SWTICH:

RAN – Running conf

NVRAM – startup conf

Flash – Image OS

Repeater – in a network we can have maximum 4 repeaters . (Satellite communication)

DCE – communication

DTE- transmission

* There are two types of protocols:

1. Routed protocols
2. Routing protocols

**Three types of routing**

1. Static routing – where n/w administrator determines the path for data transmission.
2. Dynamic routing – where path is determines using no. of routing algorithms. RIP (Routing information protocol), OSPF (Open shortest path first), IGRP (Interior), EIGRP (Enhanced Interior), BGP, IS-IS (Intermediate system to intermediate system)

Algorithms are:

1. Distance vector algorithm
2. Link state algorithm
3. Default routing -

**Syntax for static routing:**

* Ip route <destination ip address> <subnet mask> <next hop address> or <exit interface id> <Administrative Distance (provides the measure for reliability)>
* By default value of the administrative distance is 0 when we are giving the next hop address and value is 1 when we are selecting exit interface id

**ROUTING INFORMATION PROTOCOL(Routing by rumors)**

**Algorithms are:**

* Dijksha’s algo (Link state algo) – recreating the nw topology whenever we add a router or remove
* Bellman ford algorithm (Distance vector algo )
* Metric – no. of hops

Maximum hops can be 15 i.e 0 to 15

Convergency rate = updation in a nw

Every **30 seconds** hello packets are sent from one router to another. If router doesn’t respond to hello packets then previous router will send packet till 180 seconds.(hold on timer)

“” 240 seconds (flush down timer)

After 240 seconds if no response then consider the router is inactive and flushes the database.

Disadvantages:

Low convergency rate

Metric

RIP Version:

Version 1: - does not support subnetting

Version 2: - classless routing protocol

Syntax:

* **Router rip**
* **Version 2**
* **Network <source network id 1>**
* **Network <source network id 1>**
* **no auto summary**

**OPEN SHORTEST PATH FIRST**

It uses link state algorithm to determine the best path for data transmission. Also called as SPF.

Metric – bandwidth (cost is interface bandwidth between source and destination by overall autonomous system bandwidth) and hop count.

Maximum hops counts are 255 hops and convergency rate is 10 seconds

**Routing table, topology table and adjacency table** is shared within network if there is a reply. It is stored on the backbone area i.e Area 0. in link state DB. Backbone area is the area where 2 or more routers are connected directly or indirectly to the entire routers. The router which is directly connected to the Area 0 router is Designated router and which is indirectly connected through Designated router is called as backup designated router.

Every **10 seconds** hello packet has been sends. And same as RIP

Syntax for OSFP:

* **router ospf <process id>**
* **network <src network id>**
* **network <src network id > <inverse mask> area <id>**

**IGRP**

Metric – cost, delay and hop count is max 225

Convergency – 90 seconds

It uses Routing table, tt, neighbor table.   
It supports CIDR

**EIGRP**

Metric – cost, delay and hop count is max 225

Convergency – 5 seconds

It uses Routing table, tt, neighbor table. It also supports classful routing.

It uses adavanced algo i.e DUAL (Defuasing update algorithm )

Syntax :

* **router eigrp <as no>**
* **network <source network id>**
* **no auto summary**

**ACCESS CONTROL LIST**

**Applying set of permission over routers interface to control the incoming and outgoing traffic. ACL can be only applied on the interface of the router. Every ACL has a denial statement which is accompanied by a permit statement.**

**Two categories:**

1. **Standard ACL’s –** This are traditional ACL’s where the permission or ACL is applied on the destination end using the source address.

It can be used for blocking all the service and block a particular host or entire subnet.

ACL id range is 1 to 99 and extended range is 1300 to 1999.

Standard ACL blocks the two way communication.

1. **Extended ACL’s –** uses both source and destination address and can be applied on both source and destination end. It can be used for blocking particular service, port number or any ip address. ACL id range is 100-199 and extended range is 2000 to 2999.

Extended ACL blocks the one way communication.

1. **Named ACL**: which is extended version of the extended ACL where instead of using the ACL id here we will used a name.

