RESPONSE TO LSR
- TYPE 5: LINK STATE ACKNOWLEDGEMENT: ACKNOWLEDGES THE RECEIPT OF LSAs

1. Hello
2. Database Description (DBD)
3. Link-State Request (LSR)
4. Link-State Update (LSU)
5. Link-State Acknowledgment (LSAck)

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.

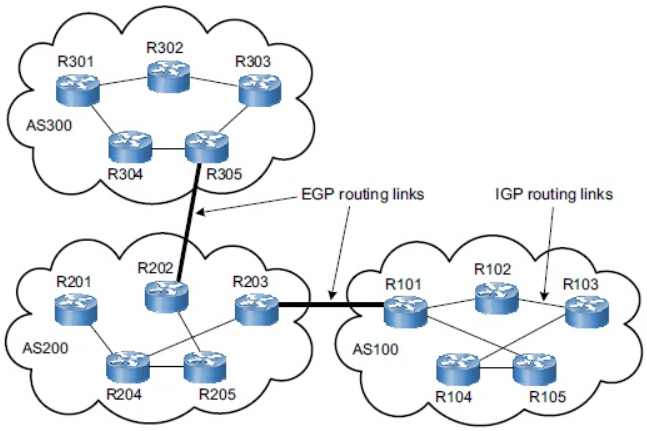
3) Routing information Table Routing table contains information about the best path calculated by the shortest path first algorithm in the database table.

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 :

