NETWORK ROUTING & SWITCHING BASICS

Contents

Fundamentals of Networking.
OSI and TCP/IP MODEL.
IP addressing and subnetting.
IP routing basics.
Switching basics.
Network Cabling.
WAN Technologies.

Fundamentals of Networking

Networking:- Networking allows exchange of information and resources between devices by using routers, switches and wireless routers or AP's.

Types of traffic:-

a. Unicast:- Packet sent from one node to other node.

b. Multicast:- Packet sent from one node to multiple nodes.

c. Broadcast:- Packet sent from one node to all nodes within broadcast domain.

Collision domain:- A network segment where collision can occur is called Collision domain.

Broadcast domain:- A network segment where all nodes can reach each other by broadcast.

ARP:- Address Resolution Protocol finds the MAC address of a host from a known IP address.

Duplex:-

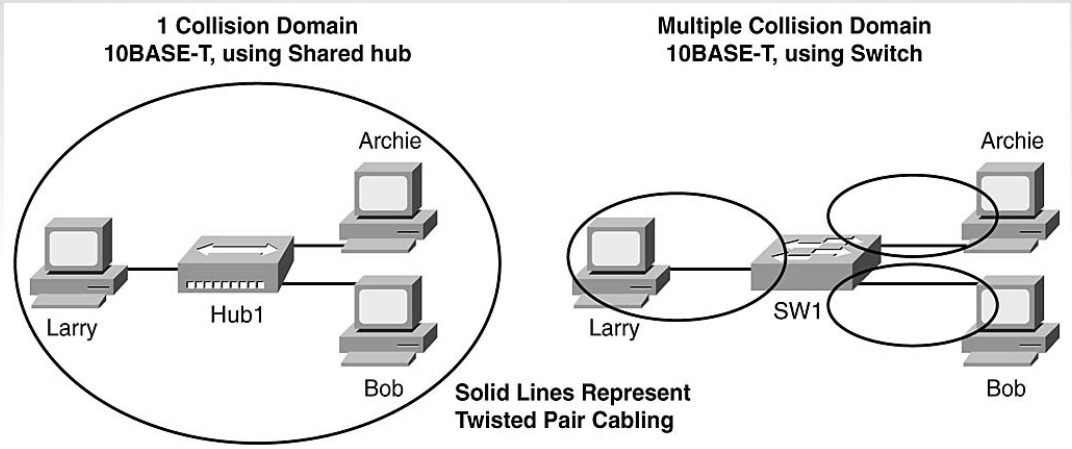
a. Half Duplex:- When one node is transmitting data, no other node can transmit.

b. Full Duplex:- All the nodes can transmit or receive at the same time.

Collision domain

Hub(half duplex):- hub is a multi-port repeater, all the nodes connected to hub are in one collision domain.

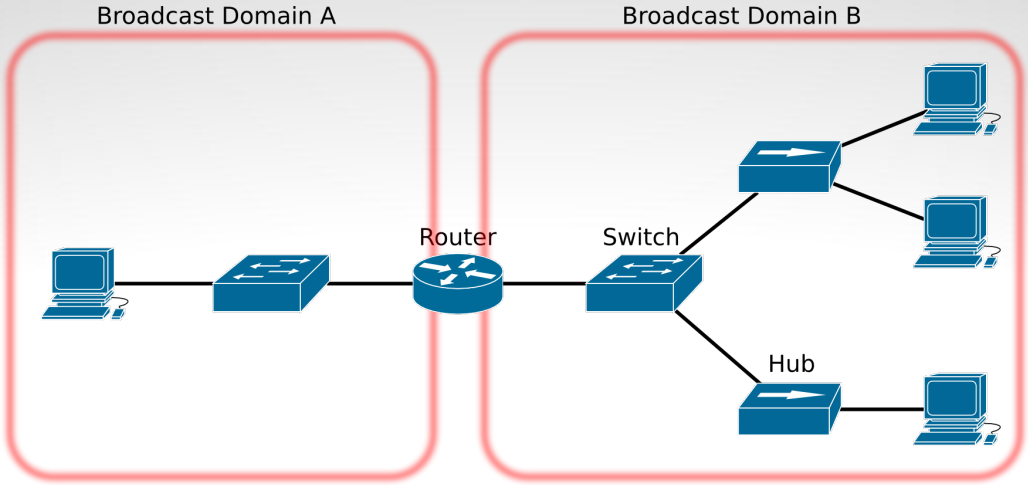
Switch:- Switch breaks collision domain, all the nodes connected to switch are in separate collision domain.



Broadcast Domain

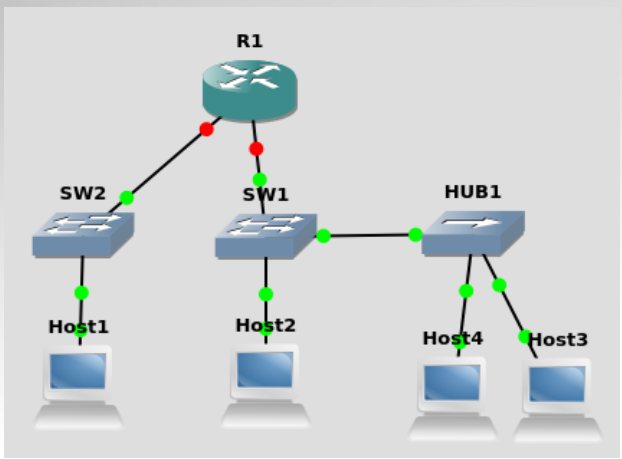
Switch:- All the nodes connected to a switch are in one broadcast domain(if and only if switchports are not assigned to different VLAN).

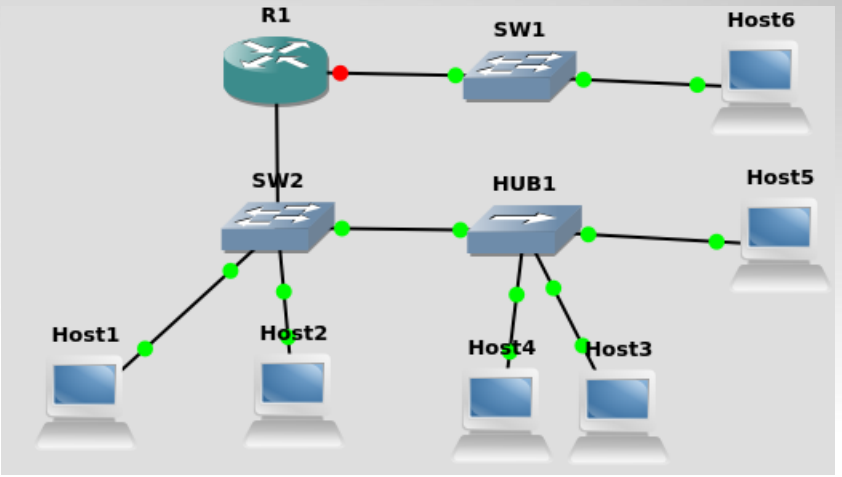
Router:- All the nodes connected to a router are in separate collision and broadcast domain.



