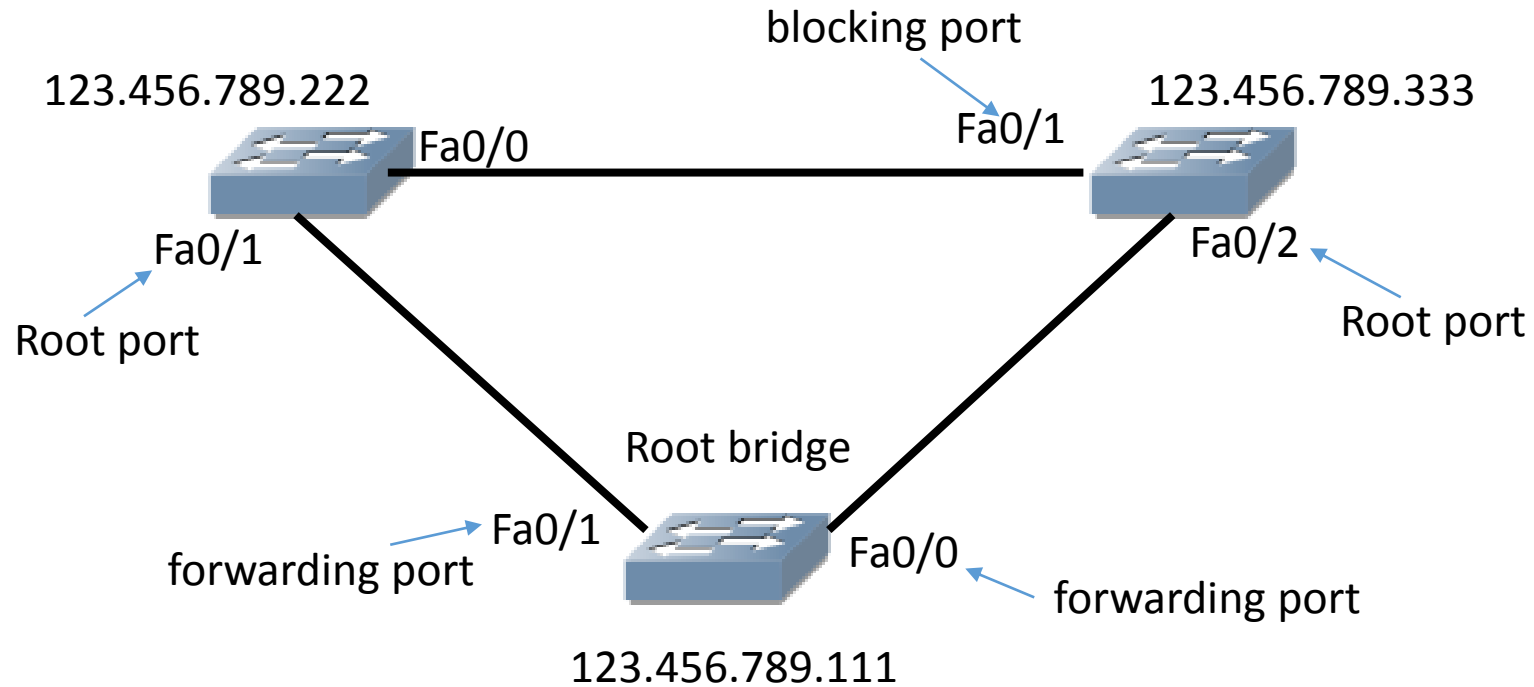# In 60 Days –ICND 2 (200-101)

The Ultimate Cram Guide

Spanning Tree Protocol (STP)

- STP runs on all switches in the network

- STP is maintained by only one switch in the network

- STP maintaining switch is known as 'root bridge/switch'

- Basic job of STP : To select blocking and forwarding port.

- On root bridge, all ports will be in forwarding state.

- The port of other switch directly connecting root bridge is known as 'root port'.

Root Bridge is selected based on two criteria :

i - Lowest priority (default is 32768).
ii - Lowest MAC id of the switch

blocking port

123.456.789.222

Fa0/0

Fa0/1

123.456.789.333

Fa0/1

Fa0/2

Root port

Root port

Root bridge

Fa0/1

Fa0/0

forwarding port

forwarding port

123.456.789.111

STP Enhancements

- EtherChannel

- PortFast

- BPDU Guard

- Rapid STP

Rapid STP (RSTP)

- IEEE 802.1w

- STP convergence 50 seconds. RSTP 2 secs.