Global Subnet Mask

–Customized Subnet Mask

Wild Card Mask

255.255.255.255
–255.255.255.240

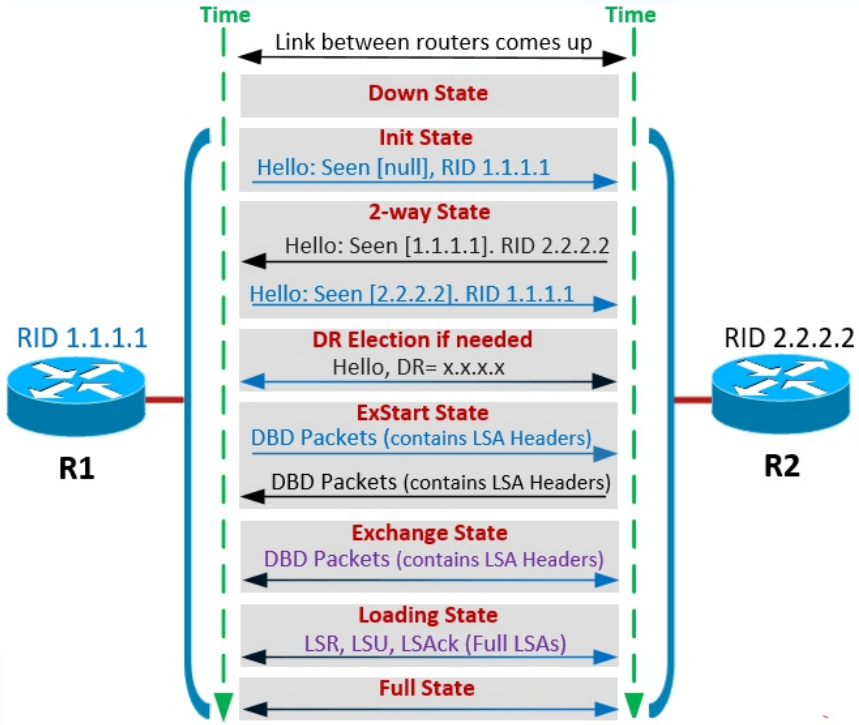
---

0. 0. 0. 15

Configuring OSPF

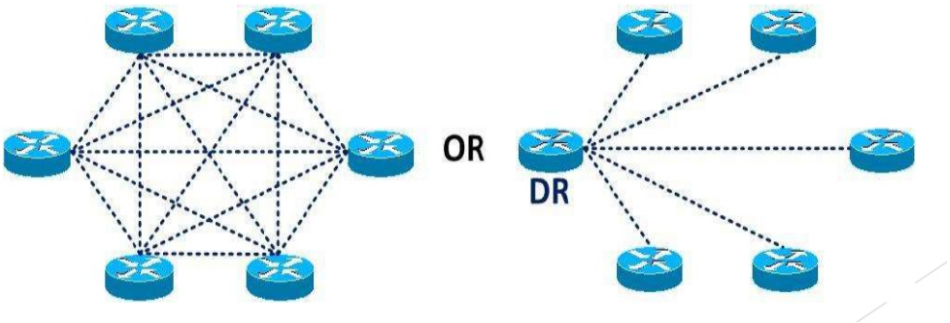
Router(config)# router ospf <pid>
Router(config-router)# network <Network ID> <wildcard mask> area <area id>

OSPF STATES



DR/BDR

- DR : DESIGNATED ROUTER BDR: BACKUP DESIGNATED ROUTER
- DR SERVE AS COLLECTION POINTS OF LINK STATE ADVERTISEMENTS
- BDR BACKS UP THE DR
- GREATLY REDUCES OSPF TRAFFIC



- DR/BDR Selection
- First Router to Initialize
- Router with Highest Priority ID
- Router with Highest Router ID
- Set the Highest Router ID
- Highest Loopback Interface IP Address
- Highest Interface IP Address

Designated Router Operation

- Designated Router (DR)
  - Listens for LSAs on all designated routers multicast address of 224.0.0.6
  - Transmits network LSA to other routers on 224.0.0.5
  - Ensures that all routers on that network have the same synchronized LSBD
- Backup Designated Router (BDR)
  - Listens for LSAs via all designated routers multicast address of 224.0.0.6
  - Listens for network LSAs on 224.0.0.5
  - Ensures quick failover if the designated router is no longer reachable
- Other OSPF routers
  - Transmits LSAs to DR and BDR using 224.0.0.6
  - Listens for network LSAs on 224.0.0.5

HSRP – Hot Standby Routing Protocol

HSRP stands for Hot standby routing protocol. It is also known as gateway redundancy protocol. It is a Cisco proprietary protocol.

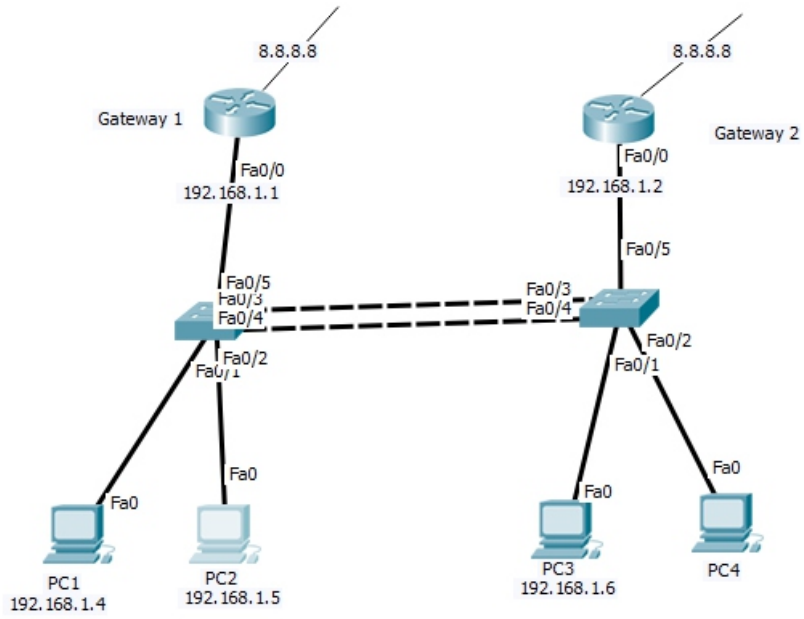
HSRP is used for gateway load balancing. In HSRP, there are 2 gateways one stay in active mode and another is standby mode. In normal condition, all traffic goes to active gateway, but if active gateway goes down because of any issue, then all traffic shift to standy gateway. When active gateway come back again traffic shift to active gateway.

