ENCOR Study Guide

Alexander

March 19, 2025

OCG

Forwarding and Layer 2

VLANs are defined in the IEEE 802.1Q standard, which states that 32 bits are added to the packet header in between the Source MAC and the EtherType/Size fileds. 16 bits for the Tag protocol identifier (TPID) and 16 for the Tag control information (TCI). The TPID is a 16-bit field set to a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged frame. This field is located at the same position as the EtherType field in untagged frames, and is thus used to distinguish the frame from untagged frames. The TCI can be broken into the following subfields: Priority code point (PCP) which is 3 bits and refers to 802.1p CoS and maps to the frame priority level, Drop eligible indicator (DEI) which is a 1 bit and may be used in conjuction or separately from PCP to indicate if the frame is eligible to be dropped in the presence of congestion, VLAN identifier (VID) is a 12 bit field specifying the VLAN to which the frame belongs.

The VLAN identifier has only 12 bits, which provide 4094 unique VLANs. Catalyst switches use the following logic for VLAN identifiers:

- VLAN 0 is reserved for 802.1p traffic and cannot be modified or deleted.
- VLAN 1 is the default VLAN and cannot be modified or deleted.
- VLANs 2 to 1001 are in the normal VLAN range and can be added, deleted, or modified as necessary.
- VLANs 1002 to 1005 are reserved and cannot be deleted.
- VLANs 1006 to 4094 are in the extended VLAN range and can be added, deleted, or modified as necessary.

A routed subinterface is required when there are multiple VLANs on a switch that require routing, and it is not desirable to use a dedicated physical routed interface per VLAN, or there are not enough physical router interfaces to accommodate all the VLANs. To overcome this issue, it is possible to create a trunk port on the switch and create a logical subinterface on the router. A subinterface is created by appending a period and a numeric value after the period. Then the VLAN needs to be associated with the subinterface with the command encapsulation dot1q vlan-id.

With Catalyst switches, it is possible to assign an IP address to a switched virtual interface (SVI), also known as a VLAN interface. An SVI is configured by defining the VLAN on the switch and then defining the VLAN interface with the command interface vlan vlan-id.The switch must have an interface associated to that VLAN in an up state for the SVI to be in an up state. If the switch is a multilayer switch, the SVIs can be used for routing packets between VLANs without the need of an external router.

Some network designs include a point-to-point link between switches for routing. For example, when a switch needs to connect to a router, some network engineers would build out a transitVLAN (for example, VLAN 2001), associate the port connecting to the router to VLAN 2001 could exist elsewhere in the Layer 2 realm, or that a spanning tree could impact the topology. Instead, the multilater switch port can be converted from a Layer 2 switch port to a routed switch port with the interface configuration command no switchport. Then the IP address can be assigned to it.

Access Port: An access port is a type of switch port that is configured to carry traffic for only one VLAN (Virtual Local Area Network). It does not tag the Ethernet frames with VLAN identifiers and is used to connect end devices such as computers and printers to the network.

ARP (Address Resolution Protocol): ARP is a network protocol used to map an IP address (Layer 3) to a MAC address (Layer 2) within a local network. When a device needs to communicate with another device on the same local network and knows its IP address, ARP is used to discover the corresponding MAC address to facilitate frame delivery.

Broadcast Domain: A broadcast domain is a logical segment of a network in which any broadcast packet sent by a device is received by all other devices within the same domain. Broadcast domains are typically bounded by routers or layer 3 devices, as these devices prevent broadcast packets from crossing into other segments of the network.

CEF (Cisco Express Forwarding): CEF is a high-performance, Layer 3 packet switching technique used in Cisco routers. It improves packet forwarding efficiency by maintaining a Forwarding Information Base (FIB) and an adjacency table to quickly route packets through the network without requiring extensive routing table lookups.

Collision Domain: A collision domain is a network segment where data packets can collide with one another when being sent over the same network medium. In Ethernet networks, collision domains are typically bounded by switches or bridges that separate segments to reduce packet collisions.

CAM (Content Addressable Memory): CAM is a type of memory used in network switches to store MAC addresses and their associated ports. It allows for rapid lookup of MAC addresses when forwarding frames by comparing the incoming MAC address against stored entries to determine the appropriate outgoing port.

Layer 2 Forwarding: Layer 2 forwarding refers to the process of switching Ethernet frames based on MAC addresses at the Data Link layer (Layer 2) of the OSI model. The switch uses the MAC address table to forward frames to the appropriate port.

Layer 3 Forwarding: Layer 3 forwarding involves routing packets based on IP addresses at the Network layer (Layer 3) of the OSI model. Routers use routing tables and algorithms to determine the best path for forwarding packets across different network segments.

FIB (Forwarding Information Base): The FIB is a data structure used by routers and switches to store routing or forwarding information for quick lookup and packet forwarding decisions. It is used by CEF in Cisco devices to determine the outgoing interface for packets based on their destination IP addresses.

MAC Address Table: The MAC address table, also known as the forwarding table or content addressable memory (CAM) table, is used by network switches to map MAC addresses to specific switch ports. This table enables efficient frame forwarding by directing traffic only to the port associated with the destination MAC address.

Native VLAN: The native VLAN is a VLAN that is associated with an 802.1Q trunk port where untagged frames are sent. The native VLAN's purpose is to ensure that untagged traffic is correctly associated with a VLAN, preventing VLAN tag miscommunication on trunk links.

Process Switching: Process switching is a method of packet forwarding in which the CPU of a router processes each packet individually. This method involves a high degree of CPU intervention, which can result in slower forwarding performance compared to hardware-based methods.

RIB (Routing Information Base): The RIB is a data structure used by routers to store routing information learned from various routing protocols. It contains details about network routes and their metrics, which are used by the router to make forwarding decisions.

Trunk Port: A trunk port is a type of switch port that can carry traffic for multiple VLANs by tagging frames with VLAN identifiers. It is used to connect switches or other networking devices to maintain VLAN information across

network segments.

TCAM (Ternary Content Addressable Memory): TCAM is a specialized type of memory used in network devices to perform high-speed lookups of IP addresses and other data. Unlike traditional CAM, TCAM supports three states (0, 1, and "don't care"), enabling more complex matching operations used in features like access control lists (ACLs) and routing tables.

VLAN (Virtual Local Area Network): A VLAN is a logical network segment that groups together devices on different physical LANs into a single broadcast domain. VLANs are used to segment network traffic for security, performance, and organizational purposes, isolating traffic between different groups of devices even if they share the same physical network infrastructure.

Forwarding architectures refer to the methods and systems that network devices (like routers and switches) use to process and forward packets through a network. The main types of forwarding architectures: store-and-forward, cut-through, fragment-free, Virtual Output Queuing (VOQ), Application-Specific Integrated Circuits (ASICs), network processors, Software-Defined Networking (SDN). Store-and-forward is a packet-switching method in which a network device receives the entire packet before forwarding it to the next hop. This approach allows the device to perform error checking on the received packet, typically using Cyclic Redundancy Check (CRC) mechanisms to ensure data integrity. By buffering the entire packet, the device can also handle packets of varying sizes and manage them more effectively. While this method enhances reliability and can reduce the chances of forwarding corrupted packets, it introduces latency, as the device must wait until the complete packet is received before any forwarding action is taken. This delay can impact overall network performance, especially in high-throughput environments where speed is critical. Cut-through switching is a method that allows a network device to begin forwarding a packet as soon as it reads the destination address, without waiting for the entire packet to be received. This technique significantly reduces latency, making it faster than the store-and-forward method. As soon as the switch identifies the destination port, it starts transmitting the packet towards its destination, which is particularly beneficial in scenarios where low latency is paramount, such as in real-time applications. However, cut-through switching lacks error checking until the entire packet has been transmitted, which can lead to forwarding of corrupted packets if issues arise during transmission. Consequently, while cut-through offers speed advantages, it does so at the potential cost of data integrity. Fragment-free switching represents a compromise between the store-and-forward and cut-through methods. In this approach, the switch reads the first 64 bytes of a packet, which typically contain the header information and any collision data. If the initial segment appears valid, the switch begins forwarding the packet, thus avoiding the transmission of fragmented packets caused by collisions. This method reduces the likelihood of forwarding corrupted packets while still allowing for lower latency than pure store-and-forward systems. While fragment-free switching enhances performance in environments with high collision rates, it does not offer the same level of reliability as full store-and-forward, since it only checks a portion of the packet before forwarding. Virtual Output Queuing (VOQ) is a sophisticated switching architecture that addresses the issue of head-of-line blocking in traditional queuing systems. In VOQ, each input port maintains a separate queue for each output port, allowing packets destined for different outputs to be processed concurrently. This architecture enables more efficient use of bandwidth and minimizes latency by allowing multiple flows to be forwarded without being impeded by packets queued at the front of the line. VOQ is particularly advantageous in high-capacity switches and routers, as it optimizes resource utilization and enhances throughput. However, implementing VOQ can be complex, requiring additional memory and management resources, making it more challenging to deploy in simpler network environments. Application-Specific Integrated Circuits (ASICs) are specialized hardware components designed for high-speed packet processing in networking devices. ASICs are optimized for specific tasks, such as packet forwarding, routing, or encryption, enabling them to operate with high efficiency and low latency. By utilizing parallel processing and dedicated pathways for data, ASICs can handle vast amounts of traffic simultaneously, making them ideal for high-performance switches and routers. Their customization allows for tailored functionality to meet the specific needs of network applications. However, the design and manufacturing of ASICs can be costly and time-consuming, resulting in reduced flexibility compared to general-purpose processors, as any changes to functionality typically require redesigning the hardware. Network processors are programmable chips designed to handle complex networking tasks, such as packet inspection, classification, and traffic management. Unlike ASICs, which are hardwired for specific functions, network processors provide flexibility, allowing for the implementation of various protocols and features through software. This programmability enables network operators to adapt to changing requirements and to perform deep packet inspection for enhanced security measures. While network processors can

