

Contents

1. Routing Protocols – EIGRP.....	1
2. Routing Protocols – OSPF.....	3
3. Routed Protocols - Frame Relay.....	5
4. IPv6 Addressing.....	6
5. VLANs and VTP.....	7
6. Ether Channel.....	8
7. Spanning Tree Protocol.....	9
8. Router Redundancy (VRRP/HSRP).....	11
9. Frequently Used Commands.....	13

EIGRP (Enhanced Interior Gateway Protocol)

Important terms used in EIGRP

Successor: A route (or routes) selected as the primary route(s) used to transport packets to reach destination. Note that successor entries are kept in the routing table of the router.

Feasible successor: A route (or routes) selected as backup route(s) used to transport packets to reach destination. Note that feasible successor entries are kept in the topology table of a router.

DUAL (Diffusing Update Algorithm): Enhanced IGRP uses DUAL algorithm to calculate the best route to a destination

Routing metrics used by IGRP

Bandwidth: This represents the maximum throughput of a link.

MTU (Maximum Transmission Unit): This is the maximum message length that is acceptable to all links on the path. The larger MTU means faster transmission of packets.

Reliability: This is a measurement of reliability of a network link. It is assigned by the administrator or can be calculated by using protocol statistics.

Delay: This is affected by the bandwidth and queuing delay.

Load: Load is based among many things, CPU usage, packets processed per sec

Important Command in EIGRP

1. **show ip eigrp topology** : To display entries in the EIGRP topology table, use the show ip eigrp topology command in EXEC mode.
2. **show ip eigrp neighbours**: To display the neighbors discovered by EIGRP, use the show ip eigrp neighbors command in EXEC mode. It shows when neighbors become active and inactive. The neighbor parameters displayed include Address, Interface, Holdtime, Uptime, Q, Seq Num, SRTT, and RTO.
3. **show ip route eigrp**: Displays the EIGRP routes installed in the route table.
4. **show ip eigrp interface**: Use the show ip eigrp interfaces command to determine on which interfaces EIGRP is active, and to find out information about EIGRP relating to those interfaces. The details shown include interfaces on which EIGRP is configured, numbered of directly connected EIGRP neighbours on each interface, Mean SRTT, etc.

Important Features of EIGRP

1. Unlike RIP and IGRP, EIGRP updates are not periodic. EIGRP updates are sent only when there is a topological change in the network.
2. In EIGRP, the router doing the summarization will build a route to null0 for the summarized address. This ensures that the packets that are not destined for any network are routed to null and thus dropped.
3. EIGRP provides the option of disabling route summarization. The command no auto-summary can be used for this purpose. This option is not available in RIP and IGRP.
4. You can summarize routes in EIGRP at any arbitrary bit boundary

Packet types used by EIGRP when communicating with its neighboring EIGRP routers

1. **Hello Packets** - EIGRP sends Hello packets once it has been enabled on a router for a network. These messages are used to identify neighbors and once identified, serve or function as a keep alive mechanism between neighbors. EIGRP Hello packets are sent to the link local Multicast group address 224.0.0.10. Hello packets sent by EIGRP do not require an Acknowledgment to be sent confirming that they were received.
2. **Acknowledgment Packets** - An EIGRP Acknowledgment (ACK) packet is simply an EIGRP Hello packet that contains no data. Acknowledgment packets are used by EIGRP to confirm reliable delivery of EIGRP packets. ACKs are always sent to a Unicast address, which is the source address of the sender.
3. **Update Packets** - EIGRP Update packets are used to convey reachability of destinations. Update packets contain EIGRP routing updates. When a new neighbor is discovered, Update packets are sent via Unicast to the neighbor which they can build up its EIGRP Topology Table. It is important to know that Update packets are always transmitted reliably and always require explicit Acknowledgment.
4. **Query Packet** - EIGRP Query packets are Multicast and are used to reliably request routing information. EIGRP Query packets are sent to neighbors when a route is not available and the router needs to ask about the status of the route for fast convergence. If the router that sends out a Query does not receive a response from any of its neighbors, it resends the Query as a Unicast packet to the non-responsive neighbor(s). If no response is received in 16 attempts, the EIGRP neighbor relationship is reset.
5. **Reply Packets** - EIGRP Reply packets are sent in response to Query packets. The Reply packets are used to reliably respond to a Query packet. Reply packets are Unicast to the originator of the Query.
6. **Request Packets** - Request packets are used to get specific information from one or more neighbors and are used in route server applications. These packet types can be sent either via Multicast or Unicast, but are always transmitted unreliably.