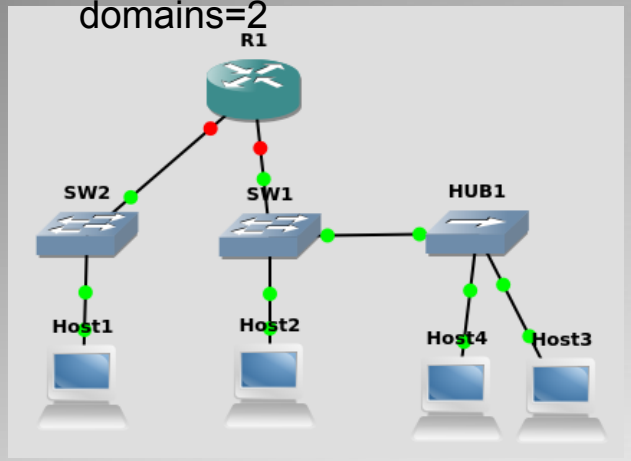
Practice questions

Identify the total no. of collision and broadcast domains in the following:-

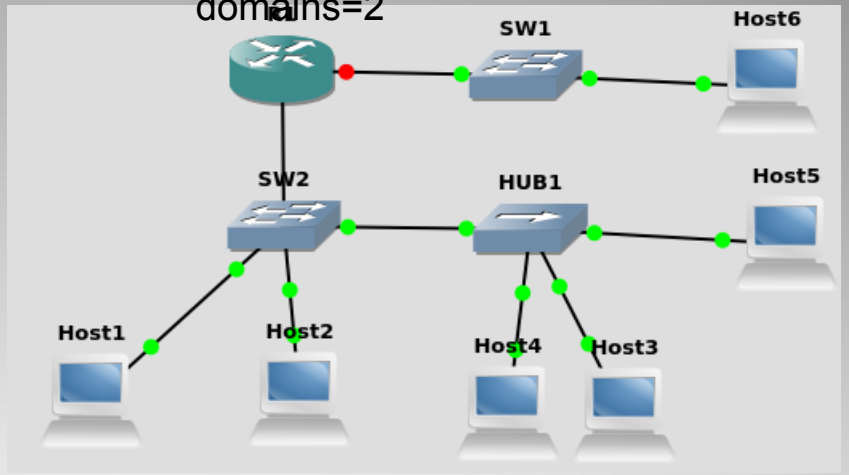


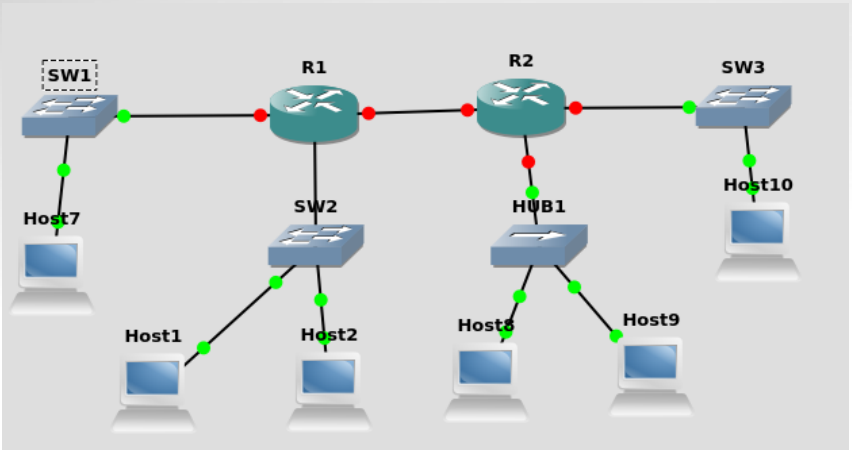


Collision domains= 5
Broadcast domains=2



Collision domains=6
Broadcast domains=2





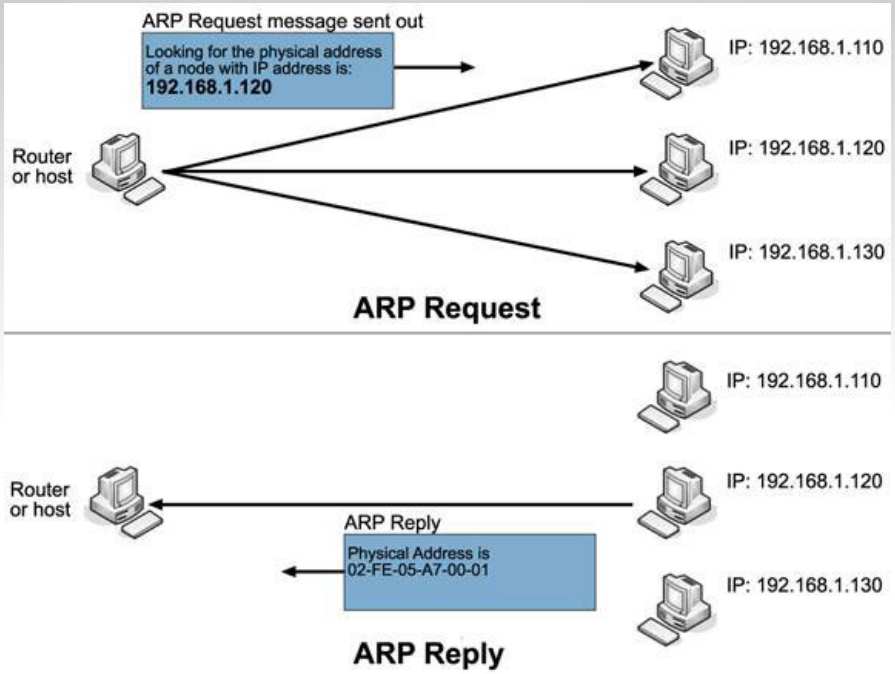
Collision domain=
Broadcast domain=

ARP

ARP

a. Host searches for ip address to MAC address mapping in its ARP cache.

b. If mapping is missing then host follows below mentioned steps.



OSI & TCP/IP Model

OSI Model(Open System Interconnection).

TCP/IP Model.

Seven Layers of OSI model.

Comparison between TCP/IP and OSI Model.

OSI & TCP/IP Model

OSI Model is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to their underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols.

TCP/IP protocol describe the movement of data between the source and destination or the internet.

Layer	Function	Example
Application (7)	Services that are used with end user applications	SMTP,
Presentation (6)	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
Session (5)	Establishes/ends connections between two hosts	NetBIOS, PPTP
Transport (4)	Responsible for the transport protocol and error handling	TCP, UDP
Network (3)	Reads the IP address form the packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the data packet	Switches
Physical (1)	Send data on to the physical wire.	Hubs, NICS, Cable

Seven Layers of OSI Model

Application Layer(7):- All the application like gmail, google, operate at application level.

Presentation Layer(6):- This is the layer where OS resides, takes care of encryption, decryption, encoding, decoding data, It takes data from application layer and hand it overs to Session Layer.

Session Layer(5):- It is responsible for creating, managing and terminating Session between local and remote machines.

Transport Layer(4):- It chops data into segments.

a. TCP(transmission control protocol):- reliable delivery of data.
b. UDP(User datagram Protocol):- Unreliable but faster delivery of data.
c. Port Number:- It identifies traffic between transport and upper layers.
d. Flow control.

Network Layer(3):- It further divides segments into packets.

a. Routing.
b. Single network interface for all the upper layer traffic.
c. Data Packets and Route update packets.
d. Devices at layer 3:- Routers, L3 Switches, Firewalls, WAN optimization devices(Silverpeak, Riverbed etc).

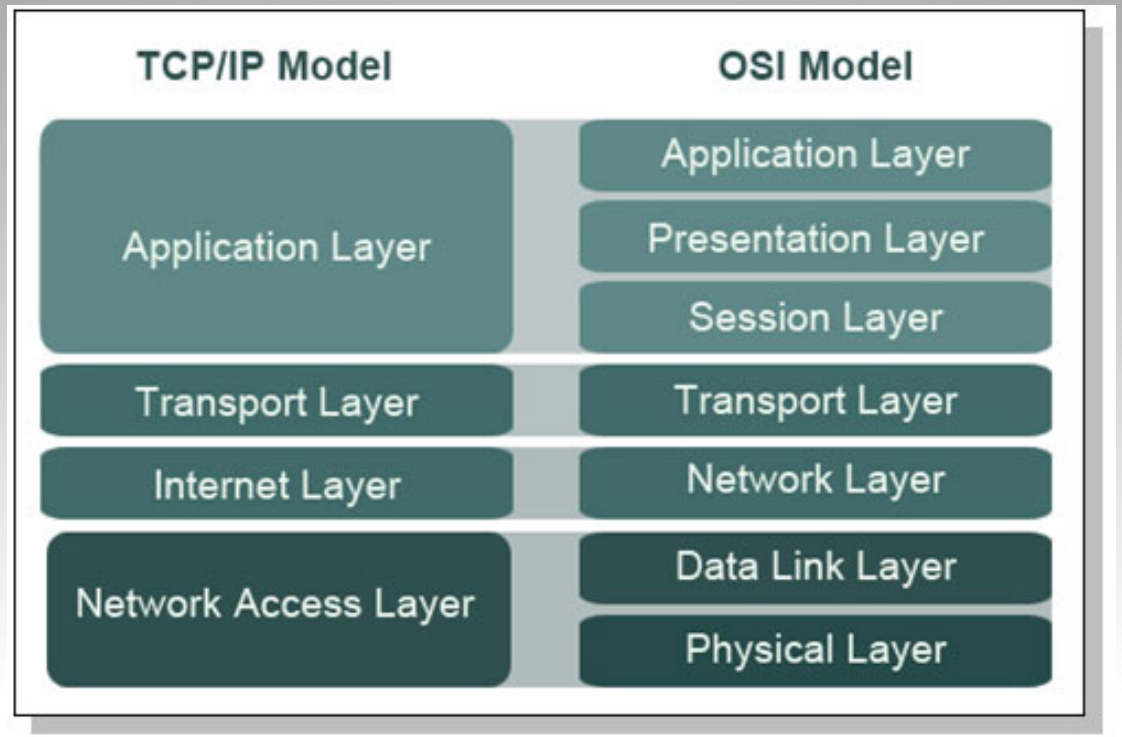
Data link layer(2):- Provides physical transmission of data based on layer 2(MAC) addresses over lan segment.

a. Formats the message into frames.
b. Performs error detection.
c. Logical Link Control(LLC) and Media Access Control(MAC).
d. Devices at Layer2:- L2 Switches, Bridges.

Physical Layer(1):- It Sends and receives bits.

a. Devices at Physical layer:- Hubs, Repeater.

Comparison between OSI & TCP/IP



Practice questions

According to TCP/IP model identify which layer the below given protocols belong to:-

1. SNMP:- simple network management protocol collects network related information.
2. HDLC:- Layer 2 encapsulation protocol, cisco proprietary.
3. UDP:- User datagram protocol(unreliable but faster delivery of data).
4. TCP:- Reliable delivery of data.
5. SMTP:-Simple mail transfer protocol, used for mail delivery.
6. PPP:- encapsulation protocol, open standard.
7. FTP:- File transfer protocol, used for transferring files.
8. IP: Internet protocol.
9. ICMP: Internet control message protocol, used for testing network connectivity.
10. IGMP: Internet group management protocol, used for management of multicast group.
11. SFTP: Secure file transfer protocol, used for transfer of files in secured way.
12. Telnet: Used for creating telnet sessions.

Answers

1. SNMP:- Application or Process layer.
2. HDLC:- Network Access layer.
3. UDP:- Transport or Host to Host layer
4. TCP:- Transport or Host to Host layer
5. SMTP:-Application or Process layer
6. PPP:- Network Access layer
7. FTP:- Application or Process layer.
8. IP: Internet layer
9. ICMP: Internet layer
10. IGMP: Internet layer
11. SFTP: Application or Process layer protocol.
12. Telnet: Application or Process layer protocol.

IP Addressing & Subnetting

IP address is software address.

Hierarchical ip addressing scheme.

a. Class A,B,C,D,E addresses.

b. Network and host addresses.

c. Reserved IP addresses.

d. Private IP addresses.

Subnetting.

a. CIDR(Classless inter-domain routing).

b. VLSM(Variable length subnet mask).

IP Address

IP address has two parts.

a. Network part.

b. Host part.

IPv4 address:-

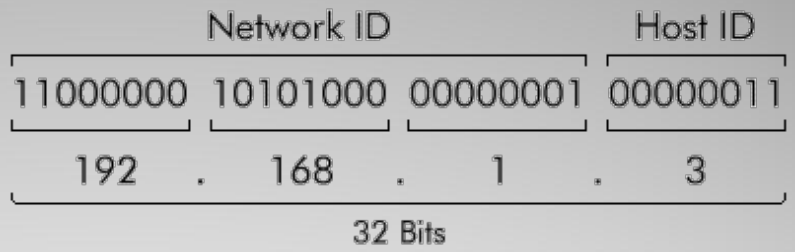
a. It is made up of 32 bits.