provide significant versatility and support advanced functionalities, they generally operate at slower speeds compared to ASICs due to their more complex architectures. As such, they are often used in environments where flexibility and advanced processing capabilities are prioritized over raw performance. Software-Defined Networking (SDN) is an innovative network architecture that decouples the control plane from the data plane, allowing centralized control over network resources. In SDN, a central controller manages the network, directing traffic flows and implementing policies across multiple devices, which can be configured and monitored programmatically. This separation enables greater flexibility, as network administrators can quickly adapt to changing demands, implement dynamic traffic management, and automate network operations through software applications. SDN also facilitates more efficient resource utilization and simplifies network management, as changes can be made from a single point of control. However, this centralized approach can introduce challenges such as increased latency for control messages and potential risks associated with a single point of failure, necessitating robust security measures and high availability strategies.

In a centralized forwarding architecture within a single network device, the control plane and data plane functions are tightly integrated, with the control plane responsible for making all forwarding decisions. The device contains a central routing processor that manages the routing table, handles protocol updates, and calculates the best paths for incoming packets. When a packet arrives, the ingress line card sends it to the routing processor, which analyzes the packet's header and consults the routing table to determine the appropriate output port. This decision is then communicated back to the line card for forwarding. While this architecture simplifies processing and allows for a cohesive decision-making process, it may introduce latency, as packets must traverse the routing processor before forwarding. Additionally, if the routing processor becomes overwhelmed or fails, packet forwarding can be severely disrupted, highlighting the importance of robust design and redundancy within the device.

In a distributed forwarding architecture within a single network device, the control and data plane functions are more decentralized, allowing individual components to operate independently. Each ingress line card is equipped with its own local forwarding engine and routing information, enabling it to make forwarding decisions without having to rely on a central processor. When a packet arrives, the line card can immediately consult its local forwarding table to determine the appropriate output port, allowing for faster processing and reduced latency. This independence enhances performance, especially under high traffic loads, as each line card can handle packets concurrently without bottlenecking at a central control point. However, this decentralized approach can lead to challenges in maintaining consistent routing information across multiple line cards, as updates must be propagated and synchronized among them. Overall, distributed forwarding within a single device promotes efficiency and speed, making it well-suited for handling high volumes of traffic.

Ingress line cards are responsible for receiving incoming packets from the network. They perform initial processing, such as buffering and determining the destination of the packets. In a centralized forwarding architecture the ingress line cards may send packets to a centralized control plane for processing. After receiving forwarding decisions from the central controller, they then pass the packets to the switch fabric. For distributed forwarding architectures the ingress line cards can make forwarding decisions locally based on routing tables stored on the line cards themselves, reducing the need to communicate with a central controller.

Egress line cards handle outgoing packets, sending them to the appropriate destination on the network. For centralized forwarding, egress cards like ingress cards depend on the central controller's instructions for the proper routing to packets. In a distributed forwarding architecture would have the egress line cards making independent forwarding decisions based on local tables, helping to expedite the forwarding process.

The role of the switches fabric is to facilitate communication between ingress and egress line cards. It transfers packets from the input ports to the output ports. In a centralized model, the switch fabric is often controlled by the central processor, which directs traffic based on the global forwarding decisions. For distributed forwarding the fabric operates in a way that allows for fast, direct communication between line cards without needing to reference a centralized control point for each packet.

Route Processor Engines (RPEs) are responsible for maintaining routing tables and making routing decisions. It runs the control plane functions. In centralized architectures, the RPE is often part of a central controller that oversees the entire network. It processes incoming route information and disseminates updates to line cards. In a distributed

scenario, each device has its own RPE that independently processes routing protocols and updates its local routing table, enabling localized decision-making.

Forwarding engines roll is to use the routing information from the route processor to make realtime forwarding decisions for packets. With a centralized model the forwarding engine will rely on direction form the centralized route processor, making forwarding decisions based on the information received from it. Imagine a distributed model where the forwarding engine works independently, utilizing local routing tables to make fast, efficient forwarding decisions without needing to consult a central point.

In centralized forwarding architectures, the route processor and forwarding decisions are made at a central point, while ingress and egress line cards primarily handle the input and output of packets with the switch fabric facilitating the movement of data. In contrast, distributed forwarding allows for localized decision-making, where each component (line cards, RPE, forwarding engine) operates independently, enhancing speed and scalability. Both architectures utilize the same components but in different configurations and operational dynamics, with centralized architectures relying on a singular control point and distributed architectures spreading the decision-making processes across multiple devices.

Software Cisco Express Forwarding (CEF) is a packet-switching method that leverages the device's CPU to manage routing and forwarding tasks. In this architecture, when a packet arrives at a network device, the software CEF examines the packet headers and makes forwarding decisions based on the routing table stored in the device's memory. This process involves several steps: the incoming packet is received, the routing processor performs a lookup in the forwarding information base (FIB), and then the packet is sent out through the appropriate interface. While software CEF provides flexibility and supports advanced features like policy-based routing and deep packet inspection, it can introduce latency due to reliance on the CPU for forwarding decisions. This architecture is typically utilized in smaller devices or scenarios where complex processing is required, but it may not scale well under high traffic conditions due to potential CPU overload.

Hardware CEF (hCEF) is a more efficient forwarding mechanism that offloads the packet processing tasks from the CPU to specialized hardware components, such as application-specific integrated circuits (ASICs) or dedicated forwarding engines. In hardware CEF, the control plane still manages routing protocols and updates the FIB, but the actual packet forwarding is performed by dedicated hardware, enabling high-speed processing and reduced latency. When a packet arrives, the hardware component quickly performs lookups in the FIB and forwards packets with minimal CPU intervention. This architecture is highly scalable and can handle larger volumes of traffic with greater efficiency, making it suitable for high-performance network devices. The use of hardware CEF allows for features such as load balancing and fast switching, while maintaining lower latency and higher throughput compared to software CEF.

Switch Database Management (SDM) templates are configurations applied to Cisco switches that define how system resources are allocated for various features, such as routing, VLANs, and access control lists (ACLs). SDM templates help optimize the switch's performance based on the specific needs of the network. By configuring SDM templates, administrators can allocate resources to match the expected traffic patterns, whether the focus is on IP routing, VLAN management, or other functionalities. For instance, a template might prioritize IP unicast routing if the switch is primarily used for Layer 3 routing, or it might optimize for bridging if the primary function is Layer 2 switching. Administrators can select from various predefined templates or create custom configurations to tailor the device's performance. Properly managing SDM templates is crucial, as improper configurations can lead to resource shortages or degraded performance, particularly in high-traffic scenarios.