- Ports – Root(forwarding)/Designated(forwarding)/Backup(blocking)/Alternate(blocking)/Disabled

- PVST+ works with RSTP to allow for an individual STP instance per VLAN (so you could choose a different root bridge per VLAN!)

- Enable with:

```
Switch(config)#spanning-tree mode rapid-pvst
```

Etherchannel

- Groups physical ports into a logical interface
- Load balances traffic but config must match both sides
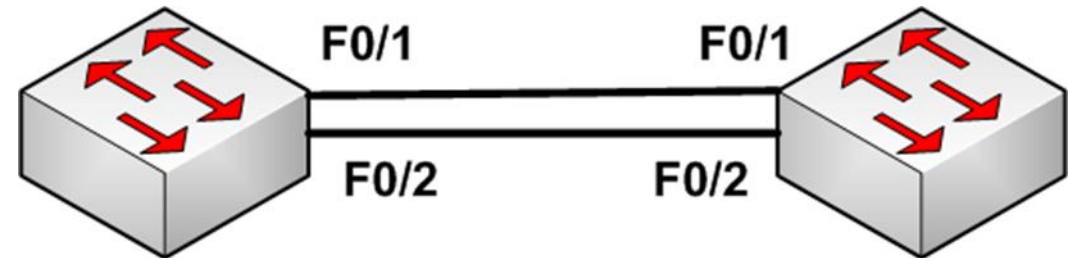

```
Switch1(config)#int range f0/1-2
Switch1(config-if-range)#switchport mode access
Switch1(config-if-range)#channel-group ?
  <1-6>  Channel group number
Switch1(config-if-range)#channel-group 1 mode ?
  active     Enable LACP unconditionally
  auto       Enable PAgP only if a PAgP device is detected
  desirable  Enable PAgP unconditionally
  on         Enable Etherchannel only
  passive    Enable LACP only if a LACP device is detected
Switch1(config-if-range)#channel-group 1 mode desirable
```

First hop routing protocol

- First hop routing protocol provides protection from default gateway failover by providing backup routers.

- In the event of failover, backup router takes place of active router.

- Provides Load balancing

- Provides Redundancy

- Three First hop routing protocol :
    - HSRP - Hot Standby Router Protocol
    - VRRP - Virtual Router Redundancy Protocol
    - GLBP - Gateway Load Balancing Protocol

HSRP - Hot Standby Router Protocol

- It is a CISCO proprietary protocol
- Uses UDP port 1985
- Sends Hello message on multicast address 224.0.0.2
- Hello message interval – 3 sec and Hold timer – 10 sec
- Priority by default is 100
- Supports tracking
- HSRP state :
    Active
    Standby

Configuration HSRP

```
R1(config)#interface vlan 100
R1(config-if)#ip address 192.168.100.11 255.255.255.255.0
R1(config-if)#standby 1 ip 192.168.100.1
R1(config-if)#standby priority 150
R1(config-if)#standby 1 preempt


R2(config)#interface vlan 100
R2(config-if)#ip address 192.168.100.22 255.255.255.255.0
R2(config-if)#standby 1 ip 192.168.100.1
R2(config-if)#standby priority 200
R2(config-if)#standby 1 preempt
```

VRRP - Virtual Router Redundancy Protocol

- VRRP is similar in functionality as HSRP
- A virtual router representing a group of routers is known as VRRP group
- Virtual router uses physical interface/virtual interface IP address.
- VRRP group range from 0 to 255
- Uses IP protocol 445
- Advertisement interval timer 1 sec and hold timer 3 sec
- Preempt is by default enabled
- Virtual MAC 00-00-5e-00-01-xx (xx is the group number)