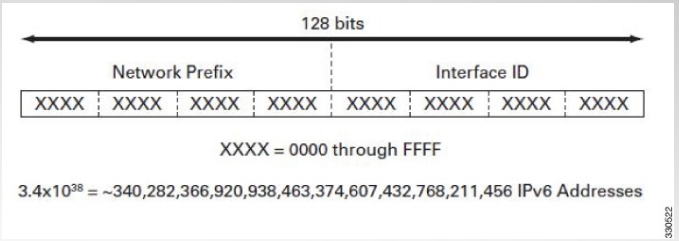
b. Represented mostly as decimal.

IPv6 address:-

a. It is made up of 128 bits.

b. Represented mostly as hexadecimal.





Hierarchical IP Addressing Scheme

IP address range: 0.0.0.0 to 255.255.255.255

IP addresses are divided into Classes.

Subnet mask:- It masks IP address so as to differentiate network bits from host bits.

Class	Subnet Mask decimal	No. of Hosts per Network	No. of Networks	Start -End Address
A	255.0.0.0	16 Million	127	1.0.0.0 - 126.255.255.255
B	255.255.0.0	65000	16000	128.0.0.0 - 191.255.255.255
C	255.255.255.0	254	2 Million	192.0.0.0 - 223.255.255.255
D	Reserved for multicast groups			224.0.0.0 - 239.255.255.255
E	Reserved for future use, or Research and Development Purposes			240.0.0.0 - 254.255.255.254

Network & Broadcast Address

Network Address:- We get Network address after turning all the host bits off(0) in an ip address.

Eg let 172.16.10.121/16, then network address=172.16.0.0

Broadcast Address:- We get broadcast address after turning all the host bit on(1) in an ip address.

Eg: Let 172.16.10.121/16, then Broadcast address=172.16.255.255.

Valid Host range:- Valid host range is the range of ip address which can be assigned to host. We get valid host range after removing network and broadcast address from total available address range.

Eg: for network 172.16.0.0/16, valid host range is 172.16.0.1 to 172.16.255.254.

Private IP address range

Private IP addresses are used inside an organization and are not routed over the internet.

Saves lot of IP addresses.

Class	Private Address Ranges
Class A	10.0.0.0 – 10.255.255.255
Class B	172.16.0.0 – 172.31.255.255
Class C	192.168.0.0 – 192.168.255.255
Loopback	127.0.0.0 – 127.255.255.255 (127.0.0.1)

Subnetting

Subnetting is process of dividing large network into small networks.

There are two ways to subnet a network

a. CIDR

b. VLSM

CIDR:- It stands for Classless Inter-Domain Routing.

Used by ISP's to allocate IP addresses to a company.

All the network have same subnet.

Eg: vodafone gives 42.10.80.0/24 to SBI.

VLSM: It stands for Variable Length Subnet Mask.

An Enterprise uses VLSM to assign IP addresses to its routers, switches, servers etc.

Depending upon the need of IP addresses network is divided into subnets.

Eg: SBI uses 42.10.80.0/30 on ISP router and core router.

Subnetting formula-es

- To find network address

ex. 172.16.10.23/21
no. of network bits=21, no of host bits=11
turn all host bit 0 in 172.16.10.23
we get 172.16.8.0

- To find broadcast address

ex. 172.16.10.23/21
turn all host bits 1 in 172.16.10.23
broadcast address=172.16.15.255

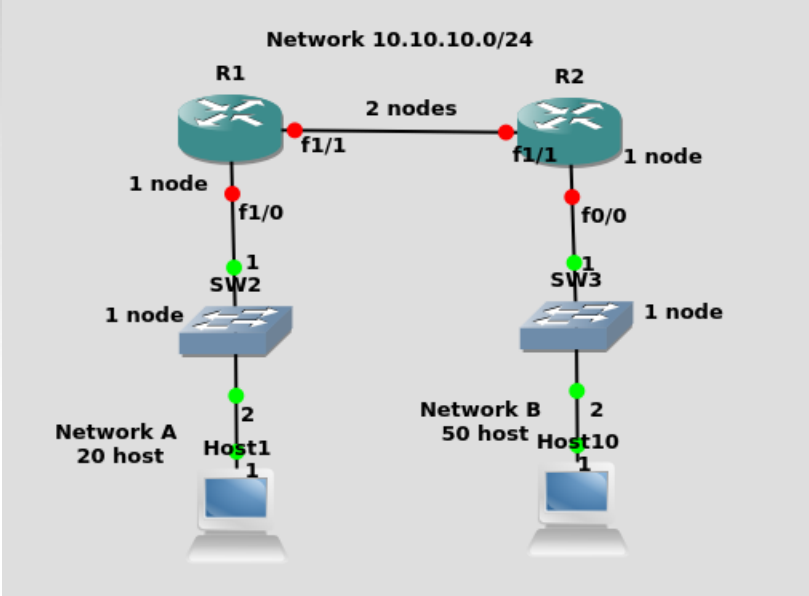
- Total no. of addresses in subnet=2h (h=total no. of host bits.)
- Total no. of valid host in subnet= 2h-2(-network address, - broadcast address)
- To find total no. of subnets

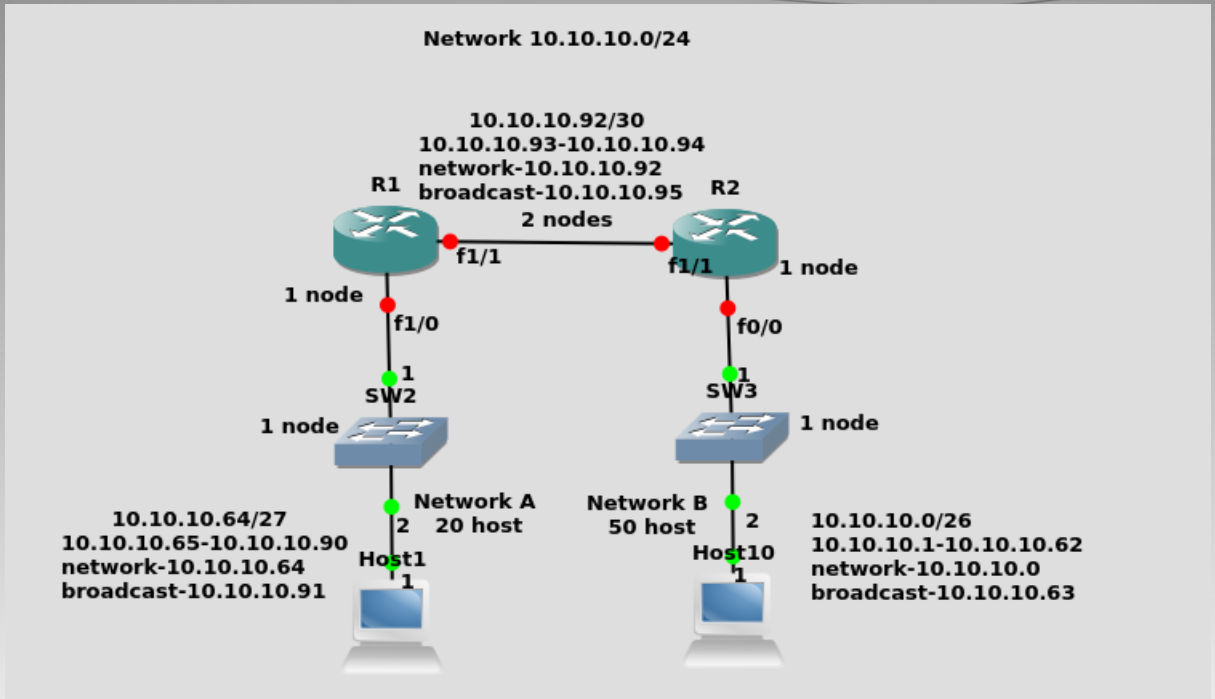
ex. 172.17.0.0/16 find total no. of subnets of block 64.
Block 64 means total no. of host bits=6 ie 26=64.
total no. of network bits=(total no. of bits – total no. of network bits(given)) - (no. Of host bits)
total no. of network bits=(32-16) – 6=10
total no. of subnets= 2n=210=1024 (n=total no. of network bits)

VLSM

In VLSM a network is given to you and you are asked to break that network into smaller networks as per the need of IP addresses.

Example 1

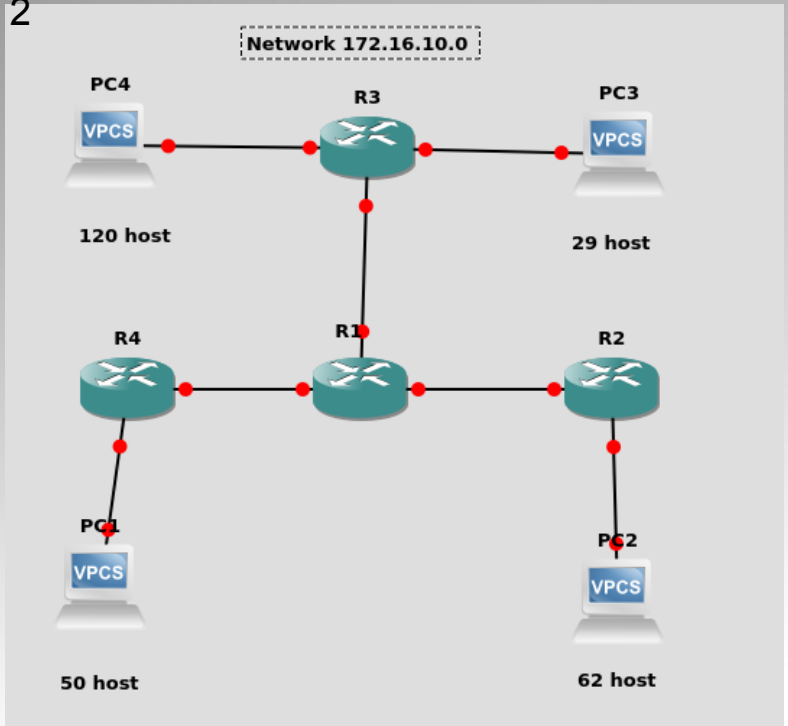




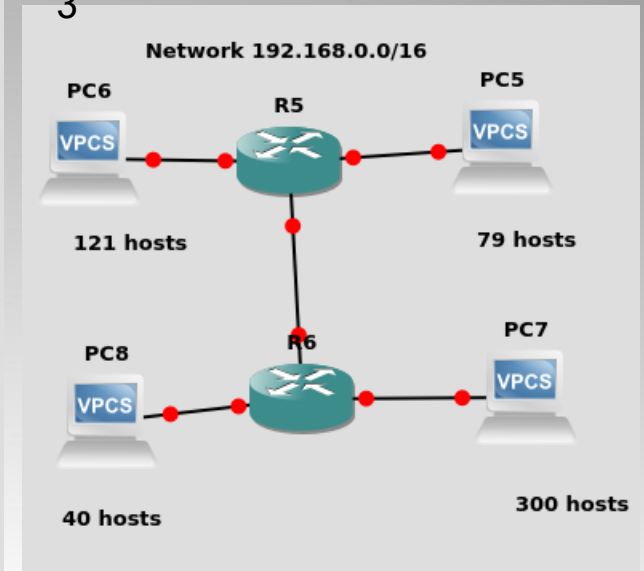
Network A
Needs 22 IP's therefore we need
Block of 32 IP's

Network B
Needs 52 IP's therefore we need
Block of 64 IP's

Example 2



Example 3



IP Routing Basics

Routing:- is a process of taking packet from one devices and sending it through network to another device on another network.