COMMANDS

Define a VLAN

- vlan *vlan-id*
- name *vlan-name*

Configure an interface as a trunk port

- switchport mode trunk

Configure an interface as an access port assigned to a specific VLAN

- switchport mode access
- switchport access vlan {*vlan-id* | name *name*}

Configure a static MAC address entry

- mac address-table static mac-address vlan *vlan-id* interface *interface-id*

Clear MAC address from the MAC address table

- clear mac address-table dynamic [{address *mac-address* | interface *interface-id* | vlan *vlan-id*}]

Assign an IPv4 address to an interface

- ip address *ip-address subnet-mask*

Assign a secondary IPv4 address to an interface

- ip address *ip-address subnet-mask* secondary

Assign an IPv6 address to an interface

- ipv6 address *ipv6-address/prefix-length*

Modify the SDM database

- sdm prefer {vlan | advanced}

Display the interface that are configured as a trunk port an all the VLANs that they permit

- show interfaces trunk

Display the list of VLANs and their associated ports

- show vlan [{brief | id *vlan-id* | name *vlan-name* | summary}]

Display the MAC address table for a switch

- show mac address-table [address *mac-address* | dynamic | vlan *vlan-id*]

Display the current interface state, including duplex, speed, and link state

- show interfaces status

Display the Layer 2 configuration information for a specific switch port

- show interfaces *interface-id* switchport

Display the ARP table

- show ip arp [*mac-address* | *ip-address* | vlan *vlan-id* | *interface-id*]

Display the IP interface table

- show ip interface [brief | *interface-id* | vlan *vlan-id*]

Display the IPv6 interface table

- show ipv6 interface [brief | *interface-id* | vlan *vlan-id*]

BPDU (Bridge Protocol Data Unit): A type of network message exchanged between switches (bridges) in a network to maintain the Spanning Tree Protocol (STP). BPDUs help switches to discover and maintain the network topology, determine the root bridge, and calculate the shortest paths.

Configuration BPDU: A type of BPDU used by switches to exchange information about the network topology, including the root bridge identifier, path cost to the root bridge, and port roles. Configuration BPDUs are used during STP calculations to build and maintain the spanning tree.

Designated Port: In STP, a port on a switch that is selected to be the forwarding port for a particular network segment. It is the port that has the best path to the root bridge for that segment. Each segment has one designated port.

Forward Delay: A timer used in STP that defines how long a port stays in the Listening and Learning states before transitioning to the Forwarding state. This delay helps to ensure that all network topology changes are properly processed before the port starts forwarding traffic.

Hello Time: The interval at which BPDUs are sent out by the root bridge to maintain the STP topology. This timer helps in detecting changes in the network and ensures that all switches are synchronized with the current topology.

Local Bridge Identifier: A unique identifier assigned to each switch (bridge) in an STP network, usually consisting of the switch's Bridge Priority and MAC address. It helps to uniquely identify each switch in the network for STP operations.

Max Age: A timer that defines how long a switch should keep a BPDU before discarding it if no newer BPDU is received. This timer helps to ensure that outdated information about the network topology is eventually removed.

Root Bridge: The central switch in an STP network that serves as the reference point for all path calculations. The root bridge is selected based on the lowest Bridge ID, which is a combination of the bridge's priority and MAC address.

Root Bridge Identifier: A unique identifier for the root bridge in an STP network, consisting of the bridge's priority and MAC address. This identifier is used to distinguish the root bridge from other switches in the network.

Root Path Cost: The cumulative cost of the path from a switch to the root bridge. It helps in determining the best path to the root bridge. Each switch calculates this cost based on the cost of each link in the path.

Root Port: The port on a switch that has the lowest path cost to the root bridge. It is the port used to forward traffic towards the root bridge. Each non-root switch has one root port.

System Priority: A value used in combination with the MAC address to form the Bridge ID. The system priority helps in determining the root bridge and other switch roles in the STP process.

System ID Extension: A part of the Bridge ID that extends the MAC address space to uniquely identify switches. This extension allows for a larger number of unique bridge identifiers, especially in networks with many switches.

Topology Change Notification (TCN): A message sent by a switch to notify all other switches in the STP network of a topology change. TCNs trigger the recalculation of the spanning tree to adapt to the changes in the network topology.

COMMANDS

Set the STP max age

- spanning-tree vlan *vlan-id* max-age

Set the STP hello interval

- spanning-tree vlan *vlan-id* hello-time *hello-time*

Set the STP forwarding delay

- spanning-tree vlan *vlan-id* forward-time *forward-time*

Display the STP root bridge cost

- show spanning-tree root

Display the STP information (root bridge, local bridge, and interfaces) for one or more VLANs

- show spanning-tree [vlan *vlan-id*]

Identify when the last TCN occurred and which port was the reason for it

- show spanning-tree [vlan *vlan-id*] detail

802.1D Port States

- Disabled: The port is in an administratively off position (that is, shut down).
- Blocking: The switch port is enabled, but the port is not forwarding any traffic to ensure that a loop is not created. The switch does not modify the MAC address table. It can only receive BPDUs from other switches.
- Listening: The switch port has tgransitioned from a blocking state and can now send or receive BPDUs. It cannot forward any other network traffic. The duration of the state correlates to the STP forwarding time. The next port state is learning.
- Learning: The switch port can now modify the MAC address table with any network traffic that it receives. The switch still does not forward any other network traffic besides BPDUs.; The duration of the state correlates to the STP forwarding time. The next port state is forwarding.
- Forwarding: The switch port can forward all network traffic an can update the MAC address table as expected. This is the final state for a switch port to forward network traffic.
- Broken: The switch has detected a configuration or an operational problem on a port that can have major effects. The port discards packets as long as the problem continues to exist.

802.1D Port Roles

- Root port: A network port that connects to the root bridge or an upstream switch in the spanning-tree topology. There should be only one root port per VLAN on a switch.
- Designated port: A network port that receives and forwards BPDU frames to other swithces. Designated ports provide connectivity to downstream devices and switches. There should be only on active designated port on a link.
- Blocking port: A network port that is not forwarding traffic becuase of STP calulations.

These port types are expected on Catalyst switches:

- P2P: This port type connects with another network device (PC or RSTP switch).
- P2P edge: This port type specifies that portfast is enabled on this port.

The interface STP cost is an essential compnent for root path calulation because the root path is found based on the cumulative interface STP cost to reach the root bridge. The interface STP cost was originally stored as a 16-bit value with a reference value of 20 Gbps. As switches have developed with higher-speed interfaces, 10 Gbps might not be enough. Another method, called long mode, uses a 32-but value and uses a reference speed of 20 Tbps. The original method, known as short mode, has been the default for most switches, but has been transitioning to long mode based on specific platform and OS versions. Devices can be configured with the long-mode interface cost with thecommand spanning-tree pathcost method long. The entire Layer 2 topology should use the same setting for every device in the environment to ensure a consistent topology. Before you enable this setting in an environment, it is important to conduct an audit to ensure that the setting will work.

The root bridge election process is a critical component of the Spanning Tree Protocol (STP), which is used to prevent loops in network topologies with multiple switches. Here's a detailed explanation of how the root bridge election process works:

1. Bridge IDs: Each switch in an STP topology has a unique identifier called the Bridge ID, which consists of two parts: the Bridge Priority (a configurable value) and the MAC address of the switch. The default Bridge Priority is typically set to 32768.

2. Initiation of Election: When STP begins, all switches consider themselves potential root bridges. Each switch starts by advertising its Bridge ID to its neighbors through Bridge Protocol Data Units (BPDUs).

3. BPDU Tansmission: Each switch sends out BPDUs containing its own Bridge ID to all of its neighboring switches. This process occurs periodically, allowing switches to communicate and evaluate their IDs.

4. Comparing Bridge IDs: Upon receiving BPDUs from other switches, each switch compares the Bridge IDs. The switch with the lowest Bridge ID is elected as the root bridge. The comparison process involves:

    - First comparing the Bridge Priority values. The switch with the lowest priority value is favored.
    - If the priorities are equal, the switch with the lowest MAC address wins.

5. Consensus on Root Bridge: As BPDUs are exchanged, all switches will eventually agree on a single root bridge, as they all will learn and propagate the same BPDU with the lowest Bridge ID.

6. Convergence: Once the root bridge is elected, the other switches determine their roles (designated ports and blocked ports) in the network topology based on their distance from the root bridge, which is measured in terms of path cost. The switches will then update their forwarding tables to reflect the new topology.

7. Stable State: The network converges to a stable state with one root bridge and a loop-free topology. This state is maintained until there is a change in the network, such as a switch failure or configuration change, prompting a reelection process.