**Syntax for standard:**

* #ip access-list standard id
* #deny <ip add> <wild cad mask> **OR**
* #deny host <ip add>
* #permit any
* ASSIGNING TO A INTERFACE
* #interface <serial> OR <fa0/0>
* Ip access-group <acl id> in/out

**Syntax for extended:**

* #ip access-list extended id
* #deny ip <source ip add> <wild cad mask> <destn ip add> <wild cad mask> **OR**
* #deny ip host <source ip add> host <destn ip add>
* #permit ip any
* ASSIGNING TO A INTERFACE
* #interface <serial> OR <fa0/0>
* Ip access-group <acl id> in/out

**EIGRP TO RIP**

* Router rip
* Redistribute eigrp <as no> metric <hop count>
* Eg. Redistribute eigrp 1 metric 5

**RIP to EIGRP**

* Router eigrp <as no>
* Redistribute rip metric <bandwidth> <delay> <reliability> <bandwidth loading> <MTU>
* Eg. Router eigrp 1
* Redistribute rip metric ?
* Redistribute rip metric 10000 10 255 100 1000

**OSPF to RIP**

* Router rip
* Redistribute ospf <process id> metric <hop count>
* Eg. Redistribute ospf 10 metric 5

**RIP to OSPF**

* Router ospf <process id>
* Redistribute rip metric <internal> subnets
* Eg. Router ospf 10
* Redistribute rip metric 200 subnets

**ADDRESS TRANSLATION**

**NAT –** mapping of the one IP space to another. NAT where a private IP address gets mapped to a public IP address in order to connect to the external network.

Types: It has concept of inside local, inside global, outside local and outside global.

1. Static NAT : where one private IP address gets mapped to one fixed public IP address.
2. Dynamic NAT : the private IP address gets mapped to a pool of public IP address with the help of ACL.

**Static NAT:**

* **Ip nat inside source static <private ip address> <public ip address>**
* **Interface serial <id IN>**
* **Ip nat inside**
* **Interface serial <id OUT>**
* **Ip nat outside**

**Eg. Ip nat inside source static 10.1.1.1 203.14.1.1**

**Dynamic NAT:**

* **Access-list <std> permit <network address> <wildcard address>**
* **Ip nat inside source list <acl id > pool <pool name>**
* **Ip nat pool <pool name> <start address> <end address> netmask <subnet mask>**

**PAT –** where multiple users are connecting to same IP address with different port values or number in order to connect to the external network. (multiple private IP address maps to one single public IP address on different port number)

**Backup and Restore**

**IOS Backup**

**Configuration Backup on router:**

* **Show version**
* **Show flash – copy file name, height size file**
* **Copy flash tftp**

**Paste file name**

**Ip of that server**

**Giver name in which that file has to be saved.**

* **Copy running-config startup-config**
* **Copy startup-config tftp**

**Server IP**

**If you want you can give name or else if it will take default name.**

* **Erase startup-config – it will delete data in router**
* **Show startup-config – to check**
* **Reload**
* **Copy tftp running-config**

**VLAN**

**Logically Dividing the physical LAN into multiple isolated LAN is a VLAN technique.**

**Switch function in 3 different m odes:**

1. **Access mode – switch port is functioning under access mode when it is connected to another end device.**
2. **Trunc mode - switch port is under trunc mode when it is connected to the another switch.**
3. **Dynamic mode –**

**SPANNING TREE**

When we having multiple switches in a network there is broadcast storm occurs this result as a bandwidth chocking.

STP is a protocol.

It removes the redundant path available in a network.

It uses root bridge – It is a switch which has the highest root id and is always under the forwarding mode. Any switch is connected to the root switch is also under the forwarding mode.

Root id is calculated by a protocol or value called as bridging protocol data unit (BPDU). Data unit is consists of mac id.

Modes in STP:

1. Disable mode – switch port is not active
2. Blocking mode - switch port is active but it will not responds(does not transmit any data).
3. Learning mode - whenever switch receives a packet it will learn what is mac id of that packet
4. Listening mode – whenever two switch are communicating then other switch should listen it.
5. Forwarding mode – forward packets to the other switch to reach destination.

**InterVLAN / Router on Stick**

First do vlan on switch say 10 and 20.

Give gateway for all pc

Go to Switch:

* Int fa 0/1
* Switchport mode trunk

Go to Router:

* En
* Conf t
* Int fa 0/0
* No ip address
* No shutdown
* Int fa 0/0.1
* Encapsulation dot1q 10
* Ip address <gateway> <subnet mask> eg: ip address 10.1.1.10 255.255.255.0
* Int fa 0/0.2
* Encapsulation dot1q 20
* Ip address <gateway> <subnet mask>

**IntraVLAN**

**VIRTUAL LAN TRUNKING PROTOCOL (VTP)**

VTP is a sub protocol which supports STP for removing the redundant path in a switch network and also trunk the VLAN’s from one switch to another.