Configuration VRRP

```
R1(config)# interface fast 0/0
R1(config-if)# ip address 10.10.10.21 255.0.0.0
R1(config-if)# vrrp 1 priority 120
R1(config-if)# vrrp 1 authentication cisco
R1(config-if)# vrrp 1 ip 10.10.10.10
R1(config-if)# vrrp 1 track 1


R2(config)# interface fast 0/1
R2(config-if)# ip address 10.10.10.11 255.0.0.0
R2(config-if)# vrrp 1 priority 150
R2(config-if)# vrrp 1 authentication cisco
R2(config-if)# vrrp 1 ip 10.1.0.10
R2(config-if)# vrrp 1 track 1
```

GLBP – Gateway Load Balancing Protocol

- GLBP acts similar to HSRP and VRRP

- It provide load balancing which is limitation in HSRP and VRRP

- Uses UDP port 3222

- Hello message interval – 3 sec and Hold timer – 10 sec

- Active Virtual Gateway (AVG) is elected from the group and other become backup AVG

- AVG is responsible for answering ARP request for virtual IP address.

- Three types of Load balancing algorithm used by GLBP:
    Weighted
    Round-Robin
    Host Dependent

Configuration GLBP

```
R1(config)# interface fastethernet 0/0
R1(config-if)# ip address 192.168.100.11 255.255.255.255.0
R1(config-if)# glbp 10 ip 192.168.100.254
R1(config-if)# glbp 10 preempt
R1(config-if)# glbp 10 priority 250
R1(config-if)# glbp 10 load-balancing host-dependent


R2(config)# interface fastethernet 0/0
R2(config-if)# ip address 192.168.100.22 255.255.255.255.0
R2(config-if)# glbp 10 ip 192.168.100.254
R2(config-if)# glbp 10 preempt
R2(config-if)# glbp 10 priority 100
R2(config-if)# glbp 10 load-balancing host-dependent
```

Virtual Private Network (VPN)

- Virtual Private Network (VPN) are encrypted network transported over public network such as Internet.
- VPN carries private data over public network using advanced encryption and tunneling methods
- VPN provides:
    - Privacy
    - Authenticate
    - Data integrity
- Data packet is encrypted & encapsulated with new header to provide security.
- VPN can be configured for point to point network, point to multipoint and for host based remote access.

VPN Tunneling protocol

- **L2TP : Layer 2 Tunneling Protocol**

  It does not provide encryption; it is a combination of L2F and PPTP

- **GRE : Generic Routing Encapsulation**

  GRE does not provide encryption, it encapsulates IP, CLNP, IPX in IP packet.

- **IPSec : Internet Protocol Security**

  IPSec provide encryption , supports unicast and provides data integrity.

- **L2F : Layer 2 Forwarding**

  It does not provide encryption , L2F was designed for point to point network traffic.