Router needs two things for packet delivery:-

a. Destination address.

b. Route till destination address.

c. Static route, default route, Dynamic route.

d. Terminology:- Administrative distance, routing loops, distance vector, link state, hybrid, hop count,

e.Loop avoidance:- split horizon, route poisoning, holddowns,

f. Routing protocols:- RIP, OSPF, EIGRP.

Static Route

Static route:- Manually adding routes in router's routing table.(AD=1).

Benifits:-

a. 0 bandwidth & 0 CPU utilization.

b. Security as only the administrator can add the routes.

Downside:-

a. Possibility of human error.

b. Whenever new network is added, route needs to be added manually on all routers.

Command syntax:- ip route [destination_network] [mask] [next-hop address or exit interface] [administrative distance] [permanent]

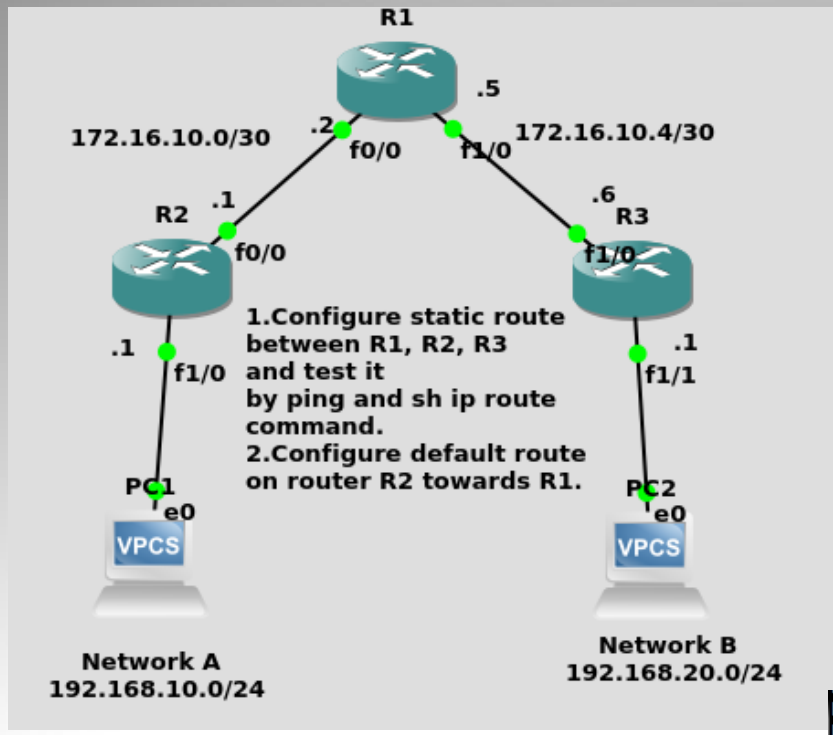
Default route:- It is type of static route.

Instead of adding a route to a specific network it tells the router to forward all packets to next hop.

It is mostly used in stub networks.

Command syntax:- ip route 0.0.0.0 0.0.0.0 [next-hop or exit interface] [administrative distance] [permanent]

Lab-Static & default route




```
R2(config)#ip route 172.16.10.4 255.255.255.252 172.16.10.2 200
R2(config)#ip route 192.168.20.0 255.255.255.252 172.16.10.2 200
R2(config)#exit
R2#wr
```

```
R1(config)#ip route 192.168.10.0 255.255.255.0 172.16.10.1 200
R1(config)#ip route 192.168.20.0 255.255.255.0 172.16.10.6 200
R1(config)#end
R1#wr
```

```
R3(config)#ip route 172.16.10.0 255.255.255.252 172.16.10.5 200
R3(config)#ip route 192.168.10.0 255.255.255.0 172.16.10.5 200
R3(config)#end
R3#wr
```

```
R2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.10.2 to network 0.0.0.0

S*    0.0.0.0/0 [150/0] via 172.16.10.2
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.16.10.0/30 is directly connected, FastEthernet0/0
L        172.16.10.1/32 is directly connected, FastEthernet0/0
S        172.16.10.4/30 [200/0] via 172.16.10.2
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, FastEthernet1/0
L        192.168.10.1/32 is directly connected, FastEthernet1/0
      192.168.20.0/30 is subnetted, 1 subnets
S        192.168.20.0 [200/0] via 172.16.10.2
```

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.10.2 150
R2(config)#
```

Dynamic Routing

Dynamic routing are of two types Internal and external.

Internal Dynamic routing:- It exists internal to an autonomous system. Eg:- RIP, OSPF, EIGRP, IGRP, IBGP.

External Dynamic routing:- It exists in-between the autonomous systems.Eg:- BGP, EGP(not in use these days).

Routing Terms

Administrative distance:- It is the trustworthiness of a route, route with least AD is preferred the most.

Autonomous system:- An AS is a collection of networks under a common administrative domain, which basically means that all routers sharing the same routing table information are in the same AS

Hop count:- It is no. of routers(L3 device) which a packet must pass to get to the destination.

Network converge:- When neighbor-ship is established between two routers and traffic can pass through it is said that network has converged.

Distance Vector routing protocol:- It finds the best path to a network on the basis of hop count.

a. Path with least hop count is preferred the most.

b. eg: RIP,RIPv2.

Cost:- path is cost=reference bandwidth/bandwidth=108/bandwidth

Link State routing protocol:- It finds the best path to a network on multiple factors like cost, bandwidth etc.

a. Path with least cost is preferred the most.

b. Makes three tables : routing table, topology table, neighbor table.

b. eg: OSPF.

Hybrid routing protocol:- It has properties of both distance vector and link state routing protocols.

a. Eg: EIGRP.

Route redistribution:- It is used to publish routes from one routing protocol to another.

eg. if we want to publish routes learnt through OSPF into BGP we will use route redistribution.

Routing loop avoidance

Routing loops:- Routing loops occur when a packet is circulated between two or more routers.

Loop avoidance:-

Max hop count:- RIP limits hop count to 15.

a. If a packet is received with hop count of 16 to a router, packet will be discarded.

Split Horizon:- It restricts router from advertising the route out of the interface from where it had first learned the route.

Route Poisoning:- Advertising the route to unreachable network with infinite hop count.

a. If link to network goes down then router attached to that network will advertise route to that network with hop count of infinity.

b. This tells other routers that the specified network is not reachable.

RIPv2

True Distance vector.

Sends complete routing table out of all active interfaces every 30 seconds.

Uses hop count to find best path.

Max hop count=15.

RIPv1 uses only classful routing that is all the network must use the same subnet mask.

RIP timers:-

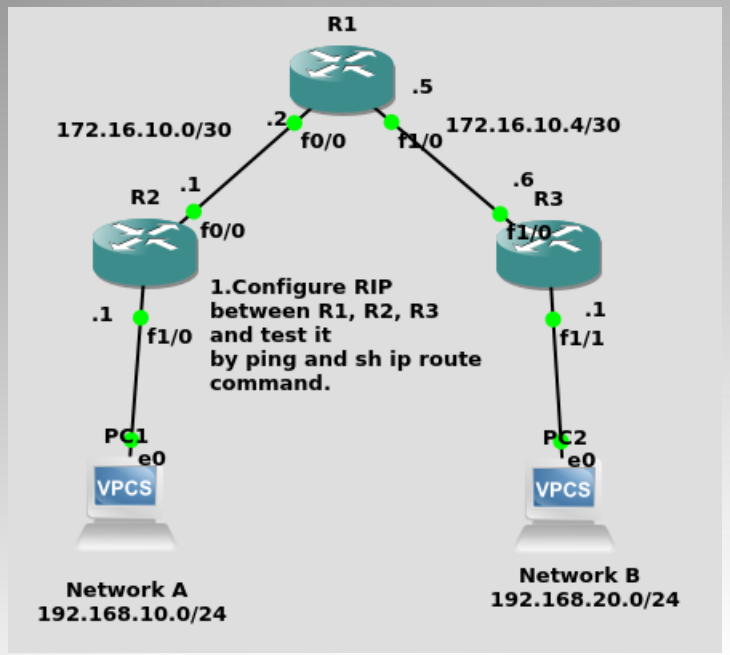
a. Route update timer:- time period after which complete routing update is sent(default is 30 sec)

b. Route invalid timer:- timer period after which a route becomes invalid, if no update is received containing that route(default is 180 sec)

c. Holddown timer:- routing information is suppressed during holddown. A route enters a holddown when that route is received with unreachable hop count.(default is 180 Sec)

d. Route flush timer:- Time period between route becoming invalid and route getting removed from routing table.(default is 240 sec)

Lab-RIP




```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 172.16.10.4
R3(config-router)#network 192.168.20.0
R3(config-router)#end
R3#wr
```

```
R2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.10.2 to network 0.0.0.0

S*    0.0.0.0/0 [150/0] via 172.16.10.2
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.16.10.0/30 is directly connected, FastEthernet0/0
L        172.16.10.1/32 is directly connected, FastEthernet0/0
R        172.16.10.4/30 [120/1] via 172.16.10.2, 00:00:07, FastEthernet0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, FastEthernet1/0
L        192.168.10.1/32 is directly connected, FastEthernet1/0
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
R        192.168.20.0/24 [120/2] via 172.16.10.2, 00:00:07, FastEthernet0/0
S        192.168.20.0/30 [200/0] via 172.16.10.2
```

```
R2(config)#router rip
R2(config-router)#ver
R2(config-router)#version 2
R2(config-router)#network 172.16.10.0
R2(config-router)#network 192.168.10.0
R2(config-router)#end
R2#wr
```

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 172.16.10.0
R1(config-router)#network 172.16.10.4
R1(config-router)#end
R1#wr
```

EIGRP

Hybrid(Advanced distance vector) routing protocol.(AD=90)

It sends complete routing table when the neighborship is established and then sends update of specific routes only when a change occurs in topology.