Different Tables Used by EIGRP

1. **Neighbor table**: The neighbor table stores information about neighboring EIGRP routers:
 - a. Network address (IP)
 - b. Connected interface
 - c. Holdtime - how long the router will wait to receive another HELLO before dropping the neighbor; default = 3 * hello timer
 - d. Uptime - how long the neighborhood has been established
 - e. Sequence numbers
 - f. Retransmission Timeout (RTO) - how long the router will wait for an ack before retransmitting the packet; calculated by SRTT
 - g. Smooth Round Trip Time (SRTT) - time it takes for an ack to be received once a packet has been transmitted
 - h. Queue count - number of packets waiting in queue; a high count indicates line congestion
2. **Topology table**: It contains only the aggregation of the routing tables gathered from all directly connected neighbors (not the entire network!). This table contains a list of destination networks in the EIGRP- routed network together with their respective metrics. Also for every destination, a successor and a feasible successor are identified and stored in the table if they exist. Every destination in the topology table can be marked either as "Passive", which is the state when the routing has stabilized and the router knows the route to the destination, or "Active" when the topology has changed and the router is in the process of (actively) updating its route to that destination.
3. **Routing table**: Stores the actual routes to all destinations; the routing table is populated from the topology table with every destination network that has its successor and optionally feasible successor identified (if unequal-cost load-balancing is enabled using the variance command). The successors and feasible successors serve as the next hop routers for these destinations.

OSPF and OSPF Area

OSPF is a link state technology that uses Dijkstra algorithm to compute routing information.

An OSPF area is a collection of networks and routers that have the same area identification. OSPF process identifier is locally significant.

OSPF router ID determination

1. Use the address configured by the ospf router-id command
2. Use the highest numbered IP address of a loopback interface
3. Use the highest IP address of any physical interface
4. If no interface exists, set the router-ID to 0.0.0.0

OSPF Priority

The ip ospf priority command is used to set manually which router becomes the DR. The range is 0-255 and the default is 1. 0 means it will never be DR or BDR.

DR and BDR Election

When two or more routers are contending to be a DR (designated Router) on a network segment, the router with the highest OSPF priority will become the DR for that segment. The same process is repeated for the BDR. In case of a tie, the router with the highest RID will win.

OSPF Area Types

Standard Area : Default OSPF area type

Stub Area : External link (type 5) LSAs are replaced with a default route

Totally Stubby Area : Type 3, 4, and 5 LSAs are replaced with a default route

Not So Stubby Area (NSSA) : A stub area containing an ASBR; type 5 LSAs are converted to type 7 within the area

Router Types

Internal Router : All interfaces reside within the same area

Backbone Router : A router with an interface in area 0 (the backbone)

Area Border Router (ABR) : Connects two or more areas

AS Boundary Router (ASBR) : Connects to additional routing domains; typically located in the backbone

OSPF LSA Types

- a. LSA 1 (Router LSA): Generated by all routers in an area to describe their directly attached links (Intra-area routes). These do not leave the area.
- b. LSA 2 (Network LSA): Generated by the DR of a broadcast or Nonbroadcast segment to describe the neighbors connected to the segment. These do not leave the area.
- c. LSA 3 (Summary LSA): Generated by the ABR to describe a route to neighbors outside the area (Inter-area routes).
- d. LSA 4 (Summary LSA): Generated by the ABR to describe a route to an ASBR to neighbors outside the area.
- e. LSA 5 (External LSA): Generated by ASBR to describe routes redistributed into the area. These routes appear as E1 or E2 in the routing table. E2 (default) uses a static cost throughout the OSPF domain as it only takes the cost into account that is reported at redistribution. E1 uses a cumulative cost of the cost reported into the OSPF domain at redistribution plus the local cost to the ASBR.
- f. LSA 6 (Multicast LSA): Not supported on Cisco routers.
- g. LSA 7 (NSSA External LSA): Generated by an ASBR inside a NSSA to describe routes redistributed into the NSSA. LSA 7 is translated into LSA 5 as it leaves the NSSA. These routes appear as N1 or N2 in the ip routing table inside the NSSA. Much like LSA 5, N2 is a static cost while N1 is a cumulative cost that includes the cost up to the ASBR.

LSAs used by different OSPF Areas

- a. Area backbone LSAs: The LSAs generated by Area Backbone Routers are LSA1, LSA2, LSA3, LSA4, and LSA5. Note that LSA6 is not supported by Cisco, and LSA7 is generated by NSSA router.
- b. Stub area LSAs: The Stub area router generates LSA types 1, 2, and 3. i.e. Router LSA, Network LSA, and Summary LSA.
- c. Totally Stubby LSAs: The Totally Stubby area routers generate LSA types 1 and 2. NSSA LSAs: A NSSA (Not So Stubby Area) router generates LSA types 1, 2, and 7. LSA 7 is translated into LSA 5 as it leaves the NSSA.