Now some of you have doubt, we can configure only one gateway in host config, then how traffic will shift to other without knowing the IP address of other gateway.

So, let me clarify this, when we configure HSRP, a virtual gateway is created and that becomes the gateway for all LAN hosts.

How HSRP works?

Let's understand with an example. Imagine below network is a company network



To ensure network connectivity 24/7, here we took two connection from two different vendors, so that if one goes down, traffic shift to other.

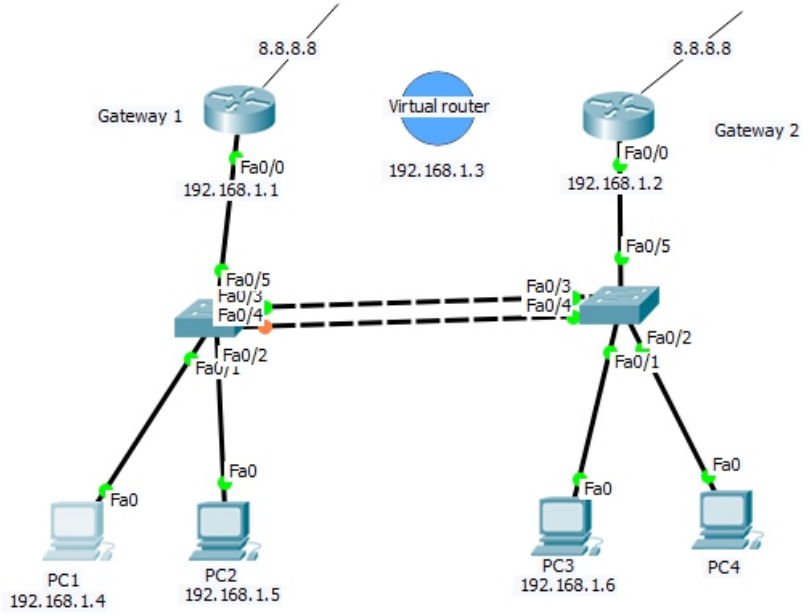
Take a situation, PC1 and PC2 have gateway 1 IP address in their config and PC3 and PC4 have gateway 2 IP address in their config. Let's suppose gateway 1 link goes down, because of some technical issue, in that case traffic should be shift to other gateway, and if gateway 2 link goes down then traffic should be shift to gateway 1.

Now, the question will traffic shift or not?

Let me tell you, traffic will not shift. Why? Because PCs have different gateway. Here we configured gateway1 in PC1 and PC2 and gateway2 in PC3. To shift traffic first we have to change the gateway manually in the host configurations.

So, what is the solution? And the answer is HSRP.

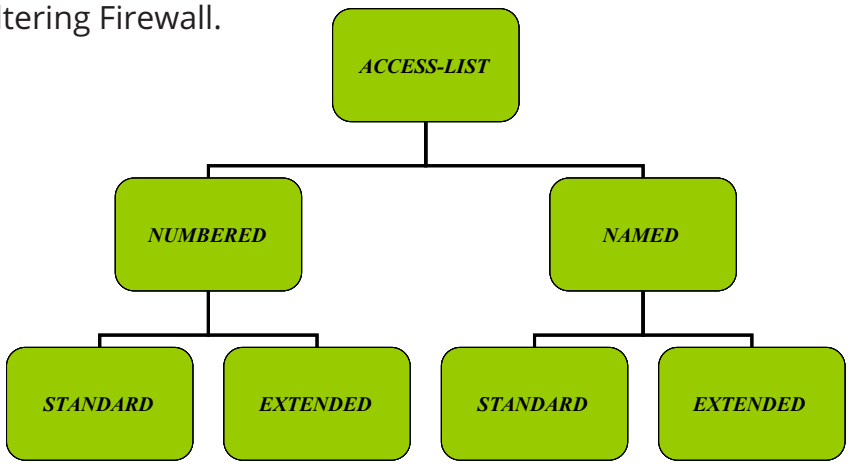
HSRP is the solution for this. In same topology, if we configure HSRP in both gateway then a virtual gateway is generated with a different IP address. And this gateway becomes the gateway for all hosts.