- **PPTP : Point-to-Point Tunneling Protocol**

  It relies on point-to-point protocol to implement security functionality, it uses control channel over TCP and a GRE tunnel to encapsulate PPP packets.
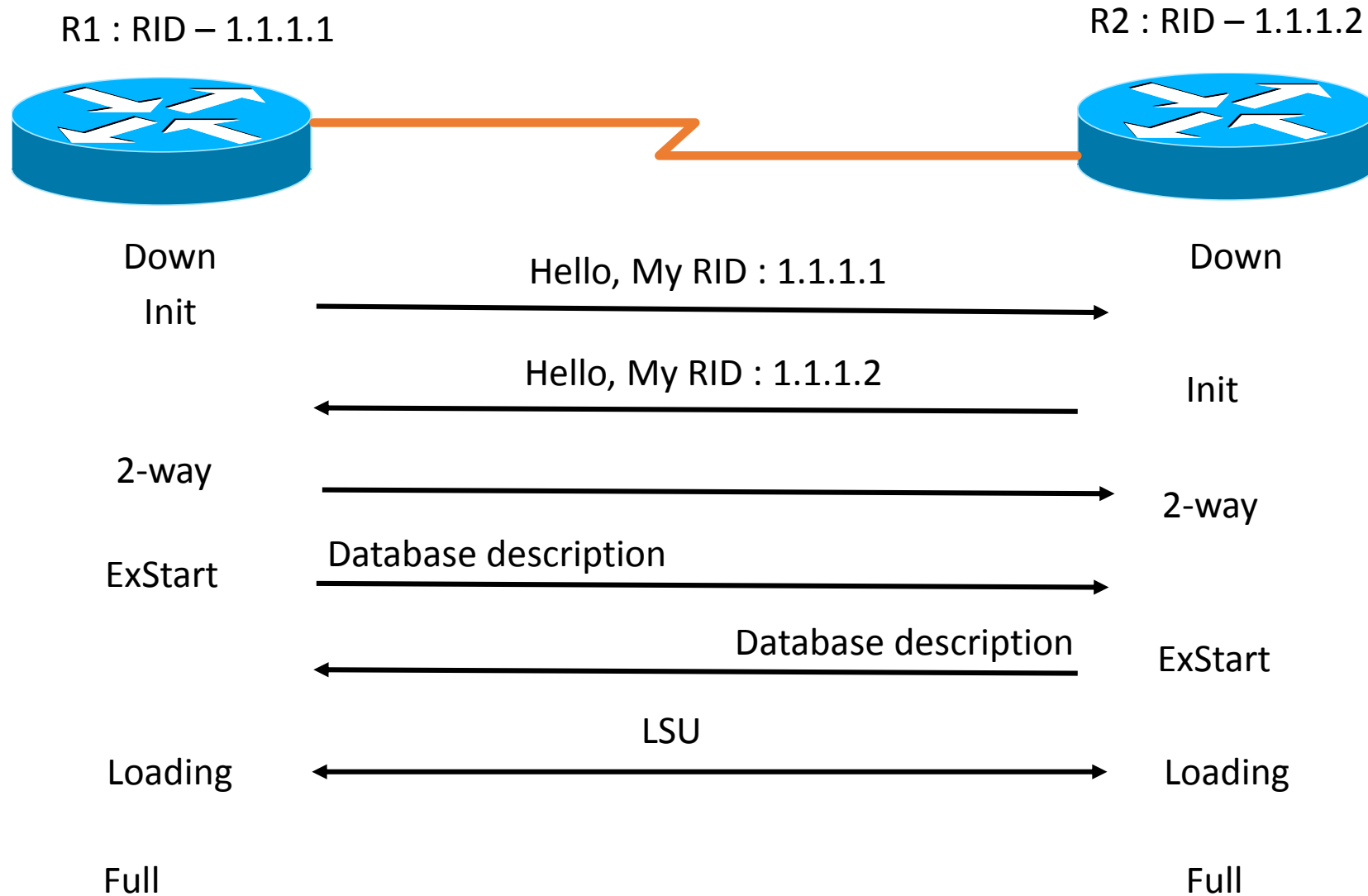
OSPF

- OSPF is open standard protocol

- Administrative distance is 110

- Metric is Cost which is calculated as
    Cost = 10^8 / Bandwidth in bps

- Faster convergence

- Hierarchical design with multiple areas

- OSPF maintains three tables :
    Neighbor table
    Database table
    Routing information Table

OSPF Network type

- BMA – Broadcast Multi-access

- Point to Point

- Point to Multipoint

❖ Router id : Every router in the OSPF network is identified by router id which can be manually assigned or automatically based on highest IP address of physical/loopback interface on the router.

❖ DR : Designated Router is selected on the basis of higher priority number which is 1 by default or on the basis of highest router id.

❖ BDR : It is selected on the basis of second highest priority or second highest router id.

OSPF Neighbourship

R1 : RID – 1.1.1.1   R2 : RID – 1.1.1.2

Down   Down

Init

Hello, My RID : 1.1.1.1

Hello, My RID : 1.1.1.2

Init

2-way

2-way

ExStart   Database description

Database description   ExStart

LSU

Loading   Loading

Full   Full

*Check neighbourship : `Router#show ip ospf neighbour`

OSPF LSA (Link State Advertisement)

- There are 7 types of LSA :

    LSA Type 1 - Router LSA

    LSA Type 2 - Network LSA

    LSA Type 3 - Summary LSA

    LSA Type 4 - ASBR summary LSA

    LSA Type 5 - External LSA

    LSA Type 6 - Multicast LSA

    LSA Type 7 - NSSA LSA

- **Command to check LSA :** `Router#show ip ospf database`

OSPF Interface Costs

Interface	Cost
ATM/Fast Ethernet, Gig Ethernet	1
HSSI	2
10Meg Ethernet	10
T1	64
DS-0 (64k)	1562
56k	1785