Important Features of Stub Area

1. A stub area reduces the size of the link-state database to be maintained in an area, which in turn results in less overhead in terms of memory capacity, computational power, and convergence time.
2. The routing in Stub and totally Stubby areas is based on default gateway. A default route (0.0.0.0) needs to be configured to route traffic outside the area.
3. The stub areas suited for Hub-Spoke topology.
4. Area 0 is not configured as Stubby or totally Stubby. This is because stub areas are configured mainly to avoid carrying external routes, whereas Area 0 carries external routes.

External Routes

The cost of external route depends on the configuration of ASBR.

There are two external packet types possible.

1. Type 1 (E1) - Here the metric is calculated by adding the external cost to the internal cost of each link that the packet crosses.
2. Type 2 (E2) - This type of packet will only have the external cost assigned, irrespective of where in the area it crosses. Type 2 packets are preferred over Type 1 packets unless there are two same cost routes existing to the destination.

Default Route Advertisement in OSPF

A default route can be advertised into OSPF domain by an ASBR router in one of two ways:

1. By using "default-information originate" command: This command can be used when there is a default route (0.0.0.0/0) already existing. This command will advertise a default route into OSPF domain.
2. By using "default-information originate always" command: This command can be used when there is a default route (0.0.0.0/0) is present or not. This command is particularly useful when the default route is not consistent. An inconsistent default route may result in flipping of the route advertised into the OSPF domain, resulting in instability of the OSPF domain routing information. Therefore, it is recommended to use "always" keyword.

Types of virtual circuits (Vcs) in Frame Relay

Frame Relay is purely a Layer 2 standard.

Two types of Vcs in FR

- 1. Permanent Virtual Circuits (PVCs):** these are permanently established connections that are used for frequent and consistent data transfers between DTEs across a Frame Relay cloud.
- 2. Switched Virtual Circuits (SVCs):** these are temporary connections used in situations requiring only occasional data transfers between DTEs across Frame Relay cloud. The terms "Call Setup", "Data Transfer", "Idle", and "Call Termination" are associated with SVCs.

Frame Relay connection types

- 1. Point-to-Point:** In point-to-point connection type, a single sub interface establishes a PVC connection to another physical interface or sub-interface
- 2. Multi-point :** In multipoint connection type, a single sub-interface is used to establish multiple PVC connections to several physical interfaces or sub-interfaces. In multipoint Frame-Relay network, split horizon rule is applicable to broadcast traffic.

Frame relay sub-interfaces

When configuring frame-relay using sub interfaces the physical interfaces on which sub interfaces are configured would not be assigned any IP address. Even if one is assigned it should be removed prior to configuring frame-relay.

If an IP address is assigned to physical interface, the sub interfaces defined within the physical interface will not receive any frames.

Split horizon is a method of preventing a routing loop in a network. To overcome the split horizon, sub-interfaces can be configured on NBMA networks.

Frame Relay encapsulation types and LMI Types

Cisco supports two types of Frame Relay encapsulation: **cisco (default), and ietf.** Use IETF when setting up a frame-relay network between a Cisco router and a non-Cisco router.

Frame-Relay LMI types are **Cisco (default), ANSI, Q933A;** LMI type is auto-sensed in IOS v11.2 and up.
Show frame-relay lmi command shows LMI stats.

DLCI (Data Link Connection Identifier)

Salient features

1. DLCIs have only local significance. It means, the end devices over FR network can have different DLCI numbers
2. DLCI number is provided by the FR service provider. DLCI number is mapped to Layer 3 protocol address using 'Frame-Relay map' statement.
3. DLCI numbers must be unique on a router.

DLCI Configuration

The command used to assign dcli number to a sub interface is:

R1(config-if)#frame-relay interface-dlci <dlci-number>

Ex: R1(config-if)#frame-relay interface-dlci 100

Note that prior to issuing the above command; issue the following command to get into proper sub interface configuration mode:

R1(config)#interface serial number.subinterface-number {multipoint | point-to-point} Ex: R1(config)#interface serial 0.1 point-to-point

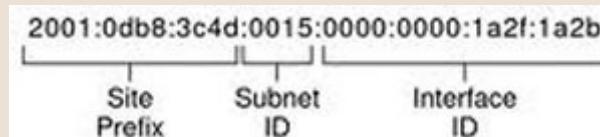
IPv6 : Points to Remember

1. IPv6 address is **128 bits** in length represented in hexadecimal
2. IPv6 Loopback address is `0:0:0:0:0:0:0:1`, also expressed as `::1`.
3. IPv6 reserves two special addresses. They are `0:0:0:0:0:0:0:0` and `0:0:0:0:0:0:0:1`.
4. Three transition strategies for migration from ipv6 to ipv4 are dual stacking, 6-to-4 tunneling and NAT-PT

IPv6 Addressing

IPv6 address consists of 8 groups of four hexadecimal digits separated by colons and which mainly consists of 3 segments called Global Prefix which is of 48 bits, subnet part with 16 bits and Interface ID called as Host part with 64 bits.