Now, if any one of gateway goes down then traffic will shift to other.

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.



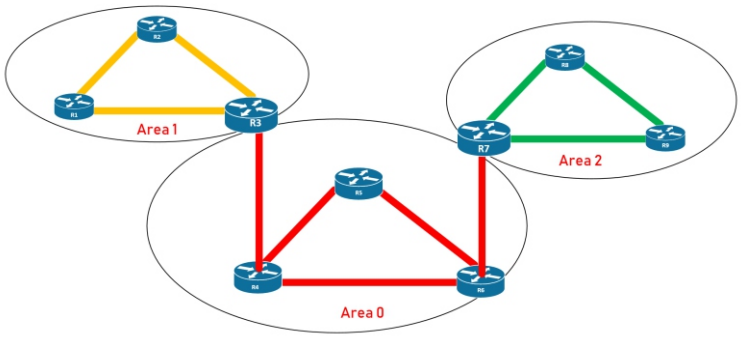
Standard Access List	Extended Access List
• The access-list number range is 1–199 • Can block a Network, Host and Subnet • Two way communication is stopped • All services are blocked. • Implemented closest to the destination. • Filtering is done based on only source I address	• The access-list number range is 100-199 • Can block a Network, Host, Subnet and Service • One way communication is stopped • Selected services can be blocked. • Implemented closest to the source. • Checks source, destination, protocol, p no

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 possi



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

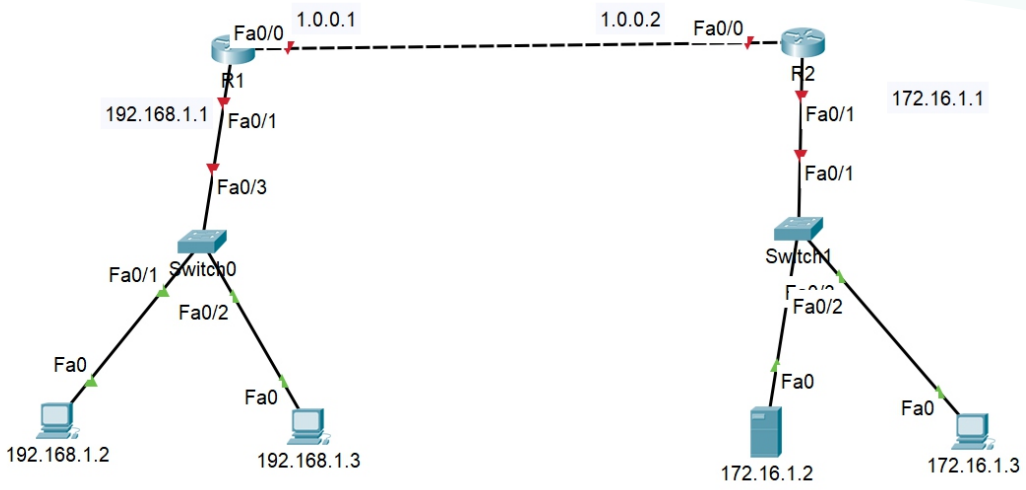
Router(config)# access-list <acl no> <permit/deny> <protocol>
<source address> <source wildcard mask>
<destination address> < destination wildcard mask> <operator> <service>

Implementation of Extended Access List

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

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

LAB Standard ACL



r1	r2
conf t int fa0/1 ip address 192.168.1.1 255.255.255.0 no shutdown int fa0/0 ip address 1.0.0.1 255.255.255.252 no shutdown router eigrp 1 network 192.168.1.0 network 1.0.0.0 no auto-summary	conf t int fa0/1 ip address 172.16.1.1 255.255.0.0 no shutdown int fa0/0 ip address 1.0.0.2 255.255.255.252 no shutdown router eigrp 1 network 172.16.1.0 network 1.0.0.0 no auto-summary