Uses metric(bandwidth, delay, load, reliability and MTU) for choosing best path.

Max hop count=255.

Uses DUAL(diffusion update algorithm) to select and maintain best path to different network.

EIGRP terms:-

a. Feasible distance(FD):- Metric of best path to a network.

b. Reported/advertised distance:- Metric of a remote network reported by a neighbor.

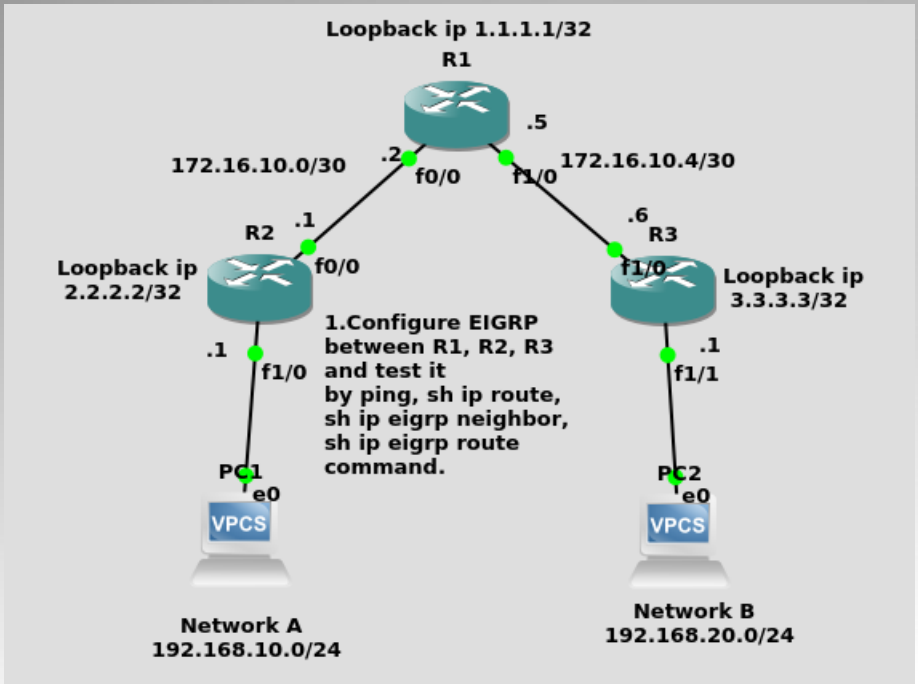
c. Feasible successor:- Route whose reported distance is less than FD, EIGRP keeps 6 feasible successor in topology table.

d. Neighbor table:- all the neighbor related information

e. Topology table:- contains all the known routes to all the known destination.

f. routing table:- route with best metric from topology table is entered into routing table.

Lab- EIGRP




```
R2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.10.2 to network 0.0.0.0

S*    0.0.0.0/0 [150/0] via 172.16.10.2
      2.0.0.0/32 is subnetted, 1 subnets
C        2.2.2.2 is directly connected, Loopback0
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.16.10.0/30 is directly connected, FastEthernet0/0
L        172.16.10.1/32 is directly connected, FastEthernet0/0
D        172.16.10.4/30 [90/30720] via 172.16.10.2, 00:02:31, FastEthernet0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, FastEthernet1/0
L        192.168.10.1/32 is directly connected, FastEthernet1/0
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
D        192.168.20.0/24 [90/33280] via 172.16.10.2, 00:01:20, FastEthernet0/0
S        192.168.20.0/30 [200/0] via 172.16.10.2
R2#sh ip eigrp nei
R2#sh ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   172.16.10.2             Fa0/0                    12 00:02:37   50   300  0  7
```

```
R2(config)#router eigrp 1
R2(config-router)#network 192.168.10.0 0.0.0.255
R2(config-router)#network 172.16.10.0 0.0.0.3
R2(config-router)#end
R2#wr
```

```
R1(config)#router eigrp 1
R1(config-router)#network 172.16.10.4 0.0.0.3
R1(config-router)#network 172.16.10.0 0.0.0.3
R1(config-router)#end
R1#wr
```

OSPF

True link state routing protocol.

Uses cost as metric for calculation best path.

Cost = reference bandwidth(108)/bandwidth.

Uses Dijkstra algorithm for finding and maintaining best paths to all the networks.

Supports multiple equal cost routes.

Consists of Area and Autonomous systems.

OSPF Terms:-

a. Link:- link is a network or router interface assigned to any given network.

b. Router ID:- ip address used to identify the router.

c. Link state database(LSA):- An OSPF data packet containing link state or routing information.

d. Designated router(DR):- A DR exchanges LSA's between non DR routers, two non DR routers don't exchange LSA with each other directly, DR is selected over multi-access(broadcast) network like ethernet.

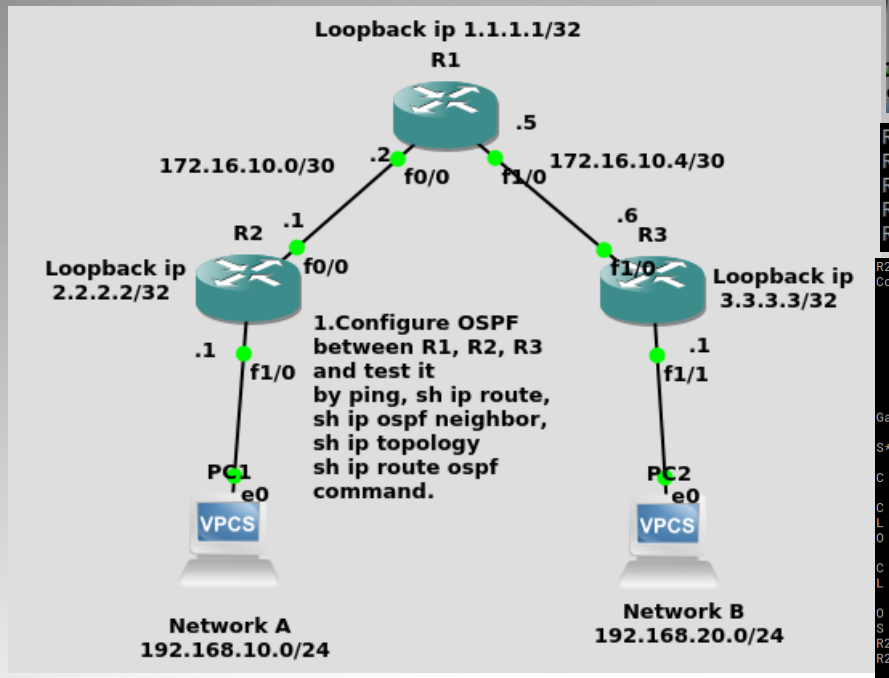
e. Backup Designated router(BDR):- backup router for DR.

f. OSPF areas:- OSPF topology is divided into areas where area 0 is called backbone area and all other area's must be connected to backbone area.

g. Area boundary router(ABR):- a router which has interfaces configured in more than one area is called ABR.

h. Autonomous system boundary router(ASBR):- a router which has interfaces configured in more that one AS.

Lab- OSPF




```
R2(config)#router ospf 2
R2(config-router)#network 172.16.10.0 0.0.0.3 area 0
R2(config-router)#network 192.168.10.0 0.0.0.255 area 0
R2(config-router)#end
R2#wr
```

```
R3(config)#router ospf 3
R3(config-router)#network
R3(config-router)#network 192.168.20.0 0.0.0.255 area 0
R3(config-router)#network 172.16.10.4 0.0.0.3 area 0
R3(config-router)#en
```

```
R2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.10.2 to network 0.0.0.0

S*    0.0.0.0/0 [150/0] via 172.16.10.2
      2.0.0.0/32 is subnetted, 1 subnets
C        2.2.2.2 is directly connected, Loopback0
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.16.10.0/30 is directly connected, FastEthernet0/0
L        172.16.10.1/32 is directly connected, FastEthernet0/0
O        172.16.10.4/30 [110/2] via 172.16.10.2, 00:07:30, FastEthernet0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, FastEthernet1/0
L        192.168.10.1/32 is directly connected, FastEthernet1/0
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
O        192.168.20.0/24 [110/3] via 172.16.10.2, 00:00:45, FastEthernet0/0
S        192.168.20.0/30 [200/0] via 172.16.10.2
R2#sh ip ospf nei
R2#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/BDR        00:00:29    172.16.10.2     FastEthernet0/0
```

```
R1(config)#router ospf 1
R1(config-router)#network 172.16.10.0 0.0.0.3 area 0
R1(config-router)#networ
*Jan 16 23:27:59.815: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on FastEthernet0/0 from LOADING to FULL, Loading Done
R1(config-router)#network 172.16.10.4 0.0.0.3 area 0
R1(config-router)#end
R1#wr
```

Switching Basics & STP

Switch function:- Address learning, Forward/filter decision, loop avoidance.

STP.

Port security.

VLAN.