The first 3 octets constitute Global Prefix, the fourth octet constitute subnet part and the last four form the Interface ID.



- Rules :**
- a) One set of 0's in the address can be replaced by `::` but this can be done only once
 - b) One or any number of consecutive groups of 0 value can be replaced with two colons (`::`)

IPv6 Header

Version	Traffic Class	Flow Label
Payload Length	Next Header	Hop Limit
Source Address		
Destination Address		

Version (4 bits) : IP version number (6)

Traffic Class (8 bits) : Used for QoS

Flow Label (20 bits) : Used for packet labelling

Payload Length (16 bits) : Length of the IPv6 payload

Next Header (8 bits) : Identifies the type of header following the IPv6 header

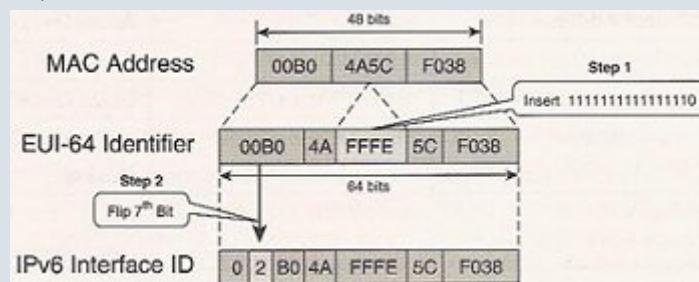
Hop Limit (8 bits) : Number of hops until the packet gets discarded.

Source Address (128 bits) : Source IP address

Destination Address (128 bits) : Destination IP address

EUI-64 Format

MAC to EUI-64 conversion inserts hex "FFFE" in the middle of a MAC addr, Then flips the U/L bit to 1, in order to create a 64-bit interface ID from a 48-bit Mac address.



IPv6 Communication Types

Unicast : used for one-to-one communication. There are 3 types of unicast addresses namely global, unique-local and link-local

Multicast : used for one-to-many communication IPv6 multicast address begins with "FF"

Anycast : used for one-to-one-of-many communication

IPv6 Address Scopes

- `::/0`-----> Default Route
- `::/128`-----> Unspecified
- `::1/128`-----> Loopback
- `FC00::/7`-----> Unique Local Unicast
- `FE80::/10`-----> Link-Local Unicast
- `FEC0::/10`-----> Site-Local Unicast
- `FF00::/8`-----> Multicast

VLANs – Points to Remember

1. VLAN 1 is the management VLAN.
2. **Static VLAN** : VLAN is statically assigned to the physical port and never changes.
3. **Dynamic VLAN** : VMPS automatically assigns VLAN based on MAC
4. **Access Link** : An access link can carry only one VLAN (used between host and switch port)
5. **Trunk Link** : A trunk link can carry multiple VLANs. Used to connect to other switches, routers, or servers
6. Two types of Trunk framing: ISL (Cisco only) and 802.1q
7. Trunk links can carry 1 to 1005 VLANs
8. Switchport modes are trunk, dynamic desirable, dynamic auto, access.

VTP – Points to Remember

1. VTP is a Layer 2 messaging protocol. It carries configuration information throughout a single domain
2. VTP Modes are
 - Server** : Create, modify, or delete VLANs (This is the default vtp mode on a switch)
 - Client** : Can't create, change, or delete VLANs
 - Transparent** : Used when a switch is not required to participate in VTP, but only pass the information to other switches
3. VTP domain is common to all switches participating in VTP
4. Pruning is a technique where in VLANs not having any access ports on an end switch are removed from the trunk to reduce flooded traffic
5. **Configuration revision number** is a 32-bit number that indicates the level of revision for a VTP packet. Each time the VTP device undergoes a VLAN change, the config revision is incremented by one.

VLAN configuration

Creating VLANs

```
SW1#vlan database
SW1(vlan)#vlan 10 name firstvlan
SW1(vlan)#vlan 20 name secondvlan
```

Access Port configuration

```
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#switchport access vlan 20
```

Access port config to a range of interfaces

```
SW1(config)#interface range fa 0/2 - 5
SW1(config-if)#switchport access vlan 10
SW1(config)#interface range fa 0/6 - 10
SW1(config-if)#switchport access vlan 20
```

Trunk Port configuration

```
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk encapsulation dot1q
```

VTP Configuration

```
SW1#vlan database
SW1(vlan)#vtp mode (Server/Client/Transparent)
SW1(vlan)#vtp domain <name>
SW1(vlan)#vtp password <password>
SW1(vlan)#vtp pruning
```

Troubleshooting commands

1. show vlan
2. show vlan-membership
3. show vtp status
4. show interfaces trunk
5. show interface <interface-name> switchport

EtherChannel

EtherChannel is a port link aggregation technology used primarily on Cisco networking devices. It allows grouping of several physical Ethernet links to create one logical Ethernet link for the purpose of providing fault-tolerance and high-speed links between switches, routers and servers.