Standard ACL Objective:

Block PC 192.168.1.2 to reach Server 172.16.1.2

Block PC 192.168.1.3 to reach whole network 172.16.0.0

Standard ACL Objective:

Block PC 192.168.1.2 to reach Server 172.16.1.2

Block PC 192.168.1.3 to reach whole network 172.16.0.0

Make access list

R2(config)#access-list 1 deny host 192.168.1.2

R2(config)#access-list 1 deny host 192.168.1.3

R2(config)#access-list 1 permit any

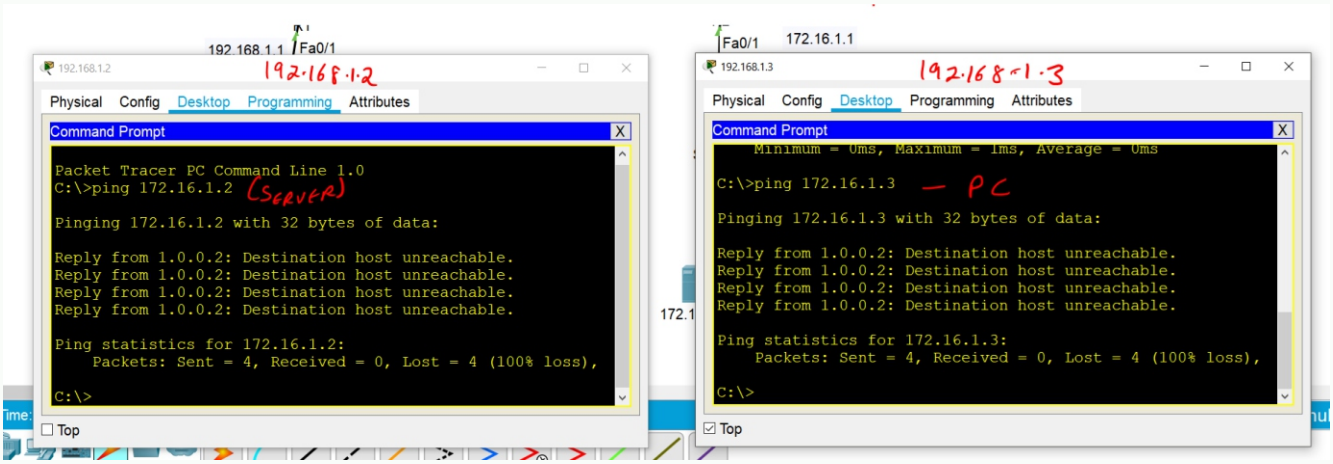
Apply access list

R2(config)#int fa0/1

R2(config-if)#ip access-group 1 out

```
R2#show access-lists
Standard IP access list 1
    10 deny host 192.168.1.2 (256 match(es))
    20 deny host 192.168.1.3
    30 permit any (5 match(es))
```

Hence, traffic is blocked.