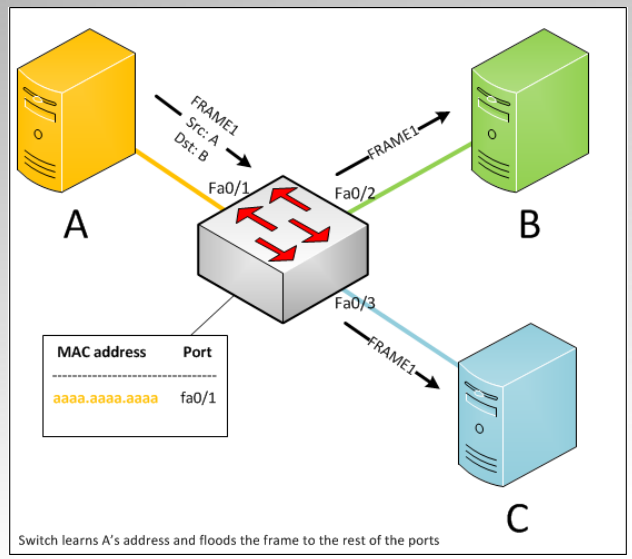
Inter-VLAN routing(router on stick and SVI).

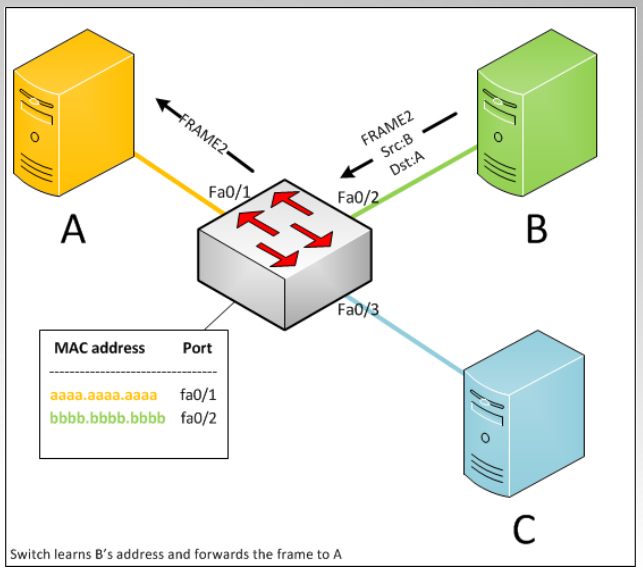
Switch stacking, cascading and clustering.

Tracing MAC address.

Switch function

Address learning:-





- Forward/Filtering decision:-

a. Flooding:- a switch floods the frame out of all the ports except the ingress port when destination mac is unknown via unknown unicast flooding.

b. Forwarding:- a switch forwards a frame when destination mac is know.

c. Filtering:- a switch filters a frame when both source and destination mac are on the same port(when hub is connected to switch).

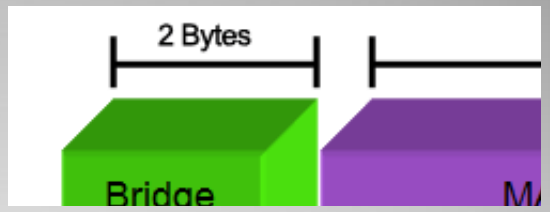
- Loop Avoidance:- Switches use STP for loop avoidance.

Spanning Tree Protocol

When more than 2 switches are connected to each other for redundancy, it can cause loops.

To avoid looping at layer 2 STP is used.

STP terms:-



a. Bridge ID:- switch with lowest bridge id becomes root bridge.

b. Root Bridge:- Focal point of network. All the packets has to pass through root bridge.

c. BPDU:- Bridge Protocol Data Unit are packets containing information about switches which help in selecting root bridge and other such information.

d. Port Cost:- It determines the best path when multiple paths are available and non of the links are root port.

e. Root Port:- Link or switchport directly connected to root bridge.

f. designated port:- Port having the best cost, it is marked as forwarding port.

g. Non-designated port:- Port having higher cost, it is put in blocked state.

- STP 802.1d:- creates 1 spanning tree instance for entire switch irrespective of VLANS.
- Spanning tree port states:-

a. Blocking:- a blocked port does not forward frames.

b. Listening:- listens to BPDU and prepares to forward frames without populating MAC address table.

c. learning:- listens to BPDU, prepares to forward frames, also populates MAC address table.

d. forwarding:- forwards frames.

e. disabled:-(administrative) a port in disabled state does not participate in STP and does not forward frames.

PVST & PVST+

- PVST:- Per VLAN spanning tree protocol.

a. It is cisco proprietary.

b. It is same as STP 802.1d but offers spanning tree per VLAN.

- c. Load balances the traffic.
- RSTP(802.1w):- Rapid spanning tree protocol.
- Achieves faster convergence than STP.
- RSTP port state:-

a. Discarding.

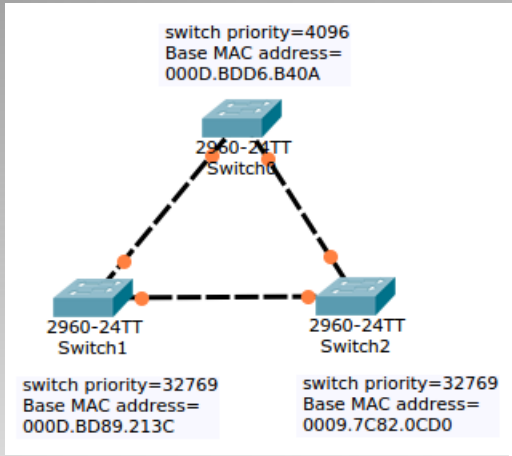
b. Learning.

c. Forwarding.

- PVST+: Per VLAN spanning tree protocol plus.

a. Same as PVST but achieves faster convergence.

Lab- STP

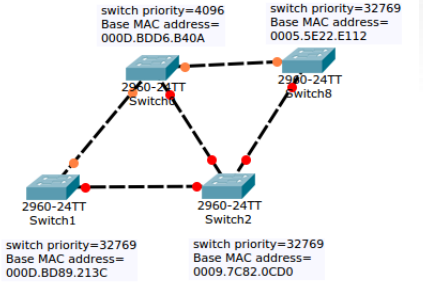



```
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
             Address     000D.BDD6.B40A
             Cost        19
             Port        2(FastEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0009.7C82.0CD0
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

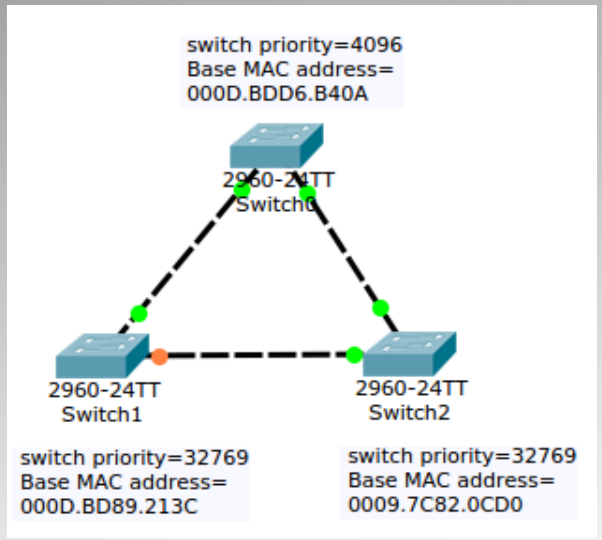
```
Switch(config)#spanning-tree vlan 1 priority 4096
Switch(config)#end
Switch#
```

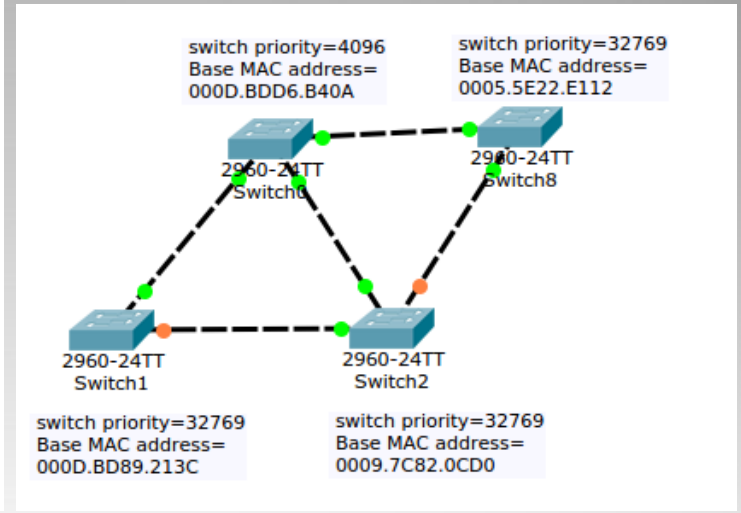



```
Switch#show spanning-tree summary
Switch is in pvst mode
Root bridge for: default
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
VLAN0001                    0         0        0          2          2

-------------------- -------- --------- -------- ---------- ----------
1 vlans                     0         0        0          2          2
```


switch priority=4096
Base MAC address=
000D.BDD6.B40A
2960-24TT
Switch0
2960-24TT
Switch1
2960-24TT
Switch2
switch priority=32769
Base MAC address=
000D.BD89.213C
switch priority=32769
Base MAC address=
0009.7C82.0CD0


switch priority=4096
Base MAC address=
000D.BDD6.B40A
switch priority=32769
Base MAC address=
0005.5E22.E112
2960-24TT
Switch0
2960-24TT
Switch8
2960-24TT
Switch1
2960-24TT
Switch2
switch priority=32769
Base MAC address=
000D.BD89.213C
switch priority=32769
Base MAC address=
0009.7C82.0CD0

Port Security

Port Security allows to set policy on the following:-

Number of MAC address dynamically assigned to switchport.

Set a static MAC address on a switchport.

Set penalties if above policies are broken.

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int range fa0/3 - 4
S1(config-if-range)#switchport port-security maximum ?
  <1-8192>  Maximum addresses
S1(config-if-range)#switchport port-security maximum 1
S1(config-if-range)#switchport port-security mac-address sticky
S1(config-if-range)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
S1(config-if-range)#switchport port-security violation shutdown
S1(config-if-range)#exit
```

VLAN

Virtual LAN is a broadcast domain that is partitioned at data link layer.

Switches break the broadcast domain by creating VLAN.

Network nodes in different VLAN need Inter-vlan routing to communicate with each other.

Switchport modes

Access:- Allow transfer of packets of 1 VLAN.