Features of EtherChannel that is running PagP

1. PAgP helps in the automatic creation of Fast EtherChannel.
2. PAgP does not group ports configured for dynamic VLANs. PagP requires that all ports in a channel must belong to the same VLAN or should be configured as trunk ports.
3. PAgP does not group ports that work at different speeds or port duplexes.
4. The load distribution algorithm in EtherChannel can use source IP, destination IP, a combination of source and destination IPs, Source MAC, destination MAC, or TCP/UDP port numbers for decision process. If there are only two links in the EtherChannel, only 1 bit in the IP are required. If there are 4 links in the EtherChannel, 2 bits are required. An XOR on 2 bits can have 4 possible outcomes. Similarly, for an 8 link EtherChannel, 3 bits are required. Conventionally, rightmost bits are always used for XOR operation.

Important Features of Bundled Ports Using EtherChannel

1. EtherChannel can support from two to 8 links to be bundled into one logical link. Therefore, if Gigabit Ethernet links are bundled, 8 links represents 8 Gbps of one-way bandwidth, and 16 Gbps for full-duplex operation.
2. The bundled ports must have identical Spanning Tree settings
3. The bundled ports must have the same speed, duplex, and Ethernet media.
4. The bundled ports must belong to the same VLAN if not used as VLAN trunk.
5. If the bundled ports represent a VLAN trunk, then they must have same native VLAN, and each port should have same set of VLANs in the trunk.
6. The EtherChannel also provides link redundancy. If one of the bundled links fail, the traffic through the failed link is distributed to other working links in the channel. The failover is transparent to the end user. Similarly traffic again flows through the restored link, as and when a link is restored.
7. Note that the load balancing can be done based on source IP, destination IP, both source and destination IP (XOR), source and destination MAC addresses or TCP/UDP port numbers.

PagP (Short for Port Aggregation Protocol)

PagP helps in the automatic creation of Fast EtherChannel links. PagP is protocol is Cisco proprietary link aggregation protocol used in Cisco switches routers, and servers.

LACP (Short for Link Aggregation Control Protocol)

LACP is different from PAgP. LACP is a standards based protocol and conforms to IEEE standard 802.3ad, whereas PAgP is a Cisco proprietary protocol.

PAgP modes and the corresponding action

1. ON mode does not send or receive PAgP packets. Therefore, both ends should be set to ON mode to form an EtherChannel.
2. Desirable mode tries to ask the other end in order to bring up the EtherChannel.
3. Auto mode participates in the EtherChannel only if the for end asks for participation. Two switches in auto mode will not form an EtherChannel.

Important Commands

1. **switch# show etherchannel port**
Used for verifying the channel negotiation mode of an EtherChannel.
2. **Switch# show etherchannel summary**
Shows each port in the channel along with the status flag.
3. **Switch(config)# port-channel load-balance src-ip**
Will configure load balancing on EtherChannel switch links using source IP address.

STP – Points to Remember

1. STP is a layer 2 protocol that runs on switches and bridges, the purpose of STP is to remove switching loops. By default, STP is enabled on cisco switches.
2. All switches participating in STP exchange info with other switches in the network Through messages known as **BPDUs** (Sent out at a frequency of 2 sec on every port)
3. STP port states are **Blocked, Listen, Learn, Forward, Disabled**
4. The command “show spanning-tree” includes the following info
 - i. VLAN number
 - ii. Root bridge priority, MAC address
 - iii. Bridge timers (Max Age, Hello Time, Forward Delay)

STP Port Roles

1. **Root** : A bridge can have only one root port. The root port is the port that leads to the root bridge. All bridges except the root bridge will have a root port. the root port is in the STP forwarding state.
2. **Designated** : One designated port is elected per link (segment). The designated port is the port closest to the root bridge. Each designated port is in the STP forwarding state
3. **Alternate** : Alternate ports lead to the root bridge, but are not root ports. The alternate ports maintain the STP blocking state.
4. **Backup**: This is a special case when two or more ports of the same bridge (switch) are connected together, directly or through shared media. In this case, one port is designated, and the remaining ports block. The role for this port is backup.

Selection Criteria

Root Bridge Selection

The switch with the lowest Bridge ID is chosen as root.
 Bridge ID is a combination of switch priority (32768 by default and the range is 0 to 65535 with increments of 4096) and switch's MAC address

Designated Bridge Selection

- i. In a LAN segment, the bridge with the lowest path cost to the Root Bridge will be the DB **OR**
- ii. If there are two bridges in the LAN segment with equal path cost to the Root Bridge, then the Bridge with the lowest Bridge ID becomes the DB.