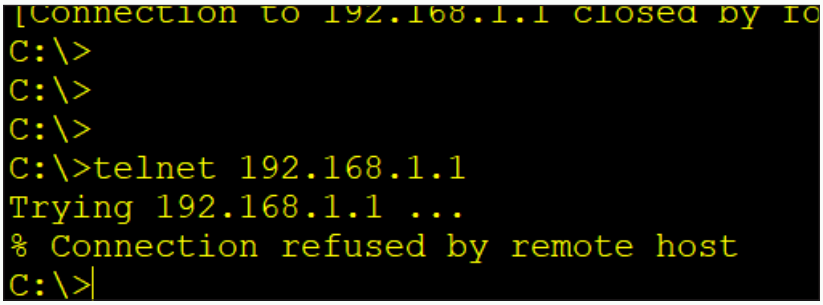


Block Telnet Access for all networks on R1 except **192.168.1.0**

Configure telnet on R1

line vty 0 4
password cisco
login
exit
enable password cisco

Permit 192.168.1.0
Explict deny

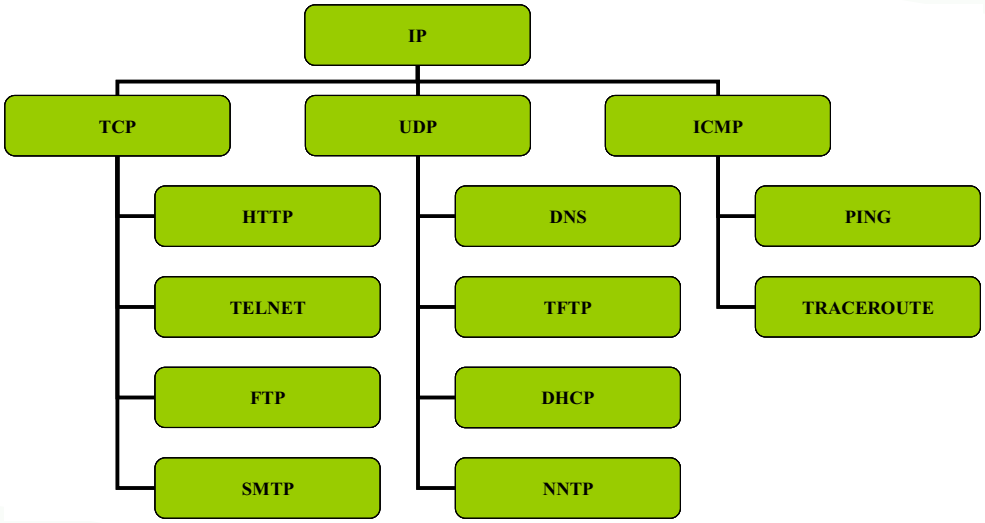


Make ACL

R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255

Apply Inside Line vty – always apply inbound

R1(config)#line vty 0 4
R1(config-line)#access-class 1 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>

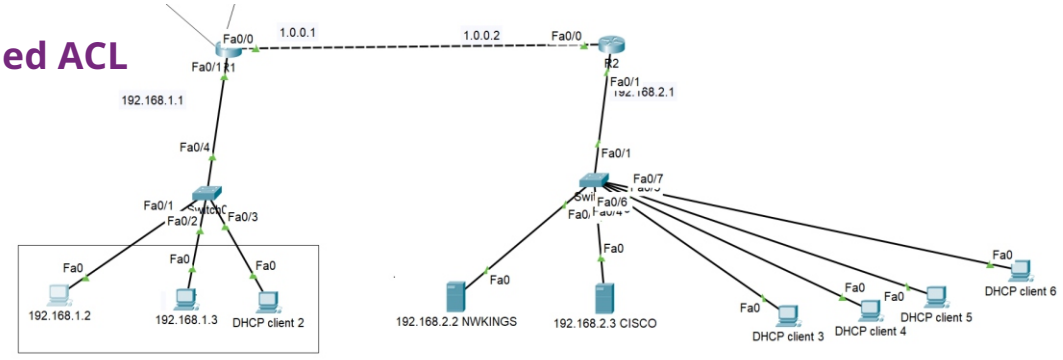
Implementation of Standard Named Access List

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>

LAB Extended ACL



Objective :

Block HTTP - 80

PC 192.168.1.2 > Nwkings 192.168.2.2

PC 192.168.1.3 > Cisco 192.168.2.3

```
R1(config)#access -list 100 deny tcp host 192.168.1.2 host 192.168.2.2 eq 80
R1(config)#access -list 100 deny tcp host 192.168.1.3 host 192.168.2.3 eq 80
```

Block FTP - 21

Network 192 .168.1.0 > Nwkings 192.168.2.2

```
R1(config)#access -list 100 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 21
```