EIGRP

- Uses IP protocol 88
- Classless
- Hybrid of distance vector and link state
- Multicasts updates to 224.0.0.10
- Uses feasible successors to determine alternative routes
- Feasible successor a backup route based on topology table
- EIGRP does triggered updates
- It is Cisco proprietary protocol
- Maximum hop count limit is 100 by default, can be extended to 255
- Supports equal and unequal load balancing

- Metric of EIGRP is composite, in form of K-values:
  - K1 – Bandwidth = 1
  - K2 – Load = 0
  - K3 – Delay = 1
  - K4 – Reliability = 0
  - K5 – MTU = 0
- K-value must match between routers to form neighbourship
- Final metric is calculated as bandwidth + delay.
- Works on DUAL – Diffusing update algorithm

❖Feasible Distance (FD) – Total distance from source to destination is known as FD.

❖Advertised Distance (AD) – It is the distance told by next hop router regarding the destination.

❖Successor – Best route or the shortest path to the destination is known as Successor.

❖Feasible Successor - It is the second best route to the destination. *Current FD > AD
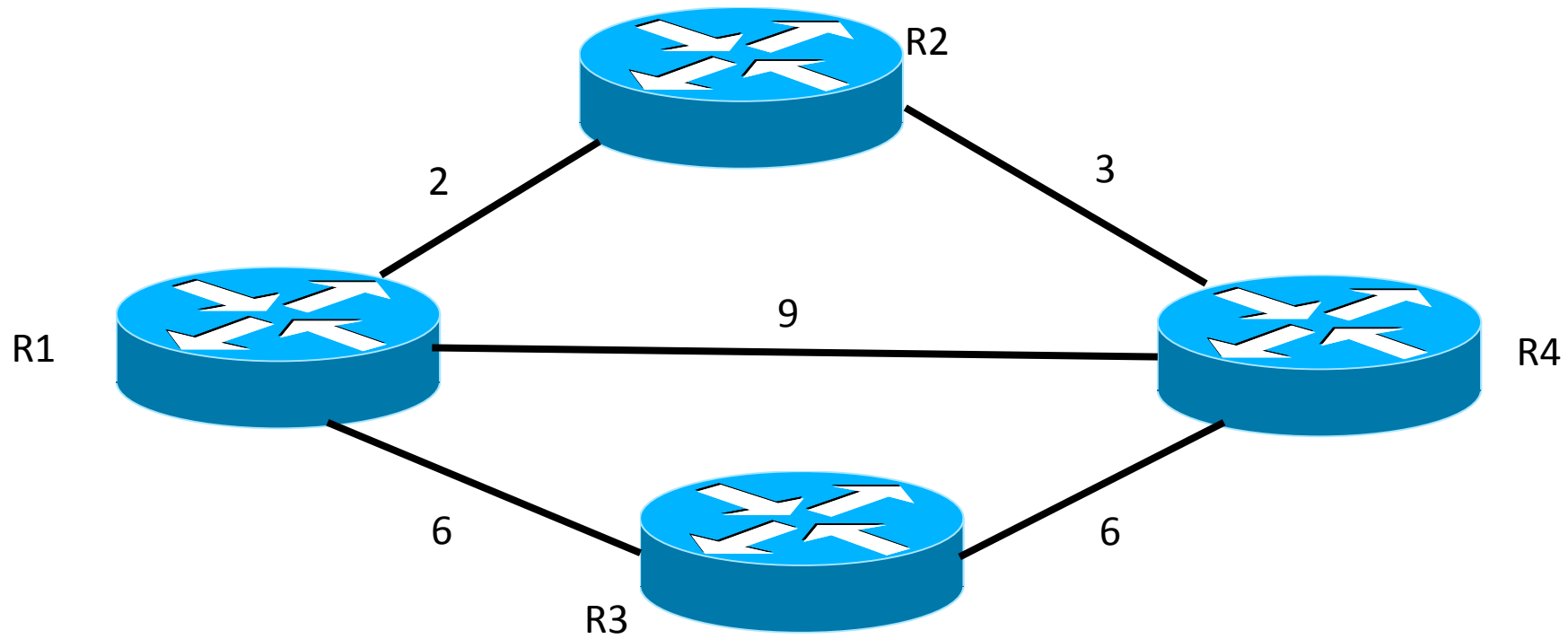
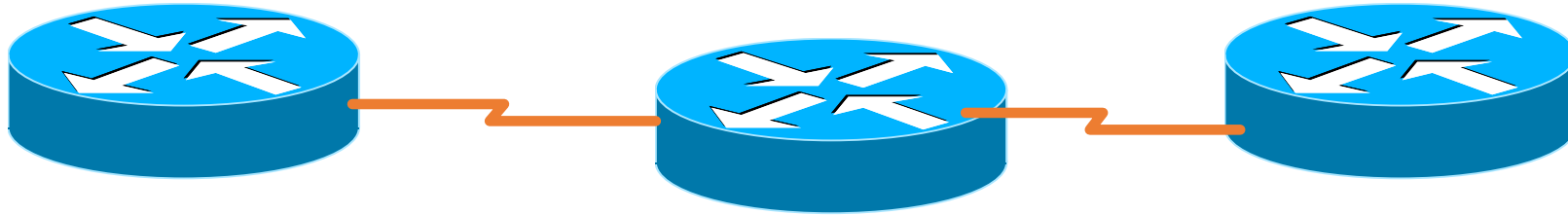| R1 to R4 Via	FD	AD	S	FS	
R2	5	3	✓	-	
R4	9	4	-	✓	Since 5>4
R3	12	6	-	✗	Since 5<6