Root Port Selection

- i. If there are 2 or more paths to reach the Root Bridge, select the bridge port associated with the lowest accumulated path cost. **OR**
- ii. If the path cost to reach the root bridge over 2 or more bridge ports is same, then: select the neighboring switch with the lowest Switch ID value to reach the Root Bridge **OR**
- iii. If there are two or more ports on the same bridge with the lowest path cost, then:
 - * Select the port with the lowest Port Priority value, if you have multiple paths to reach the Root Bridge via same neighbor switch. **OR**
 - * If all the ports are configured with same priority number (32 by default), select the lowest port number on the switch.

Designated Port Selection

- i. The switch port (associated with the DB) on the LAN segment with the lowest accumulated path cost to the Root Bridge will be selected as DP for the given segment. **OR**
- ii. If a switch has redundant connections to the network segment, the switch port with the lowest port priority (32 by default) is selected. **OR**
- iii. If there is again a tie (it can happen if the priorities of the ports on this switch are the same), then the lowest numbered port on the switch is selected.

Default Timers

Hello-----> 2s
 Forward Delay-----> 15s
 Max Age-----> 20s

Link Costs

Bandwidth	Cost
10 Mbps----->	100
100 Mbps----->	19
1 Gbps----->	4
10 Gbps----->	2

Spanning Tree Port States

The ports on a switch with enabled Spanning Tree Protocol (STP) are in one of the following five port states.

1. Blocking
2. Listening
3. Learning
4. Forwarding
5. Disabled

A switch does not enter any of these port states immediately except the blocking state. When the Spanning Tree Protocol (STP) is enabled, every switch in the network starts in the blocking state and later changes to the listening and learning states.

Blocking - During blocking state, the port is listening to and processing BPDUs. After 20 seconds, the switch port changes from the blocking state to the listening state.

Listening - After blocking, a root port or a designated port will move to a listening state. During the listening state the port discards frames received from the attached network segment it also discards frames switched from other ports for forwarding. At this state, the port receives BPDUs from the network segment and directs them to the switch system module for processing. After 15 seconds, the switch port moves from the listening state to the learning state.

Learning - A port moves into the learning state after the listening state. During the learning state, the port is listening for and processing BPDUs. In the listening state, the port starts to process user frames and starts updating the MAC address table. Userframes are not forwarded to the destination. After 15 seconds, the switch port moves from learning to forwarding.

Forwarding - Once in the forwarding state the port sends traffic. In a forwarding state, the port will process BPDUs, update its MAC Address table with frames that it receives, and forward user traffic through the port. Forwarding State is the normal operational state.

Disabled - A port in the disabled state does not participate in frame forwarding and is considered non-operational.

Protection against sudden loss of BPDUs

1. BPDUs Skew Detection
2. Root Guard
3. BPDUs Guard
4. UDLD
5. Loop Guard

1. **Root Guard** - When configured at the interface level, BPDUs Guard shuts the port down as soon as the port receives a superior BDU. To enable root guard, use the command:
`switch(config-if)# spanning-tree guard root`

If the superior BPDUs are no more received, the port is restarted the normal STP states to return to normal use.

2. **BPDUs Guard** - Here if any BDU (superior or not) is received on a port configured with BPDUs guard, the port is immediately put into errdisable state. The port is effectively shutdown. To enable BPDUs guard use the command at interface configuration mode:
`switch(config-if)# spanning-tree bpduguard enable`

A port that is shutdown will continue to be in errdisable state even if the BPDUs are no longer received. It is recommended to use bpdus guard on all ports that have portfast enabled. The protection is useful for access layer nodes where the end user computers are expected to be connected.

3. **BPDUs Skew Detection** - It measures the amount of time that elapses from the expected time of arrival of a BDU to the actual time of arrival of the BDU. The arrival skew time condition is reported via syslog messages.

4. **Loop Guard** - The loop guard is intended to provide additional protection against L2 forwarding loops (STP loops). For example, an STP loop is created when a blocking port in a redundant topology erroneously transitions to forwarding state. The loop guard needs to be enabled on the non-designated ports to effectively prevent STP loops. Non-designated ports are the root port, alternate root ports, and ports that are normally blocking. The command used to enable loop guard is: `Switch(config-if)# spanning-tree guard loop`. The command is used at port level, loop guard is disabled by default on all switch ports.

5. **Unidirectional Link Detection (UDLD)** - The UDLD protocol allows devices connected through media such as fiber-optic or twisted-pair Ethernet to monitor the physical configuration of the cables and detect when a unidirectional link exists. If a unidirectional link is detected, UDLD shuts down the affected port and sends out an alert.