Locating Root Ports

After the switches have identified the root bridge, they must determine their root port (RP). The root bridge contunues to advertise configuration BPDUs out all of its ports. The switch compares the BPDU information received on its ports to identify the RP. The RP is selected using the following logic (where the next criterion is used in the event of a tie):

1. The interface associated to lowest path cost is more preferred.

2. The interface associated to the lowest system priority of the advertising switch is preferred next.

3. The interface associated to the lowest system MAC address of the advertising switch is preferred next.

4. When multiple links are associated to the same switch, the lowest port priority from the advertising switch is preferred.

5. When multiple links are associated to the same switch, the lower port number from the advertising switch is preferred.

Locating Blocked and Designated Switch Ports

Now that the root bridge and RPs have been identified, all other ports are considered designated ports. However, if two non-root switches are connected to each other on their designated ports, one of those switch ports must be set to a block state to prevent a forwarding loop.

1. The interface is a designated port and must not be considered an RP.

2. The switch with the lower path cost to the root bridge forwards packets, and the one with the higher path cost blocks. If they tie, they move on to the next step.

3. The system priority of the local switch is compared to the system priority of the remote switch. The local port is moved to a blocking state if the remote system priority is lower than that of the local swtich. If they tie, they move on to the next step.

4. The system MAC address of the local switch is compared to the system MAC address of the remote switch. The local designated port is moved to a blocking state if the remote system MAC address is slower than that of the local switch.

Port Fast is a feature in networking, specifically in the context of Spanning Tree Protocol (STP) on switches. When enabled on a switch port, Port Fast allows the port to skip the usual STP states (Listening and Learning) and immediately enter the Forwarding state. This is particularly useful for ports connected to end devices like computers or printers, where you want quick connectivity without the delays caused by STP convergence. By using Port Fast, you can significantly reduce the time it takes for a port to become operational after being enabled, improving network performance and responsiveness. However, it's important to use this feature carefully, as it can lead to network loops if misconfigured, especially when connecting switches or hubs.

In a stable Layer 2 topology, configuration BPDUs always flow from the root bridge toward the edge switches. However, changes in the topology have an impact on all the switch in the Layer 2 topology. The switch that detects a link status change sends a TCN BPDU towards the root bridge, out its RP. If an upstream switch receives the TCN, it sends out an acknowledgment and forwards the TCN out its RP to the root bridge. Upon receipt of the TCN, the root bridge creates a new configuration BPDU with the Topology Change flat set, and it is then flooded to all the switches. When a switch receives a configuration BPDU with the Topology Change flag set, all switches change their MAC address timer to the forwarding delay timer (witha default of 15s). This flushes out MAC address for devices that have not communicated in that 15-second window but maintains MAC addresses for devices that are actively communicating. Flushing the MAC address table prevents a switch from sending traffic to a host that is no longer reachable by that port. However, a side effect of flushing the MAC address table is that it temporarily increases the unknown unicast flooding while it is rebuilt. Remember thath this can impact hosts because of their CSMA/CD behavior. The MAC address timer is then reset to normal (300s by default) after the second configuration BPDU is received.

TCNs are generated on a VLAN basis, so the impact of TCNs directly correlates to the number of hosts in a VLAN. As the number of hosts increases, the more likely TCN generation is to occur and the more hosts that are impacted by the broadcasts. Topology changes should be checked as part of the troubleshooting process. Ports configured with Port Fast do not generate TCN BPDUs when they transition from blocking to forwarding. This means that if a device connected to a Port Fast-enabled port goes online or offline, the switch does not notify the rest of the network about this change through TCN BPDUs. Since Port Fast is typically used on ports connected to end devices (not switches), the likelihood of network loops is minimized. Therefore, not generating TCNs on these ports is generally safe. For ports that are not configured with Port Fast (typically inter-switch links), any changes in their state (like a link going down) will generate TCN BPDUs to inform the rest of the network about the topology change. In essence, enabling Port Fast prevents TCN BPDUs from being generated for state changes on those specific ports. This design choice helps maintain a faster connection for end devices while reducing unnecessary notifications about changes that are unlikely to affect the overall topology of the network. Topology changes are seen with the command show spanning-tree [vlan vlan-id] detail on a switch bridge. The output of this command shows the topology change count and time since the last change has occurred. A sudden or continuous increase in TCNs indicates a potential problem and should be investigated further for flapping ports or events on a connected switch. Flapping ports refer to network switch ports that frequently alternate between the up (active) and down (inactive) states. This behavior can cause disruptions in network performance and stability. Flapping can occur for several reasons, including: cable issues, hardware problems, misconfigurations, environment factors, overloaded network. The effects of flapping ports are: network instability, increased CPU utilization, STP convergence issues. It is important to check cables and connections, inspect configurations including duplex and speed, monitor logs for patterns, and stabilize the environment.

When a switch loses power or reboots, or when a cable is removed from a port, the Layer 1 signaling places the port into a down state, which can notify other processes, such as STP. STP considers such an event a direct link failure and can react in one of three ways, depending on the topology.

Configuration BPDU Format:

- Protocol ID (2 bytes): This is set to 0x0000 for STP.
- Version (1 byte): Indicates the version of the Spanning Tree Protocol (0 for STP).

- BPDU Type (1 byte): Set to 0 for Configuration BPDUs.
- Flags (1 byte): Contains various flags, such as the Root Port flag, which indicates whether the bridge is a root bridge or not.
- Root Bridge ID (8 bytes): The Bridge ID of the root bridge (MAC address + priority).
- Root Path Cost (4 bytes): The cost to reach the root bridge from this bridge.
- Bridge ID (8 bytes): The Bridge ID of the bridge sending the BPDU.
- Port ID (2 bytes): The ID of the port that sent the BPDU.
- Message Age (1 byte): The age of the BPDU in seconds.
- Maximum Age (1 byte): The maximum age for which the BPDU is considered valid.
- Hello Time (1 byte): The interval at which BPDUs are sent.
- Forward Delay (1 byte): The time the bridge should wait before changing states.

Topology Change Notification (TCN) BPDU Format:

- Protocol ID (2 bytes): Set to 0x0000 for STP.
- Version (1 byte): Indicates the version of the Spanning Tree Protocol (0 for STP).
- BPDU Type (1 byte): Set to 1 for TCN BPDUs.
- Flags (1 byte): Typically not used for TCN BPDUs.
- Root Bridge ID (8 bytes): The Bridge ID of the root bridge.
- Root Path Cost (4 bytes): The cost to reach the root bridge from this bridge.
- Bridge ID (8 bytes): The Bridge ID of the bridge sending the BPDU.
- Port ID (2 bytes): The ID of the port that sent the BPDU.

An example:

- s1 (root switch)
  - g1/0/2 to s2
  - g1/0/3 to s3
- s2
  - g1/0/1 to s1 (root port)
  - g1/0/3 to s3 (designated port)
- s3
  - g1/0/1 to s1 (root port)
  - g1/0/2 to s2 (blocked)

Three scenarios:

1. the link between s2 and s3 fails...how does stp react? since the link is already in a blocking state, there's no need for a TCN, and STP doesn't initiate any topology changes. Both s2 and s3 will advertise a TCN towards the root, which results in the Layer 2 topology flushing its MAC address table. Flushing the MAC table is a proactive measure to ensure that it does not use potentially outdated or invalid MAC address entries, especially since the topology may have changed. Without flushing, S1 might still have entries for MAC addresses learned from devices connected to S2 and S3. Since the topology has changed, these entries could lead to misrouting or dropped frames if traffic continues to flow based on outdated information. After the flush, as devices start communicating again, S1 can relearn MAC addresses based on the current active paths and connections. This is particularly useful in dynamic environments where devices may come and go, or ports may change states. The blocked port remains blocked, and there's no transition time needed because no ports change state. The network remains stable, and both s1 and s3 continue through their respective connections with no interruption.