Configure EIGRP

```
Router(config)#router eigrp 20
Router(config-router)#network 172.16.0.0
Router(config-router)#no auto-summary (optional)
```

EIGRP maintains three types of table:

i.   Neighbour table

ii.   Topology table

iii. Routing table

Troubleshooting

EIGRP 30

Layer 4 – wrong AS number or wrong network advertised
Layer 3 – wrong ip address or subnet mask
Layer 2 – encapsulation wrong PPP/HDLC
Layer 1 – missing clock rates on DCE / interface shutdown

WAN – Wide Area Network

- Point to Point / lease-line

  It works on serial link and requires lots of maintainence.

- Circuit Switching

  Transmitting data with the help of telephone line such as PSTN, ISDN,DSL.

- Packet Switching

 It is similar to leased line where bandwidth can be shared. Frame relay works under this technology.

PPP	Works with Cisco & non-Cisco Authentication if required	`encapsulation ppp` `ppp authentication chap/pap`
HDLC	Default on Cisco equipment	No need to configure

Frame-relay	Shared, up to 2Mbps Uses DLCI numbers and LMI for keepalives	`encapsulation frame-relay`
		`frame-relay map ip 10.1.1.1 200`
		(200 is the dlci)

Frame Relay (FR)

- Frame relay works on the concept of virtual circuits.

- There are two types of virtual circuits:
    i.   PVC (Permanent virtual circuit)
    ii.   SVC (Switched virtual circuit)

- Frame relay works on PVCs

- DLCI – Datalink connection Identifier

  FR is layer 2 WAN technology, so to identify PVC it uses DLCI numbers.

- LMI – Local Management Identifier

  Signalling protocol between ISP and our router.

  Three types of LMI :

  1. Cisco
  2. ANSI
  3. Q.933A

- FR encapsulation methods:

  Cisco

  IETF (Internet Engineering Task Force)