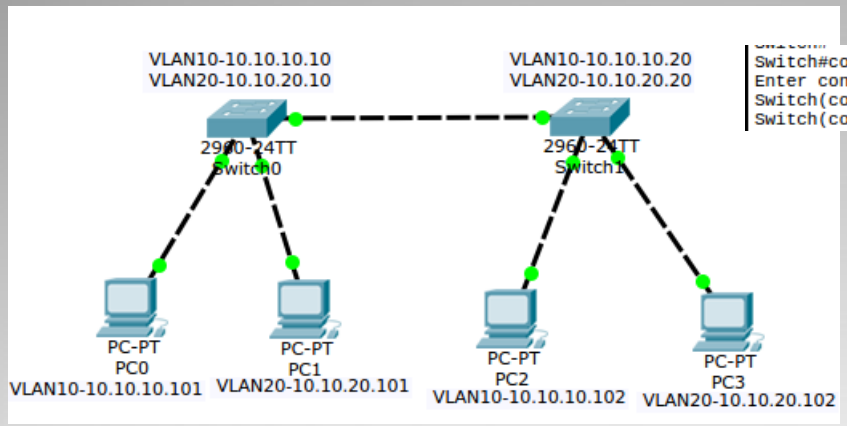
Trunk:- Allows transfer of packets of all the allowed VLAN's.

Dynamic:-

a. Auto:- Becomes trunk if the opposite switchport is trunk or dynamic desirable.

b. Desirable:- Becomes trunk if the opposite switchport is trunk, dynamic desirable or auto.

Lab-VLAN




```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#exit
```

```
Switch(config)#int fa0/2
Switch(config-if)#swi
Switch(config-if)#switchport mode access
Switch(config-if)#swi
Switch(config-if)#switchport access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#spanni
Switch(config-if)#spanning-tree port
Switch(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/2 but will only
have effect when the interface is in a non-trunking mode.
Switch(config-if)#exit
```

```
Switch#conf t
Enter configuration commands, one per line.  End with C
Switch(config)#int fa0/1
Switch(config-if)#swi
Switch(config-if)#switchport mode
Switch(config-if)#switchport mode trun
Switch(config-if)#switchport mode trunk
Switch(config-if)#swi
Switch(config-if)#switchport trun
Switch(config-if)#switchport trunk all
Switch(config-if)#switchport trunk allowed vlan
Switch(config-if)#switchport trunk allowed vlan all
Switch(config-if)#end
Switch#
```

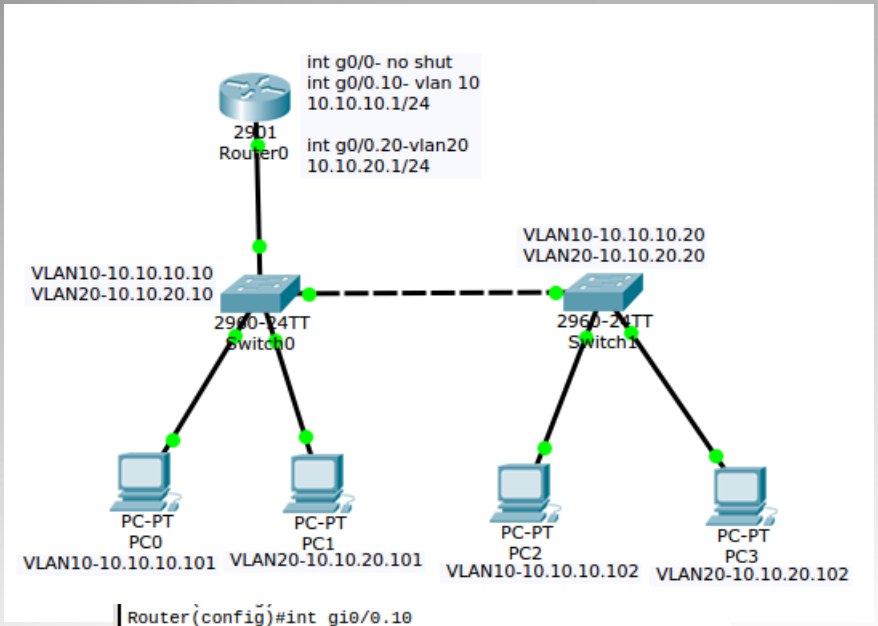
Inter-vlan routing

IVR is performed in two ways

a. using router on stick.

b. using switched virtual interface(SVI).

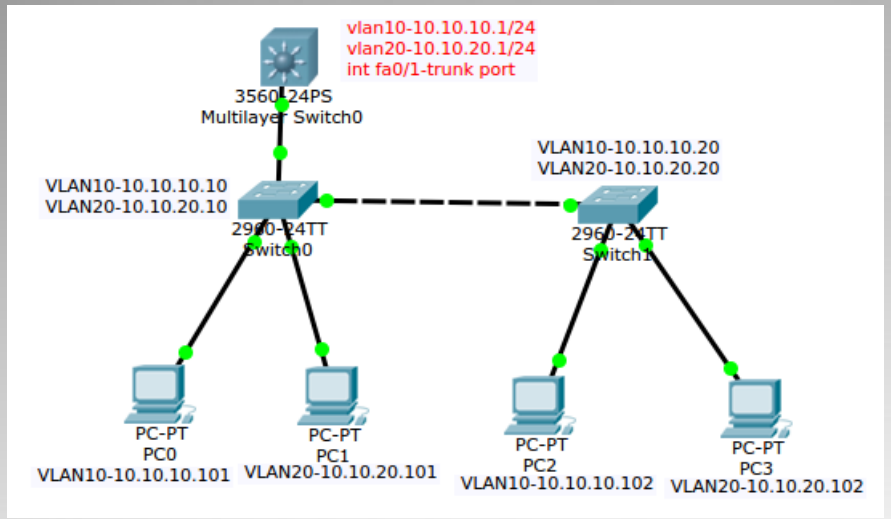
Router on stick




```
Router(config)#int gi0/0.10
Router(config-subif)#enc
Router(config-subif)#encapsulation dot
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip addd
Router(config-subif)#ip add
Router(config-subif)#ip address 10.10.10.1 255.255.255.0
Router(config-subif)#no shut
Router(config-subif)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
```

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gi0/0
Router(config-if)#no shut
Router(config-if)#no ip address
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
```

Switched Virtual Interface