2. the link between s1 and s3 fails...how does stp react? First s1 detects a link failure on its g1/0/3 interface. s3 detects a link failure on its g1/0/1 interface. Then normally, s1 would generate a TCN flag out its root port, but it is the root bridge, so it does not. s1 would advertise a TCN if it were not the root bridge. s3 removes it best BPDU received from s1 on its g1/0/1 interface because it is now in a down state. At this point, s3 would attempt to send a TCN toward the root switch to notify it of a topology change; however, its root port is down. Then s1 advertises a configuration BPDU with the Topology Change flag out of all its ports. This BPDU is received and relayed to all switches in the environment. NOTE If other switches were connected to s1, they would receive a configuration BPDU with the Topolgy Change flag set also. These packets have an impact for all switches in the same Layer 2 domain. Next s2 and s3 receive the configuration BPDU with the Topology Change flag. These switches then reduce the MAC entries. In this phase, s2 does not know what changed in the topology. Finally, there is no need to wait for the Max Age timer (default value of 20s) to age out with a link failure. s3 restarts the STP listening and learning states to learn about the root bridge on the g1/0/2 interface (which was in the blocking state previously). The total convergence time for s3 is 30s: 15s for the listening state and 15s for the learning state before s3s g1/0/2 can be made the RP.

3. the link between s1 and s2 fails...how does stp react? First s1 detects a link failure on its g1/0/2 interface. s2 detects a link failure on its g1/0/1 interface. Normally s1 would generate a TCN flag out its root port, but it is the root bridge, so it does not. s1 would advertise a TCN if it were not the root bridge. s2 removes it best BPDU received from s1 on its g1/0/1 interface because it is now in a down state. At this point, s2 would attempt to send a TCN toward the root switch to notify it of a topology change; however, its root port is down. Next s1 advertises a configuration BPDU with the Topology Change flag out of all its ports. This BPDU is then received and relayed to s3. s3 cannot relay this to s2 because it g1/0/2 port is still in a blocking state. s2 assumes that it is now the root bridge. s3 receives the configuration BPDU with the Topology Change flag from s1. s3 reduces the MAC address age timer to the forwarding delay timer to flush out older MAC entries. s3 receives s2s inferior BPDUs and discards them as it is still receiving superior BPDUs from s1. Next the Max Age timer on s3 expires, and now s3s g1/02 port transitions from blocking to listening state. s3 can now forward the next configuration BPDU it receives from s1 to s2. Finally, s2 receives s1s configuration BPDU via s3 and recognizes it as superior. It marks its g1/0/3 interface as the root port and transitions it to the listening state.The total convergence time for s2 is 50s: 20s for the Max Age timer on s3, 15s for the listening state on s2, and 15s for the learning state.

802.1W Port States:

- Discarding: The switch port is enabled, but the port is not forwarding any traffic to ensure that a loop is not created. This state combines the traditional STP states disabled, blocking, and listening
- Learning: The switch port modifies the MAC address table with any network traffic it receives. The switch still does not forward any other network traffic besides BPDUs.
- Forwarding: The switch port forwards all network traffic and updates the MAC address table as expected. This is the final state for a switch port to forward network traffic.

802.1W Port Roles:

- RP: A network port that connects to the root switch or an upstream switch in the spanning-tree topology. There should be only one root port per VLAN on a switch.

- DP: A network port that receives and forwards frames to other switches. DPs provide connectivity to downstream devices and switches. There should be only one active DP port on a link.
- Alternate port: A network port that provides alternate connectivity toward the root switch through a different switch. This is a port that provides an alternate path to the root bridge. It is a backup for a root port, which is the port that has the lowest cost to the root bridge. If the root port goes down, the alternate port can take over, helping to maintain connectivity.
- Backup port: A network port that provides link redundancy toward the shared segment within the same collision domain, which is typically a network hub.This is a port that provides a backup connection to a designated port. The designated port is the port that has the lowest cost to the segment and is responsible for forwarding traffic to and from that segment. If the designated port fails, the backup port can take over for that segment.

802.1W Port Types:

- Edge port: A port at the edge of the network where hosts connect to the Layer 2 topology with one interface and cannot form a loop. These ports directly correlate to ports that have the STP portfast feature enabled.
- Non-Edge port: A port that has received a BPDU.
- Point-to-point port: Any port that connects to another RSTP switch with full duplex. Full-duplex links do not permit more than two devices on a network segment, so determining whether a link is full duplex is the fastest way to check the feasibility of bein connected to a switch.

NOTE: Multi-access Layer 2 devices such as hubs can connect only at half duplex. If a port can connect only via half duplex, it must operate under traditional 802.1D forwarding states.

With RSTP, swtiches exchange handshakes with other RSTP switches to transition through the following STP states faster. When two switches first connect, they establish a bidriectional handshake across the shared link to identify the root bridge. This is straightforward for an environment with only two switches; however, large environments require greater care to avoid creating a forwarding loop. RSTP uses a synchronization process to add a switch to the RSTP topology without introducing a forwarding loop. The synchronization process starts when two switches are first connected. The process proceeds as follows:

1 As the first two switches connect to each other, they verify that they are connected with a point-to-point link by checking the full-duplex status.

2 They establish a handshake with each other to advertise a proposal (in configuration BPDUs) that their interface should be the DP for the segment.

3 There can be only one DP per segment, so each switch identifies whether it is the superior or inferior switch, using the same logic as in 802.1D for the system identifier (that is, the lowest priority and then the lowest MAC address). Using the MAC address from sw (0062.ec9d.c500) is the superior switch to s2 (0081.c4ff.8b00).

4 The inferior switch recognized that it is inferior and marks its local port as the RP. At that same time, it moves all non-edge ports to a discarding state. At this point in time, the switch has stopped all local switching for non-edge ports.

5 The inferior switch sends an agreement (configuration BPDU) to the root bridge, which signifies to the root bridge that synchronization is occurring on that switch.

6 The inferior switch moves its RP to a forwarding stat. The superior switch moves its DP to a forwarding state too.

7 The inferior switch repeats the process for any downstream switches connected to it.

The RSTP convergence process can occur quickly. RSTP ages out the port inforamtion after it has not received hellows in three consecutive cycles. Using default timers, the Max Age would take 20s, but RSTP requires only 6s. And thanks to the new synchronization, ports can transition from discarding to forwarding in an extremely low amount

of time.

If a downstream switch fails to acknowledge the proposal, the RSTP switch must default to 802.1D behaviors to prevent a forwarding loops.

- BPDU filter: a feature that prevents a switch port from sending or receiving Bridge Protocol Data Units (BPDUs). When enabled, the port operates in a mode where it ignores all BPDUs, effectively preventing the port from participating in STP operations. Typically used on edge ports where devices connected do not participate in STP (like end-user devices) to avoid unnecessary processing and to keep the port in a forwarding state.
- BPDU guard: a protective feature that places a port in an error-disabled state if it receives a BPDU on a port that is configured to be an edge port (a port where no BPDUs should be received). This is useful to prevent potential loops caused by mistakenly connecting switches to edge ports. If a BPDU is received, the port is disabled to protect the network.
- root guard: a feature that prevents a designated port from becoming a root port for a bridge that is not supposed to be the root bridge. If a BPDU from a superior bridge (indicating a new root) is received, the port is placed in a blocked state. It ensures that a specific switch maintains its status as the root bridge, helping to preserve the intended topology and prevent unexpected topology changes.
- STP portfast: a feature that allows a switch port to transition directly to the forwarding state from the blocking state when a device is connected. This bypasses the usual STP listening and learning states. Typically used on edge ports where end devices connect, as it speeds up the connection process and reduces the delay in getting devices online.
- STP loop guard: a feature that prevents a switch port from entering a forwarding state if it stops receiving BPDUs. It helps to protect against loops that can occur if a segment goes down and the port mistakenly assumes it can forward traffic. It is used in scenarios where unidirectional links might cause a switch to believe it is in a valid topology, thus preventing loops from forming.
- Unidirectional Link Detection (UDLD): a protocol used to detect unidirectional links between switches. It actively monitors the link status by sending messages between the two ends of a link to ensure that traffic can flow in both directions. If a unidirectional link is detected, UDLD can automatically place the affected port into an error-disabled state, preventing loops and ensuring network stability.