Configuring Frame Relay
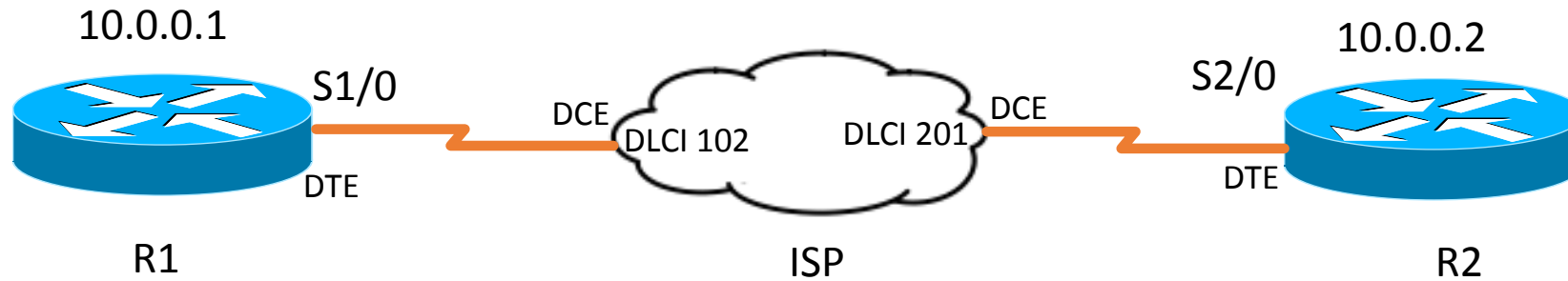

```
R1(config)#int s1/0
        #ip address 10.0.0.1 255.0.0.0
        #encapsulation frame-relay
        #frame-relay map ip 10.0.0.2 102 broadcast
        # no shut

R2(config)#int s2/0
        #ip address 10.0.0.2 255.0.0.0
        #encapsulation frame-relay
        #frame-relay map ip 10.0.0.1 201 broadcast
        # no shut
```

*imp cmd – show frame-relay map

IPv6

- To enable IPv6 on a router there are two basic commands:

  ```
  i - Router(config)#ipv6 unicast-routing  →  Enable IPv6 on router

  ii - Enable IPv6 on interface and provide ipv6 addressing


  Example:
  ipv6 unicast-routing
  !
  interface serial0/0/1
  ipv6 address 2001:fa8:1231:1::1
  ```

- Static routes

  ```
  Router(config)# ipv6 route 2001:fa8:1231:1::/64 2001:cc8:1789:2::2
  ```

- Check ping :

  ```
  Router#ping6 2001:fa8:1231:1::/64
  ```

Troubleshooting IPv6

- End device should be in the same IPv6 subnets.
- Connecting interface of the router should be in same IPv6 subnet
- Interface connecting should be in UP state
- Check missing VLANs
- Check ACL
- Check route list if routes exist.
- Check if neighbourship is formed.

Configure OSPF v3

OSPF v3 acts very similar to OSPF v2:

   configuration vise, neighbour discovery, transition from all the neighbourship
   states, Link state database

```
Router(config)#interface GigabitEthernet0/0
              #ipv6 address 2001:ca2:2:13::2/64
              #ipv6 ospf 1 area 11

              #interface serial 0/0/1
              #ipv6 address 2001:aa1:1:14::1/64
              #ipv6 ospf 1 area 22

              #ipv6 router ospf 1
              #router-id 1.1.1.1
```

OSPF v3 LSA

- 0x2001   Router LSA
- 0x2002   Network LSA
- 0x2003   Inter-area Prefix LSA
- 0x2004   Inter-area Router LSA
- 0x4005   AS-External LSA
- 0x2006   Group Membership LSA
- 0x2007   Type-7 LSA
- 0x0008   Link LSA
- 0x2009   Intra-area Prefix LSA

Three Key OSPFv3 LSA

Difference between OSPF v3 and OSPF v2

- Type 3 LSA is different

- OSPF v3 neighbours do not have IPv6 addresses in the same subnet, where as for IPv4 they should be in the same subnet

- New LSA types used by OSPFv3

Troubleshooting OSPFv3

- Check neighbor adjacencies
- Check Hello and Dead timers
- Check for OSPF area
- Check for Network types
- Check if neighourship state is 'full'
- Check if LSA are exchanged
- TS commands:
```
Router#show ipv6 protocols
Router#show ipv6 ospf interface brief
Router#show ipv6 ospf neighbor
Router#show ipv6 ospf database
Router#debug ipv6 ospf adj
```

EIGRPv6

- EIGRPv6 works in the same way as EIGRv4

- Its metric, cost is also calculated in same way

- Successor and Feasible Successor logic is same

- EIGRPv6 uses same concept of equal and unequal load balancing as in EIGRPv4.