Spanning Tree Protocols

a. Rapid Spanning Tree Protocol (RSTP) is based on the IEEE standard 802.1w. The standard has evolved from its predecessor 802.1D. 802.1w has the advantage of faster convergence over 802.1D. RSTP defines port states according to what the port does with the incoming frames. The allowed port states are as given below:

1. **Discarding**: The incoming frames are discarded. No MAC addresses are learned.
2. **Learning**: The incoming frames are dropped, but MAC addresses are learned.
3. **Forwarding**: The incoming frames are forwarded according to the learned MAC addresses.

b. PVST (Per VLAN Spanning Tree) implementation has one instance of STP running for each VLAN. Therefore, when there are 32 VLANs in the bridge network, there will be 32 instances of STP running. Also, each VLAN has a unique root, path cost etc. corresponding to that VLAN.

Router Redundancy Protocols

1. **Hot Standby Router Protocol (HSRP):** HSRP is a Cisco proprietary protocol that offers router redundancy. Here one router is elected as active router, and another router is elected as standby router. All other routers are put in listen HSRP state. HSRP messages are exchanged using multicast destination address 224.0.0.2 to keep a router aware of all others in the group.
2. **Virtual Router Redundancy Protocol (VRRP):** VRRP is very similar to HSRP. VRRP is a standards based protocol and defined in RFC 2338. VRRP sends advertisements to multicast destination address 224.0.0.18 using IP protocol.
3. **Gateway Load Balancing Protocol (GLBP):** GLBP overcomes some of the limitations of HSRP/VRRP. Here, instead of just one active router, all routers in the group can participate and offer load balancing.
4. **Server Load Balancing (SLB):** SLB provides a virtual server IP address to which client machines can connect. The virtual server, in turn, is a group of real physical servers arranged in a server farm.

Members of HSRP Group

1. **Virtual router:** virtual router is what is seen by the end user device. The virtual router has its own IP and MAC addresses.
2. **Active router:** Forwards packets sent to the virtual router. An active router assumes the IP and MAC addresses of the virtual router.
3. **Standby router:** Standby router monitors the state of HSRP by using Hello messages. It assumes the role of Active router, should the current Active router fail.

Important Features of HSRP

1. HSRP authentication is carried out in clear text.
2. The hosts served by HSRP router use the IP address of virtual router as the default IP address.
3. When an Active router fails in HSRP environment, Standby router assumes the Active router role. This new Active router will remain as Active router even if the failed Active router come back to service, irrespective of the priority levels.
4. The default HSRP standby priority is 100. If the standby priorities of routers participating in HSRP are same, the router with the highest IP address becomes the Active router.
5. Within the standby group of routers, the router with the highest standby priority in the group becomes the active router. For example, a router with a priority of 100 will become active router over a router with a priority of 50. The active router forwards packets sent to the virtual router. It maintains its active state by using Hello messages.
6. Each router in a standby group can be assigned a priority value. The range of priority values is between 0 and 255 (including 0 and 255). The default priority assigned to a router in a standby group is 100. The router with numerically higher priority value will become Active router in the HSRP standby group.
7. All routers in an HSRP standby group can send and/or receive HSRP message. Also, HSRP protocol packets are addressed to all-router address (224.0.0.2) with a TTL of 1. Note that the HSRP messages are encapsulated in the data portion of UDP packets.
8. In HSRP, the MAC address used by virtual router is made up of the following three components:
 - a. **Vendor ID:** The first three bytes of the MAC address correspond to the vendor ID.
 - b. **HSRP ID:** The next two bytes of the MAC address correspond to HSRP code. It is always 07.ac. Therefore, the virtual router MAC address will have 07.ac in the fourth and fifth bytes.
 - c. **Group ID:** The last byte of the MAC address is the group's identification number.

Virtual Router Redundancy protocol (VRRP) – Important Features

1. VRRP will have one master router, and all other routers are in the backup state.
2. VRRP router priorities range from 1 to 254. By default, the priority is set to 100. 254 is the highest priority.
3. The MAC address of the virtual router is of the form 0000.5e00.01xx, where xx is the VRRP group number in the range 0 to 255 or 0 to ff hex.
4. The interval for VRRP advertisements is 1 second by default.
5. All VRRP routers are configured to preempt the current master router by default. The router priority should be highest for the preemption to occur.

GLBP (Gateway Load Balancing Protocol) Load Balancing Methods

1. **Round robin:** Here the traffic load is distributed evenly across all routers.
2. **Weighted:** A higher weighting results in more ARP replies containing the virtual MAC address of the router with higher weight.
3. **Host-dependent:** Here each client that generates an ARP always receives the same virtual MAC. In other words, the MAC address is dependent on the host.

HSRP - Important Commands

RouterA# show standby

- Displays the HSRP router status. The command displays the router priority, state (active/standby), group Number among other things. Also, to enable HSRP debugging, used the command:

RouterA# debug standby

- Enables HSRP debugging. To disable debugging, use the command “no debug standby”

R(config-if)# standby <group-number> priority <priority-value>.

- Sets the router’s priority in the standby group.

standby <group-number> preempt

- is used to force an interface to resume Active router state. Note that the priority of the router should be higher than the current Active router.