Switch is configure in 3 different modes:

1. Server mode –
2. Client mode
3. Transparent mode

default mode of the switch is server mode and the main functionality of the server switch is creating and managing VLAN database in a network and responsible for replication VLAN database to clients.

Clients responsible for accessing the VLAN database from server switch and cannot create any additional VLAN entry.

Transparent mode where we can add additional VLAN’s to the VLAN database and act as a interface between multiple client switches.

**Syntax:**

* **Vtp mode <server/client/transparent>**
* **Vtp domain <domain name>**
* **Vtp password <password>**

**TELNET:**

* **Enable password <password>**
* **Enable secret <password>**
* **Line con 0**
* **Password <password>**
* **Line aux 0 – to enable telnet session**
* **Line vty 0 2 (0-2 means 3 pc can connect to below password)**
* **Password first**
* **Line vty 3 5**
* **Password second**
* **Go to any PC command prompt and enter telnet default gateway**

**telnet 10.1.1.10**

**Eg:**

**Router 0**

**enable password lock**

**enable secret unlock**

**line con 0**

**password open**

**line aux 0**

**password external**

**line vty 0 2**

**password remote**

**line vty 3 5**

**password console**

**PC0 – go to command prompt**

**telnet <router ip/gateway>**

**password: remote**

**>enable**

**password: unlock**

**banner motd “$$ Have a nice day $$”**

**PORT SECURITY:**

1. **Shutdown**
2. **Inactive**
3. **Active**

**Syntax:**

* **Int fa0/1**
* **Switchport mode access**
* **Switchport port-security**
* **Switchport port-security max 2**
* **Switchport port-security mac-address <mac id of the pc>**
* **Switchport port-security violation shutdown**

**Question:**

1. **Configure IP addresses in all the router**
2. **Configure ospf on broadcast multi access technology**
3. **Keep all the router in backbone area**
4. **Configure router id manually as shown below**
5. **R1 with router id 1.1.1.1**
6. **R2 with router id 2.2.2.2**
7. **R3 with router id 1.1.1.1**
8. **R1 with router id 1.1.1.1**
9. **R1 with router id 1.1.1.1**
10. **Demonstrate the ospf DR BDR Election.**

**WAN PROTOCOL**

**Router 1**

* **Show ip interface se 0/0/0**
* **Inter se 0/0/0**
* **Encapsulation ppp**
* **Ppp authentication pap/chap**
* **Ppp pap sent-username R1 password 1234**
* **Username R2 password 1234**

**Do the above for necessary router.**

**Router 1**

* **En**
* **Sh int se 0/0/1**
* **Encapsulation hdlc**
* **Hostname R2**
* **Conf t**

**Username R2 password 1234**

* **Int se 0/0/1**
* **Encapsulation ppp**
* **Ppp authentication pap/chap**
* **Ppp pap sent-username R1 password 1234**

**Router 2**

* **En**
* **Conf t**
* **Int se 0/0/0**
* **Encapsulation ppp**
* **Ppp au**
* **Ppp authentication pap**
* **Ppp pap sent-username R2 password 1234**

**Router 1**

* **Do ping 172.16.1.2**

**If it is not pinging then do changes change last lines for both routers…**

**DNS Server**

**Router**

* **Access-list 100 deny udp host 30.1.1.1 host <server ip> eq 53**
* **Access-list 100 permit ip any any**
* **Int fa 0/0**
* **Ip access-group 100 in**

**FTP Server**

**Router**

* **Access-list 100 deny tcp host 30.1.1.1 host <server ip> eq 21**
* **Access-list 100 permit ip any any**
* **Int fa 0/0**
* **Ip access-group 100 in**

**HTTP Server**

**Router**

* **Access-list 100 deny tcp host 30.1.1.1 host <server ip> eq 80**
* **Access-list 100 permit ip any any**
* **Int fa 0/0**
* **Ip access-group 100 in**

**HTTPS Server**

**Router**

* **Access-list 100 deny tcp host 30.1.1.1 host <server ip> eq 443**
* **Access-list 100 permit ip any any**
* **Int fa 0/0**
* **Ip access-group 100 in**