COMMANDS

Configure the STP priority for a switch so that it is a root bridge or a backup root bridge

- spanning-tree vlan *vlan-id* root {primary — secondary} [diameter *diameter*]
- spanning-tree [vlan *vlan-id*] priority *priority*

Configure the STP port cost

- spanning tree [vlan *vlan-id*] cost *cost*

Configure the STP port priority on the downstream port

- spanning tree [vlan *vlan-id*] port-priority *priority*

Enable root guard on an interface

- spanning-tree guard root

Enable STP portfast globally, for a specific port, or for a trunk port

- spanning-tree portfast default
- spanning-tree portfast

- spanning-tree portfast trunk

Enable BPDU guard globally or for a specific switch port

- spanning-tree portfast bpduguard default
- spanning-tree bpduguard {enable — disable}

Enable BPDU filter globally or for a specific interface

- spanning-tree portfast bpdufilter default
- spanning-tree bpdufilter enable

Enable STP loop guard globally or for a specific interface

- spanning-tree loopguard default
- spanning-tree guard loop

Enable automatic error recovery time

- errdisable recovery cause bpduguard

Change the automatic error recovery time

- errdisable recovery interval *time-seconds*

Enable UDLD globally or for a specific port

- udld enable [aggressive]
- udld port [aggressive]

Display the list of STP ports in an inconsistent state

- show spanning-tree inconsistentports

Display the list of neighbor devices running UDLD

- show udld neighbors

The placement of the root bridge is an important decision and often should be chsen to minimize the number of hops to th efurthest switch in the topology. The design should consider where redundant connections exist, connections that will be blocked, and the ability (performance) for the root switch to handle cross-switch traffic. Generally, root switches are at L2/L3 boundaries. To prevent preemptive attacks you should set the root bridge to priority of 0 and the backup at 4096...in addition to using root guard.

Using the diameter keyword when setting a new root bridge in the Spanning Tree Protocol (STP) can serve specific purposes, particularly in larger or more complex network topologies. Here's why you might consider using it:

1 control over path selection:

   - By specifying the network diameter, you can influence how STP calculates paths. If your network has specific topological requirements (e.g., limited hop counts), setting a diameter can help ensure that STP considers only appropriate paths.

2 avoiding loops:

   - By specifying the network diameter, you can influence how STP calculates paths. If your network has specific topological requirements (e.g., limited hop counts), setting a diameter can help ensure that STP considers only appropriate paths.

3 performance optimization:

- Setting a diameter can help optimize performance by limiting the complexity of the STP calculations. This can lead to faster convergence times, as STP will not need to analyze paths that exceed the specified hop count.

4 supporting larger topologies:

- In extensive networks, defining the diameter ensures that STP can handle the structure without running into issues caused by excessive hops. This can be particularly useful in environments with multiple VLANs and interconnected switches.

5 facilitating redundancy:

- By controlling the diameter, you can create redundancy in your network while ensuring that traffic paths remain efficient and manageable. This helps balance load and maintain reliability.

By changing the STP port costs, you can modify the STP forwarding path. You can lower a path that is currently an alternate port while making it designated, or you can raise the cost on a port that is designated to turn it into a blocking port. Note that the spanning-tree command modifies the cost for all VLANs unless the optional vlan keyword is used to specify a VLAN.

Port priority is a feature used in the Spanning Tree Protocol (STP) to influence the selection of which ports on a switch will be used to forward traffic. It helps determine the roles of ports in the network topology, especially in redundant network designs. Port priority helps determine which ports should be preferred for forwarding traffic versus those that should be in a blocking state. This is crucial in preventing loops in a redundant network. Each port on a switch can have a default priority value (typically 128). The priority can be adjusted to give preference to certain ports when establishing the spanning tree topology.When determining the best path to the root bridge, STP uses a combination of port priority and port costs (which are based on the speed of the link) to decide which ports to put in forwarding state and which to block. Port priority values typically range from 0 to 255. A lower value indicates a higher priority. For example, a port with a priority of 100 would be preferred over a port with a priority of 200. For switches that are not the root bridge, STP selects one port as the root port (the port with the best path to the root bridge) based on the lowest cost. If multiple ports have the same cost, port priority is used to determine which port to select. The designated port is the port on a network segment that has the lowest cost to the root bridge. If there are ties in cost, port priority is compared. Switch A has two ports connected to a network. If Port 1 has a priority of 128 and Port 2 has a priority of 64, STP will prefer Port 2 for forwarding traffic because it has a lower priority value. Port priority is a crucial component of STP that helps ensure efficient and loop-free network operation. By allowing administrators to adjust port priorities, it provides a way to influence the traffic paths in redundant network configurations.

The following scenarios are common for Layer 2 forwarding loops:

- STP disabled on a switch
- A misconfigured load balancer that transmit traffic out multiple ports with the same MAC address
- A misconfigured virtual switch that bridges two physical ports (Virtual switches typically do not participate in STP.)
- End users using a dumb network switch or hub

Preemption can be potentially dangerous in networks with spurious root switches due to several reasons:

- Flapping Root Bridge Role: If a switch constantly comes online and offline, it may cause the root bridge role to flip between different switches frequently. This ”flapping” can lead to network instability as the topology is constantly changing.
- Increased Convergence Time: When preemption occurs frequently, the network has to go through the convergence process repeatedly. Each convergence event involves re-evaluating paths and states (blocking, listening, learning, and forwarding) for all switches, which can cause temporary outages and increased latency.

- Broadcast Storms: Frequent changes in the root bridge can lead to broadcast storms, especially if multiple switches are trying to advertise their presence as the root. This can overwhelm the network with traffic, leading to degraded performance.
- Configuration Complexity: In a complex network, having multiple switches configured for preemption can make it difficult to predict which switch will be the root bridge at any given time. This unpredictability can complicate troubleshooting and network management.
- Potential Loops: If a switch that is not intended to be a stable root bridge preempts, it could cause loops in the topology if other switches don't quickly recognize the change and adjust their forwarding states accordingly.
- Inconsistent Policy Enforcement: Network policies that rely on a stable root bridge (such as Quality of Service configurations) can be disrupted, leading to inconsistent behavior across the network.

To mitigate these risks, network administrators should carefully plan and monitor their network topology, consider using techniques like Rapid Spanning Tree Protocol (RSTP) for faster convergence, and ensure that only stable and well-placed switches are configured for preemption.

Fiber-optic cables consist of strands of glass/plastic that transmit light. A cable typically consists of one strand for sending data and another strand for receiving data on one side; the order is directly opposite at the remote site. Network devices that use fiber for connectivity can encounter unidirectional traffic flows if one strand is broken. In such scenarios, the interface still shows a line-protocol up state; however, BPDUs are not able to be transmitted, and the downstream switch eventually times out the existing root pot and identifies a different port as the root port. Traffic is then received on the new root port and forwardrd out the strand that is still working, thereby creating a forwarding loop.

Unidirectional Link Detection (UDLD) allows for the bidirectional monitoring of fiber-optic cables. UDLD operates by transmitting UDLD packets to a neighbor device that includes the system ID and port ID of the interface transmitting the UDLD packet. The receiving device then repeats that information, including its system ID and port ID, back to the originating device. The process continues indefinitely. UDLD operates in two different modes:

- Normal: In normal mode, if a frame is not acknowledged, the link is considered undetermined and the port remains active.
- Aggressive: In aggressive mode, when a frame is not acknowledged, the switch sends another eight packets in 1-second intervals. If those packets are not acknowledged, the port is placed into an error state.
- BPDU filter: a feature that prevents a switch port from sending or receiving Bridge Protocol Data Units (BPDUs). When enabled, the port operates in a mode where it ignores all BPDUs, effectively preventing the port from participating in STP operations. Typically used on edge ports where devices connected do not participate in STP (like end-user devices) to avoid unnecessary processing and to keep the port in a forwarding state.
- BPDU guard: a protective feature that places a port in an error-disabled state if it receives a BPDU on a port that is configured to be an edge port (a port where no BPDUs should be received). This is useful to prevent potential loops caused by mistakenly connecting switches to edge ports. If a BPDU is received, the port is disabled to protect the network.
- root guard: a feature that prevents a designated port from becoming a root port for a bridge that is not supposed to be the root bridge. If a BPDU from a superior bridge (indicating a new root) is received, the port is placed in a blocked state. It ensures that a specific switch maintains its status as the root bridge, helping to preserve the intended topology and prevent unexpected topology changes.
- STP portfast: a feature that allows a switch port to transition directly to the forwarding state from the blocking state when a device is connected. This bypasses the usual STP listening and learning states. Typically used on edge ports where end devices connect, as it speeds up the connection process and reduces the delay in getting devices online.

- STP loop guard: a feature that prevents a switch port from entering a forwarding state if it stops receiving BPDUs. It helps to protect against loops that can occur if a segment goes down and the port mistakenly assumes it can forward traffic. It is used in scenarios where unidirectional links might cause a switch to believe it is in a valid topology, thus preventing loops from forming.
- Unidirectional Link Detection (UDLD): a protocol used to detect unidirectional links between switches. It actively monitors the link status by sending messages between the two ends of a link to ensure that traffic can flow in both directions. If a unidirectional link is detected, UDLD can automatically place the affected port into an error-disabled state, preventing loops and ensuring network stability.