```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#int vlan 10
Switch(config-if)#ip add
Switch(config-if)#ip address 10.10.10.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#vlan 20
Switch(config-vlan)#exit
Switch(config)#int vlan 20
Switch(config-if)#ip add
Switch(config-if)#ip address 10.10.20.1 255.255.255.0
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
```

Ip routing should be Enabled on L3 switch For SVI- intervlan routing.

Switch cascade, stack & cluster

Switch Cascade:- Adding a new switch when existing switch runs out of port is called cascading.

Switch Stacking

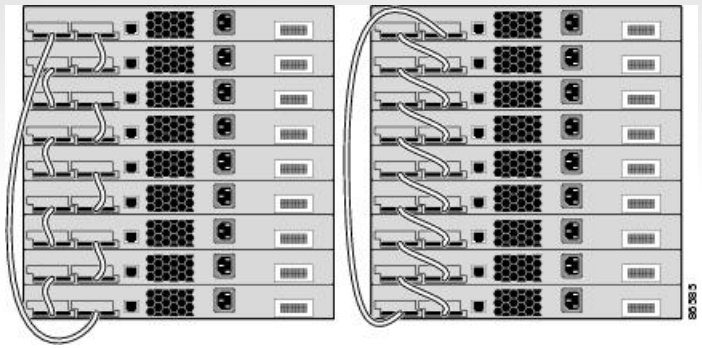
a. All the switches in a stack share one IP address.

b. Only one switch in a stack is elected Master, all other switches become slave.

c. Switch with highest priority becomes Master switch.

d. Priority range: 1 to 15.

e. Total no. of switches in a stack is 8.



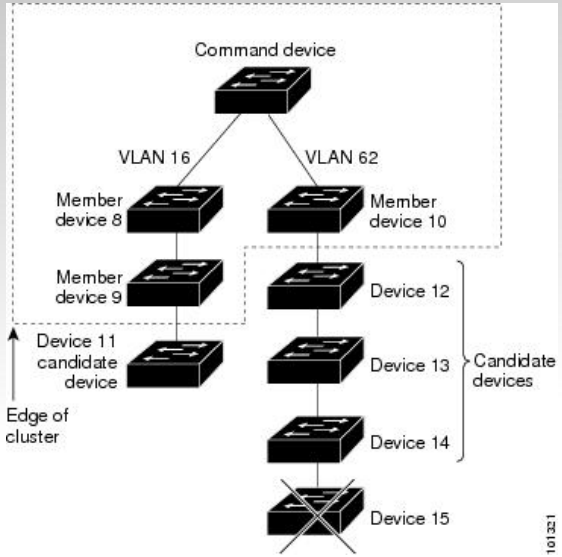
Switch Cluster:-

a. All the switches in a cluster share the ip address of command switch.

b. One switch is configured command switch, one as standby cluster command switch and all other switches as member switches.

c. Total no. of switches in a cluster cannot exceed 16.

d. All the switches must be cluster capable and CDP version 2 should be enabled to be a part of cluster



Tracing mac address:-

a. When switch ip is known to which host is connected.

Command:- show mac address-table address [mac-address of host]

to find mac address of host use:- show ip arp [ip address of host].

b. When switch ip is not known, log into core switch and execute following command.

Command:- traceroute mac [mac-address of host] [mac-address of host]

Note: option b will not work in nexus switches.

Network Cabling

Common network cable types.

Cat 5 cable.

Fiber cable.

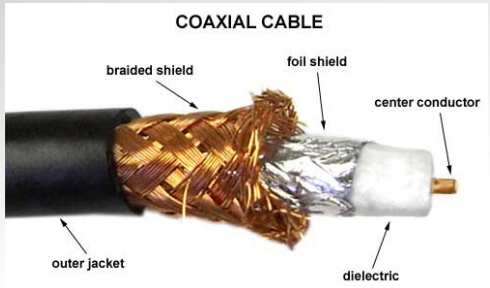
Straight and cross cables.

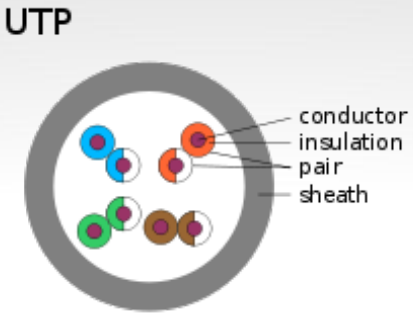
Common network cable types

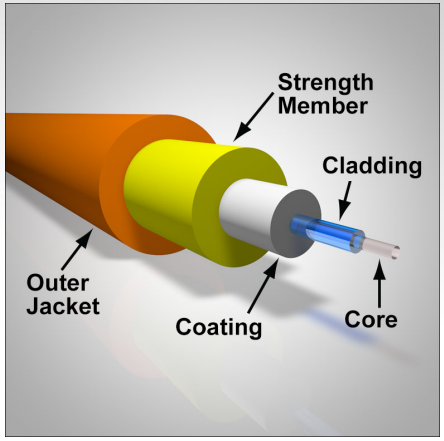
- Coaxial cable:-Coaxial cable is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield.
- Unshielded twisted pair(UTP) cable:-

Mostly used in computer networking due to lower cost compared to optical fiber and coaxial cable.

- Optical fiber:- An optical fiber cable is a cable containing one or more optical fibers that are used to carry light signals.







UTP categories

Category	Description
Category 1	Voice only(Telephone)
Category 2	Data to 4 Mbps(Localtalk)
Category 3	Data to 10 Mbps(Ethernet)
Category 4	Data to 10 Mbps(Token ring)
Category 5 Category 5e	Data to 100 Mbps(Fast Ethernet) Data to 1000 Mbps(Gigabit Ethernet)
Category 6	Data to 2500 Mbps(Gigabit Ethernet)

Category 5e

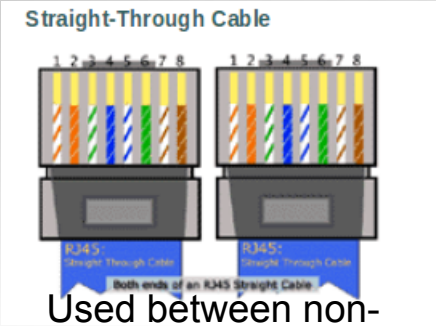
- 1000Mbps data capacity
- For runs of up to 90 meters
- Solid core cable ideal for structural installations (PVC or Plenum)
- Stranded cable ideal for patch cables
- Terminated with RJ-45 connectors

Straight & Cross cable

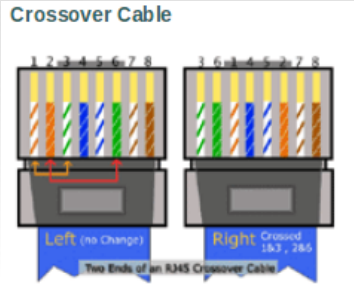
Straight Cable:- A straight-through cable contains colored wires in the same sequence at both ends of the cable.

Cross-over Cable:- A crossover cable has four colored wires that are in reverse sequence on each end of the cable.

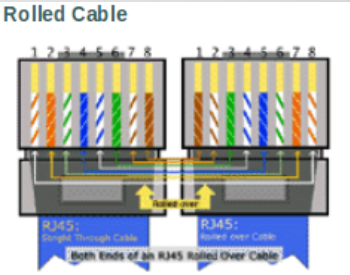
Rolled Cable:- A rolled cable contains wires that are in reverse sequence at each end of the cable



Used between non-similar devices
Like pc and switch, switch and router.



Used between similar
Devices like switch
And switch, router
and
Router, router and pc.



Used to configure
CISCO
Routers and switches.

WAN Technology

Basics of ISDN.

Basics of Frame Relay.

Basics of PPP.

Basics of ISDN

- Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network.
- Circuit Switched:- A network communication in which end to end dedicated connection is established before transferring data. Eg:- ISDN.
- Packet switched:- A network communication in which data is divided into packets and then packets are transferred from source to destination. Eg:- Frame relay, IP.
- Basic Rate Interface(BRI):- a 128 kbit/s service delivered over a pair of standard telephone copper wires

a. It consist of 2B(bearer channel for voice) 1D(data channel for data/control signal).

Primary Rate Interface(PRI):-

PRI is a telecommunications interface standard used on an Integrated Services Digital Network (ISDN) for carrying multiple DS0 voice and data transmissions between the network and a user.

It is based on the T-carrier (T1) line in the US and Canada, and the E-carrier (E1) line in Europe.

T1 lines:-

Consist of 24 Channels= 23B+1D.

Data transfer speed=1.544Mbit/sec.

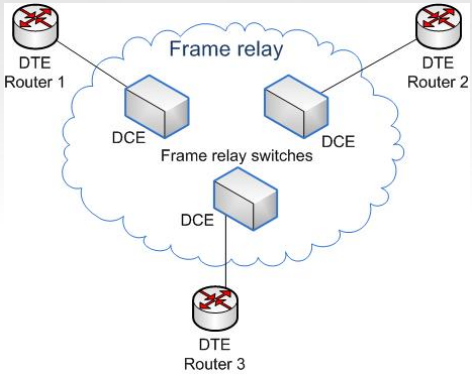
E1 lines:-

Consist of 32 Channels= 30B+1D+1timeslot(0)(for synchronization)

Data transfer speed=2.048Mbit/sec

Basics of Frame Relay

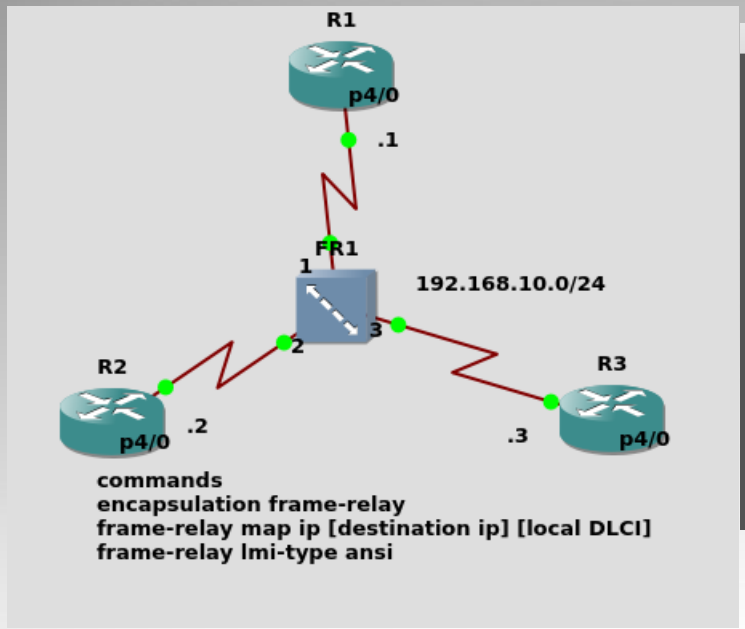
- Frame Relay is packet switched WAN technology.
- It is a Non-Broadcast Multi Access network.
- It is cost effective.
- Frame relay operate by creating virtual circuits(permanent virtual circuits).

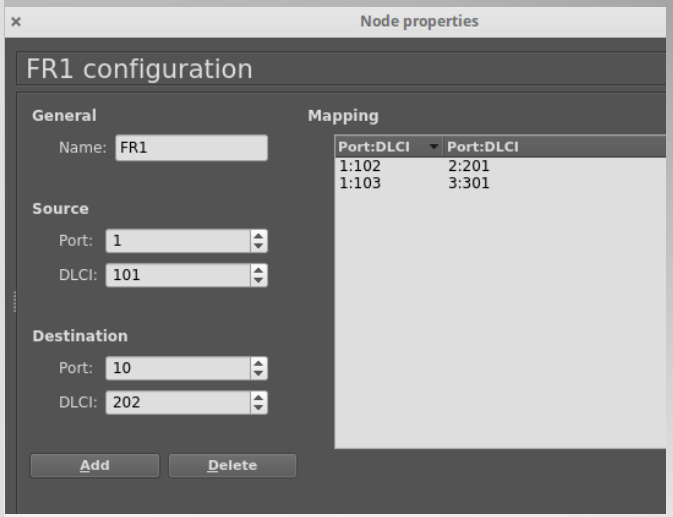


Frame Relay Terms

- Committed Information Rate:- The maximum bandwidth of data guaranteed to be delivered. In reality, it's the average amount that the service provider will allow you to transmit.
- Access Rate:- The maximum speed at which the Frame Relay interface can transmit.
- PVC(Permanent Virtual Circuit):- It is always present whether data is being transferred or not.
- DLCI(Data link connection identifiers:- DLCI is used to distinguish one PVC from another.
- LMI(Local management interface):- LMI is signaling standard used to communicate frame relay related data(like status of virtual circuits, keepalives etc) between router and frame relay switch.

Lab-Frame Relay





Introduction to PPP

- PPP(Point to Point Protocol) is a data link protocol used over asynchronous serial(dial up) or synchronous serial(ISDN).
- It is open standard.
- It is used to transfer Layer 3 packets across a Data link layer point to point link
- It can encapsulate IP, IPX, appletalk.
- LCP:- A method of establishing, configuring, maintaining, and terminating the point-to-point connection.
- NCP:- A method of establishing and configuring different Network layer protocols.
- PAP:- Password authentication protocol to authenticate PPP connection.

a. passwords are sent in clear text.

b. only performed at the initial link establishment.

- CHAP:- Challenge Handshake authentication protocol to authenticate PPP connection

a. Handshake is performed using MD5 hash function.

b. performed at initial link establishment and periodically.

PPP session establishment

Link establishment phase:-

LCP packets are sent by each PPP device to configure and test the link.

Authentication Phase:-

PAP or CHAP is used to authenticate the link.

Network layer protocol phase:-

PPP uses NCP to allow multiple network layer protocols to be encapsulated and sent over PPP data link.

Lab-PPP

configure ppp

commands
username [hostname of peer] password [same on both ends]
encapsulation ppp
ppp authentication chap pap