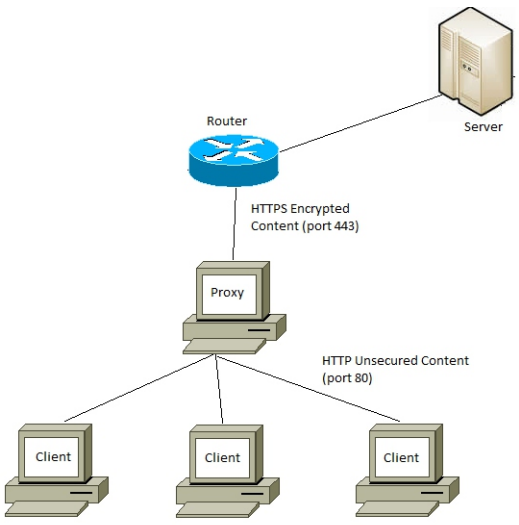
Block ICMP

Network 192.168.1.0 > Cisco 192.168.2.3

```
R1(config)#access -list 100 deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo
R1(config)#access -list 100 deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo    -reply
```

Rest Permit all

```
R1(config)#access -list 100 permit IP any any
```

Apply to interface inbound

R1(config)#int fa0/1n

R1(config-if)#ip access-group 100 in

Named ACL – You can edit Named ACL

R1(config)#ip access-list extended ABC

R1(config-ext-nacl)#deny tcp host 192.168.1.2 host 192.168.2.2 eq 80

R1(config-ext-nacl)#deny tcp host 192.168.1.3 host 192.168.2.3 eq 80

R1(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 21

R1(config-ext-nacl)#deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo

R1(config-ext-nacl)#deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo-reply

R1(config-ext-nacl)#permit IP any any

R1(config-ext-nacl)#end

R1(config)#int fa0/1

R1(config-if)#ip access-group ABC in

R1#show access-lists

Extended IP access list ABC

10 deny tcp host 192.168.1.2 host 192.168.2.2 eq www

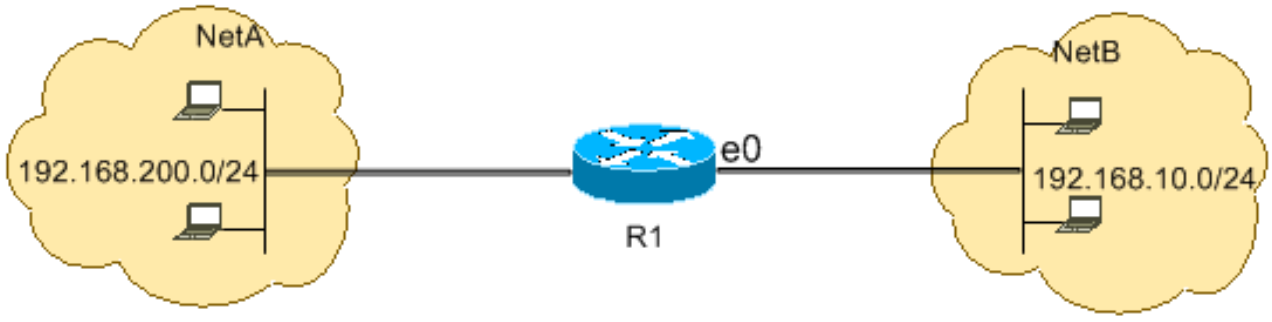
20 deny tcp host 192.168.1.3 host 192.168.2.3 eq www

30 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq ftp

40 deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo

50 deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo-reply

60 permit ip any any



If you want to remove 50 sequence number - echo reply statement

R1(config)#ip access-list extended ABC
R1(config-ext-nacl)#no 50 deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo-repl
R1#show access-lists
Extended IP access list ABC
10 deny tcp host 192.168.1.2 host 192.168.2.2 eq www
20 deny tcp host 192.168.1.3 host 192.168.2.3 eq www
30 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq ftp
40 deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.3 echo
60 permit ip any any

Router Password Breaking

1. console connnection
2. open hypertrm
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