R(config-if)# standby <group-number> ip <virtual-ip-address>

- Configures a router as a member of an HSRP standby group.

R(config-if)#standby 45 ip 192.32.16.5

- Sets group number 45 with a virtual IP address of 192.32.16.5

Syntax: R(config-if)# standby <group-number> ip <virtual-ip-address>

R(config-if)# standby <group-number> preempt

- Enables the previous Active router to resume its activity as Active router by taking over the role from lower priority Active router.

standby <group-number> preempt

- Used to force an interface to resume Active router state. Note that the priority of the router should be higher than the current Active router.

Router Show commands		
Sl. No.	Command	Explanation
1.	show access-list	Displays all accesslists from all protocols present in a specified router.
2.	show banner	Displays the banner set on the router.
3.	show cdp	Shows the status of CDP such as holdtime value,no.of packets for every 60sec.
4.	show cdp interface	It tells the CDP configuration on an interface-by-interface basis.
5.	show cdp neighbor detail	Displays info on directly connected neighbors.
6.	show cdp traffic	Displays the CDP traffic info.
7.	show clock	Displays the clock (time, date).
8.	show flash	Used to view all IOS images and file stored in flash(Default location of IOS images is in flash).
9.	show frame-relay lmi	Shows the detailed statistics regarding LMI.
10.	show frame-relay map	Displays the frame relay inverse ARP table.
11.	show frame-relay pvc <dldci_num>	Shows all the frame relay PVC's terminated and their statistics at a specified router.
12.	show history	Shows the previously executed commands.IOS device stores the last ten commands that are executed.
13.	show hosts	Displays the host table.
14.	show interfaces	To view interfaces,status,and statistics for an interface.If u don't lists a specific interface,all of the interfaces on the router are listed.
15.	show ip eigrp neighbors	Shows the list of eigrp neighbors that a specified router has.
16.	show ip eigrp topology	Displays the list of successor and feasible successors,as well as other types of routes.
17.	show ip eigrp traffic	It shows the information about trafiic statistics for eigrp.
18.	show ip interfaces	Displays status and global parameters associated with the interfaces on the router.
19.	show ip interface brief	Displays the interface operational status and IP addresses for all router interfaces.
20.	show ip nat statistics	Displays NAT statistics.
21.	show ip nat translations	Displays the NAT translations.
22.	show ip ospf	Displays general information about OSPF routing processes.
23.	show ip ospf database	Displays lists of information related to the OSPF database for a specific router.
24.	show ip ospf interface	If adjacent router's dont become neighbors, then use the command to check if the local router interface is configured correctly.
25.	show ip ospf neighbor	Displays the OSPF neighbour information.
26.	show ip ospf neighbor detail	Displays all OSPF neighbors in detail.
27.	show ip route	Displays the IP routing table.
28.	show protocols	Displays the routing protocols that have been configured and running on a specified router.
29.	show running-config	Shows the current config stored in RAM.
30.	show sessions	Shows the telnet sessions that are currently suspended.
31.	show startup-config	Shows the configuration stored in NVRAM.
32.	show version	Display version information for the hardware and firmware.
33.	show arp	Displays entries in the ARP table.

34.	show ip protocols	Displays parameters and current state of the active routing protocol process.
35.	show users	Displays users connected to the router.
36.	show ipv6 interface <interface-name>	Displays ipv6 interface configuration information.
37.	show ipv6 rip	Displays information about all current IPV6 RIP processes.
38.	show ipv6 ospf	Displays general information about OSPF routing processes.
39.	show ipv6 route	Displays routes in the IPV6 routing table.
40.	show ipv6 protocols	Displays parameters and current state of the active IPV6 routing protocol processes.
41.	show ip dhcp binding	Displays IP addresses assigned to the clients.

Switch Show commands

Sl. No.	Command	Explanation
1.	show banner	Displays the banner.
2.	show flash	Displays the file contents of the flash.
3.	show history	Displays the last 10 commands entered.
4.	show interfaces	To view interfaces,status,and statistics for an interface.
5.	show interfaces vlan 1	Displays the VLAN status and the IP address of VLAN 1.
6.	show ip interface brief	Verifies the IP configuration.
7.	show running-config	Displays the config held in DRAM.
8.	show startup-config	Displays the NVRAM config.
9.	show users	Displays the users currently logged on.
10.	show version	Display IOS version information for the hardware and firmware.
11.	show vlan	Displays vlan information.
12.	show vlan-membership	Displays vlan membership information.
13.	show mac-address-table	Displays mac-address-table information.
14.	show vtp status	Displays vtp status information such as vtp mode, vtp domain etc.
15.	show spanning-tree	Displays spanning-tree statistics,including information about root bridge and port status.
16.	show spanning-tree summary	Displays summary of port states.
17.	show spanning-tree vlan <vlan-id>	Displays STP information for the specified VLAN.