COMMANDS

Configure the switch for a basic MST refion that includes all VLANS and the version number 1

- spanning-tree mode mst
- spanning-tree mst configuration
- instance 0 vlan 1-4094
- revision 1

Modify a switch's MSTI priority or make it the root bridge for the MSTI

- spanning-tree mst *instance-number* priority *priority*
- spanning-tree mst *instance-number* root {primary | secondary}[diameter *diameter*]

Specify additional VLANs to an MSTI

- spanning-tree mst configuration
- instance *instance-number* vlan *vlan-id*

Change the MST version number

- spanning-tree mst configuration
- revision *version*

Change the port cost for a spcific MSTI

- spanning-tree mst *instance-number* cost *cost*

Change the port priority for a spcific MSTI

- spanning-tree mst *instance-number* port-priority *priority*

Display the MST configuration

- show spanning-tree mst configuration

Verify the MST switch status

- show spanning-tree mst [*instance-number*]

View the STP topology for the MST

- show spanning-tree mst interface *interface-id*

Common Spanning Tree (CST): a single spanning tree that is used to represent the entire network topology in a multi-instance environment, such as in Multiple Spanning Tree Protocol (MSTP). The CST is used to prevent loops and ensure that all VLANs can communicate efficiently over a single tree structure.

internal spanning tree (IST): a spanning tree that encompasses all VLANs in a single instance. It is used in MSTP to define the path for traffic across the network. The IST is responsible for maintaining the loop-free topology within the entire MST region.

MST instance (MSTI): a specific spanning tree configuration for a particular set of VLANs within an MST region. Each MSTI can have its own unique topology and can be used to optimize traffic paths based on the VLAN traffic patterns. MSTP allows for multiple MSTIs to be defined within the same MST region.

MST region: a collection of switches that share the same MST configuration and participate in the same MSTP. All switches within an MST region must have the same MST configuration parameters (such as region name, revision number, and mappings of VLANs to MSTIs). This ensures consistent spanning tree behavior across the switches in the region.

MST region boundary: the point at which one MST region ends and another begins. It is defined by switches that do not share the same MST configuration. These boundary switches may use different spanning tree protocols (e.g., RSTP, CST) and must interact carefully to avoid loops and ensure proper communication between regions.

PVST simulation check: a process used to verify that a network's configuration adheres to the principles of Per-VLAN Spanning Tree (PVST) operation. It ensures that the network topology can accommodate the requirements of PVST, including the management of multiple spanning trees for different VLANs. The simulation check often involves analyzing the switch configurations, port roles, and state to ensure that they are correctly set up to prevent loops and optimize traffic flow.

COMMANDS

Configure the VTP version

- vtp version {1 | 2 | 3}

Configure the VTP domain name

- vtp domain *domain-name*

Configure the VTP mode for a switch

- vtp mode {server | client | transparent | off}(required for the VTP v3 server)
- vtp primary

Configure a switch port to actively attempt to establish a trunk link

- switchport mode dynamic desirable

Configure a switch port to respond to remote attempt to establish a trunk link

- switchport mode dynamic auto

Configure the member ports for a static EtherChannel

- channel-group *etherchannel-id* mode on

Configure the member ports for an LACP EtherChannel

- channel-group *etherchannel-id* mode {active | passive}

Configure the memeber ports for a PAgP

- channel-group *etherchannel-id* mode {auto | desirable} [non-silent]

Configure the LACP packet rate

- lacp rate {fast | slow}

Configure the minimum number of member links for the LACP EtherChannel to become active

- port-channel min-links *min-links*

Configure the maximum number of member links in an LACP EtherChannel

- lacp max-bundle *max-links*

Configure a switch's LACP system priority

- lacp system-priority *priority*

Configure a switch's LACP port priority

- lacp port-priority *priority*

Configure the EtherChannel load-balancing algorithm

- port-channel load-balance *hash*

Display the VTP system settings

- show vtp status

Display the switch port DTP settings, native VLANs, and allowed VLANs

- show interface [*interface-id*] trunk

Display a brief summary update on EtherChannel interfaces

- show etherchannel summary

Display detailed information for the local EtherChannel interfaces

- show interface port-channel

Display information about LACP neighbors

- show lacp neighbor [detail]

Display the local LACP system identifier and priority

- show lacp *system-id*

Display the LACP counters for congfigure interfaces

- show lacp counters

Display information about PAgP neighbors

- show pagp neighbor

Display the PAgP counters for configured interfaces

- show pagp counters

Display the algorithm for load balancing network traffic based on the traffic type

- show etherchannel load-balance

Dynamic Trunking Protocol (DTP): a Cisco proprietary protocol used to negotiate the establishment of trunk links between switches. DTP allows switches to automatically determine whether a link should be a trunk or an access link based on the configuration of both ends. It simplifies the configuration process by enabling or disabling trunking dynamically based on the devices connected to the port.

EtherChannel bundle: a logical link that aggregates multiple physical Ethernet links into a single logical interface. This configuration provides increased bandwidth and redundancy. EtherChannel allows for load balancing across the physical links and can help improve network performance by combining the capacity of the links.

LACP interface priority: the priority value assigned to individual interfaces in a Link Aggregation Control Protocol (LACP) configuration. This priority helps determine which links are included in the EtherChannel bundle if the total number of links exceeds the configured limit. The link with the highest priority (lowest numerical value) is preferred for inclusion in the bundle.

LACP system priority: a value assigned to the entire system (switch) that participates in LACP. It helps in resolving conflicts when multiple switches attempt to form an EtherChannel. The switch with the highest system priority (lowest numerical value) will be preferred as the aggregator for the EtherChannel, which is particularly important in cases of redundancy or multiple connections.

load-balancing hash: an algorithm used to distribute traffic across the member links of an EtherChannel or other aggregated links. The hash function takes certain criteria (such as source and destination IP addresses, MAC addresses, or Layer 4 port numbers) to create a hash value that determines which link will carry the traffic. This approach optimizes bandwidth usage and reduces congestion on individual links.

member links: the individual physical Ethernet links that are aggregated together to form an EtherChannel. Each member link contributes to the overall bandwidth and redundancy of the EtherChannel. Member links must be configured identically in terms of speed, duplex mode, and encapsulation type to ensure proper functioning of the EtherChannel.

VLAN Trunking Protocol (VTP): a Cisco proprietary protocol designed to manage VLANs (Virtual Local Area Networks) across a network of switches, enabling centralized VLAN management for easier creation, modification, and deletion of VLANs throughout the network. VTP allows switches to share VLAN configuration information, ensuring that changes made on one switch are propagated to all others within the same VTP domain. There are three modes of VTP operation: Server Mode, where switches can create and modify VLANs and send updates; Client Mode, where switches can only receive updates; and Transparent Mode, where switches forward VTP messages without applying them. All participating switches must be configured with the same VTP domain name to exchange VLAN information. Additionally, VTP supports pruning, which optimizes bandwidth by preventing unnecessary VLAN traffic on trunk links to switches without assigned ports in those VLANs. Different versions of VTP exist (VTPv1, VTPv2, VTPv3), with VTPv3 offering enhancements such as improved security and support for private VLANs. While VTP simplifies VLAN management, it requires careful configuration to avoid issues like accidental deletion of VLANs.

Imagine this example again:

- s1 (root switch)
  - g1/0/2 to s2
  - g1/0/3 to s3
- s2
  - g1/0/1 to s1 (root port)
  - g1/0/3 to s3 (designated port)
- s3
  - g1/0/1 to s1 (root port)

- g1/0/2 to s2 (blocked)

If VLAN 4 contained devices only on s2 and s3, the topology could not be tuned with traffic going directly between the two switches. With PVST, the root bridge can be placed on a different switch or can cost ports differently, on a VLAN-by-VLAN basis. This allows for a link to be blocked for one VLAN and forwarding for another.

Routing

”A system of interconnected routers and related components managed under a common network administration is known as an AS, or a routing domain. The internet is composed of thousands of these AS’s spanning the globe.”