Configuration EIGRPv6

```
ipv6 unicast-routing
!
interface Loopback0
 ipv6 address 1000:AB8::/64 eui-64
 ipv6 enable
 ipv6 eigrp 1
!
ipv6 router eigrp 1
 router-id 1.1.1.1
 no shutdown
```

Network Management

- SNMP – Simple Network Management protocol

    It is application layer protocol, provides message format communication between SNMP managers (such as Cisco prime) and SNMP agents (Cisco routers). Additional security features provided in SNMPv3 are **message integrity, authentication, and encryption**.

- Maintains database called Management Information Base (MIB)

- Syslog – Syslog server logs the messages and provides display output of all messages in a managed way.

- NetFlow – Provides statistics on IP packets in the network traffic, application monitoring, accounting and billing.

IOS

- ROM is one of the major component of the router.

- ROM contains 4 program/part

    1. POST – Power On Self Test
       It checks hardware of the router

    2. Bootstrap program – It helps to find and load OPS and device config file of the router.

    3. Mini IOS and

    4. Rom-monitor mode
       It is just like safe mode of the router, it provides tourbleshooting feature like password recovery and reinstallation of IOS.
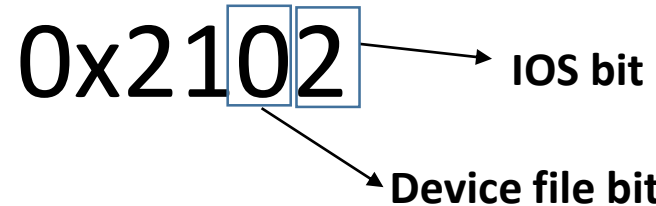
Booting process of the router

POST

↓

Bootstrap

↓

IOS (FLASH)

↓

Device file (NVRAM)

↓

Password :
Router>
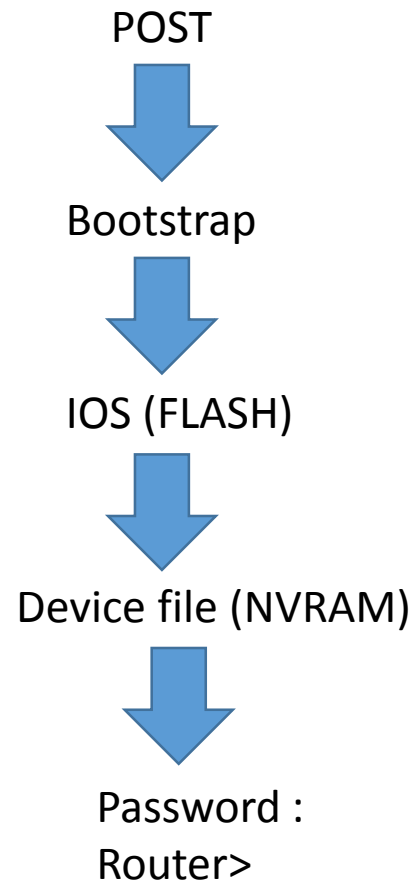
Configuration register

- It is a 16 bit hexadecimal value which defines the booting process of the router
- The default config register value is 0x2102

0x2102 ———→ **IOS bit**

———→ **Device file bit**

Device file bit :

      Vendor define 0 – 4

      0 :- 0x2100 → Normal booting

      4 :- 0x2142 → Router will bypass the NVRAM (startup) & will go to setup mode

IOS bit :

      0,1,2 – Vendor define

      3 to F – User define

      0 :- 0x2100 → Router will boot from ROM

      1 :- 0x2101 → Router will boot from Mini-IOS

      2 :- 0x2102 → Normal booting

Password recovery

- ROMMON mode is used to recover password.
- With new routers with external flash is removed and router is turned off
- On booting, router is unable to load IOS from flash, so router enters ROMMON mode and insert flash
- Set the configuration register to ignore start-up config by setting to 0x2142 and reset from ROMMON mode
- On bootup the router with flash, it will now reach enable mode without password and issue copy startup-config to running-up config command with required config
- Reset password from config mode and issue copy running config to start-up config command
- Change register value to 0x2102 and reload

```
Router#show flash:
```
   To check the flash memory content.

```
Router#show version
```
   To check IOS version, total uptime, config regiter value, memory stats, time of last loading.

```
Router(config)#license boot module <module-name> technology-package <package-name>
```
   To enable feature license activation

```
Router#show license feature
```
   Check licensing status.