The common dynamic routing protocols found on most routing platforms today are as follows:

- Routing Information Protocol Version 2 (RIPv2)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)
- Intermediate System-To-Intermediate System (IS-IS)
- Border Gateway Protocol (BGP)

- Distance Vector algorithms

  distance: the distance is the route metric to reach the network
  vector: the vector is the interface or direction to reach the network

  When routing information is received from another router, it stores that information in a local routing DB. A distance vector algorithm (Bellman-Ford/Ford-Fulkerson) is used to determine which paths are the best loop-free paths to each reachable destination. The best paths are determined, they are installed into the routing table and are advertised (from its perspective) to each neighbor router.

  Routers running distance vector protocols advertise the routing information to their neighbors from their own perspective, modified from the original route received. Therefore, a distance vector protocol does not have a complete map of the whole network; instead, its DB reflects that a neighbor router knows how to reach the destination network and how far the neighbor router is from the destination network. The advantage of distance vector protocols is that they require less CPU and memory and can run on low-end routers.

  ”An analogy commonly used to describe distance vector protocols is a road sign at an intersection indicating that the destination is 2 miles to the west; drivers trust and blindly follow this information, without really knowing whether there is a shorter or better way to the destination or whether the sign is even correct.”

  A distance vector protocol selecs a path purely based on distance. It does not account for link speeds or other factors.

- Enhanced Distance Vector algorithms

  The diffusing update algorithm (DUAL) is an enhanced distance vector algorithm that EIGRP uses to calculate the shortest path to a destination network within a routing domain. EIGRP advertises network information to its neighbors as other distance vector protocols do, but it has some enhancements, as its name suggests.

  - It offers rapid convergence time for changes in the network topology
  - It sends updates only when there is a topological change. It does not send full routing table updates in a periodic fasion, as distance vector protocols typically do.
  - It uses hellos and forms neighbor relationships just as link-state protocols do.
  - It can use bandwidth, delay, reliability, load, and MTU size instead of hop count for path calculations
  - It has the option to load balance traffic across equal-or unequal-cost paths.

- Link-state algorithms

- Path Vector algorithm

- Virtual Routing and Forwarding

Services

Overlay

Wireless

Architecture

Security

SDN

1.0 Architecture 15%

1.1 Explain the different design principles used in an enterprise network

- 1.1.a High-level enterprise network design such as 2-tier, 3-tier, fabric, and cloud
- 1.1.b High availability techniques such as redundancy, FHRP, and SSO

1.2 Describe wireless network design principles

- 1.2.a Wireless deployment models (centralized, distributed, controller-less, controller-based, cloud, remote branch)
- 1.2.b Location services in a WLAN design
- 1.2.c Client density

1.3 Explain the working principles of the Cisco SD-WAN solution

- 1.3.a SD-WAN control and data planes elements
- 1.3.b Benefits and limitations of SD-WAN solutions

1.4 Explain the working principles of the Cisco SD-Access solution

- 1.4.a SD-Access control and data planes elements
- 1.4.b Traditional campus interoperating with SD-Access

1.5 Interpret wired and wireless QoS configurations

- 1.5.a QoS components
- 1.5.b QoS policy

1.6 Describe hardware and software switching mechanisms such as CEF, CAM, TCAM, FIB, RIB, and adjacency tables

2.0 Virtualization 10%

2.1 Describe device virtualization technologies

- 2.1.a Hypervisor type 1 and 2
- 2.1.b Virtual machine
- 2.1.c Virtual switching

2.2 Configure and verify data path virtualization technologies

- 2.2.a VRF
- 2.2.b GRE and IPsec tunneling

2.3 Describe network virtualization concepts

- 2.3.a LISP
- 2.3.b VXLAN

3.0 Infrastructure 30%

3.1 Layer 2

- 3.1.a Troubleshoot static and dynamic 802.1q trunking protocols
- 3.1.b Troubleshoot static and dynamic EtherChannels
- 3.1.c Configure and verify common Spanning Tree Protocols (RSTP, MST) and Spanning Tree enhancements such as root guard and BPDU guard

3.2 Layer 3

- 3.2.a Compare routing concepts of EIGRP and OSPF (advanced distance vector vs. link state, load balancing, path selection, path operations, s, and area types)
- 3.2.b Configure simple OSPFv2/v3 environments, including multiple normal areas, summarization, and filtering (neighbor adjacency, point-to-point, and broadcast network types, and passive-interface)
- 3.2.c Configure and verify eBGP between directly connected neighbors (best path selection algorithm and neighbor relationships)
- 3.2.d Describe policy-based routing

3.3 Wireless

- 3.3.a Describe Layer 1 concepts, such as RF power, RSSI, SNR, interference, noise, bands, channels, and wireless client devices capabilities
- 3.3.b Describe AP modes and antenna types
- 3.3.c Describe access point discovery and join process (discovery algorithms, WLC selection process)
- 3.3.d Describe the main principles and use cases for Layer 2 and Layer 3 roaming
- 3.3.e Troubleshoot WLAN configuration and wireless client connectivity issues using GUI only
- 3.3.f Describe wireless segmentation with groups, profiles, and tags

3.4 IP Services

- 3.4.a Interpret network time protocol configurations such as NTP and PTP
- 3.4.b Configure NAT/PAT
- 3.4.c Configure first hop redundancy protocols, such as HSRP, VRRP
- 3.4.d Describe multicast protocols, such as RPF check, PIM and IGMP v2/v3

4.0 Network Assurance 10%

4.1 Diagnose network problems using tools such as debugs, conditional debugs, traceroute, ping, SNMP, and syslog
4.2 Configure and verify Flexible NetFlow
4.3 Configure SPAN/RSPAN/ERSPAN
4.4 Configure and verify IPSLA
4.5 Describe Cisco DNA Center workflows to apply network configuration, monitoring, and management
4.6 Configure and verify NETCONF and RESTCONF

5.0 Security 20%

5.1 Configure and verify device access control

- 5.1.a Lines and local user authentication
- 5.1.b Authentication and authorization using AAA

5.2 Configure and verify infrastructure security features

- 5.2.a ACLs
- 5.2.b CoPP

5.3 Describe REST API security
5.4 Configure and verify wireless security features

- 5.4.a 802.1X
- 5.4.b WebAuth
- 5.4.c PSK
- 5.4.d EAPOL (4-way handshake)

5.5 Describe the components of network security design

- 5.5.a Threat defense
- 5.5.b Endpoint security
- 5.5.c Next-generation firewall
- 5.5.d TrustSec and MACsec
- 5.5.e Network access control with 802.1X, MAB, and WebAuth

6.0 Automation 15%

6.1 Interpret basic Python components and scripts
6.2 Construct valid JSON-encoded files
6.3 Describe the high-level principles and benefits of a data modeling language, such as YANG
6.4 Describe APIs for Cisco DNA Center and vManage
6.5 Interpret REST API response codes and results in payload using Cisco DNA Center and RESTCONF
6.6 Construct an EEM applet to automate configuration, troubleshooting, or data collection

6.7 Compare agent vs. agentless orchestration tools, such as Chef, Puppet, Ansible, and SaltStack

In the context of IT infrastructure and network automation, orchestration tools help manage and automate configuration, deployment, and management of systems and services. These tools can generally be classified into two categories: agent-based and agentless. Agent-based tools require a software agent to be installed on the managed nodes (servers or devices). This agent communicates with a central management server to receive and execute configuration tasks. Agentless tools do not require an agent on the managed nodes. Instead, they use standard protocols (like SSH or WinRM) to connect to and configure the nodes directly. Chef uses a client-server model where the Chef client (agent) runs on each node. It communicates with the Chef server to retrieve and apply configurations. Chef uses ”recipes” and ”cookbooks” written in Ruby to define configurations. The Chef server stores these recipes and the node’s state. Puppet also uses a client-server model with Puppet agents installed on managed nodes. These agents periodically check in with the Puppet master server to apply configurations. Puppet uses ”manifests” written in its own declarative language to define configurations. The Puppet master server maintains these manifests and the node’s state. Ansible uses a push-based model where configurations are pushed from the Ansible control node to managed nodes over SSH (or WinRM for Windows). No agents are required on the nodes. Ansible uses YAML for defining playbooks which describe the desired state of the systems. It operates in an ad-hoc manner, executing commands as needed. SaltStack offers both agent-based and agentless options. In its agent-based mode, Salt uses Salt minions (agents) on managed nodes. In agentless mode, it can operate over SSH to manage systems. SaltStack uses YAML for defining configurations and states. It supports both push and pull models, and provides real-time command execution capabilities. Choosing between agent-based and agentless orchestration tools depends on factors like the size and complexity of your infrastructure, the level of control and state management required, and the existing toolchain and practices within your organization.