300-115.exam

Number: 300-115
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Cisco

300-115

Implementing Cisco IP Switched Networks (SWITCH)

Version 1.0

Exam A

QUESTION 1
The company has just completed an implementation that uses Cisco Express Forwarding (CEF) as a Layer 3 IP switching technology for optimized network performance and scalability. The following is the network infrastructure of the company. (Click the Exhibit(s) button.)

You are creating the verification plan for this implementation. This includes verifying the routes known to the routers.

Which component of the CEF switching technology contains routes to the 10.1.0.0/24 network along with the routes to the 10.1.1.0/24, 10.1.2.0/24, and 10.1.3.0/24 networks?

A. FIB
B. Adjacency table
C. Routing table
D. Topology table

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The forwarding information base (FIB) lookup table contains routes to 10.1.1.0/24, 10.1.2.0/24, and 10.1.3.0/24. CEF switching technology is an example of a topology-based switching mechanism that uses the FIB. The FIB contains the routing or forwarding information that the network prefix can reference. Thus, the FIB is the component that CEF based switching uses to store a route to 10.1.0.0/24 along with the routes to 10.1.1.0/24, 10.1.2.0/24, and 10.1.3.0/24. In the FIB, these specific entries would be ordered with the longest match followed by less specific subnets. When the switch receives a packet, it can easily examine the destination address and find the longest match entry in the FIB.

The adjacency table does not contain routes to 10.1.1.0/24, 10.1.2.0/24, and 10.1.3.0/24. The adjacency table is used by CEF to prepend Layer 2 addressing information. The adjacency table maintains Layer 2 next-hop addresses for all FIB entries. It stores the information for the nodes that are adjacent. Nodes in the network are said to be adjacent if they can reach each other with a single hop across a link layer.

The routing table does not contain routes to 10.1.1.0/24, 10.1.2.0/24, and 10.1.3.0/24. The router stores routing information, but CEF does not use the routing table for the purpose of making IP destination prefix-based switching decisions.

The topology table does not contain routes to 10.1.1.0/24, 10.1.2.0/24, or 10.1.3.0/24. The topology table is not a component of CEF switching technology. It is a component of EIGRP and stores the details of all the destinations along with the list of neighbors that advertise the destination. For each of these entries, the metrics of the neighbor advertising the destination are also stored.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify switch administration

References:
Cisco > Support > Cisco Express Forwarding Overview

QUESTION 2
What are the three RSTP port states? (Choose three.)

A. Initializing

B. Blocking
C. Learning
D. Listening
E. Forwarding
F. Discarding

Correct Answer: CEF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Rapid Spanning Tree Protocol (RSTP) uses only three port states: discarding, learning, and forwarding. The learning and forwarding states are the same as the original STP standard, but the discarding state performs the functions originally performed in the disabled, blocking, and listening STP states.

With STP, you can safely assume that a listening port is either designated or root, and is on its way to the forwarding state. Unfortunately, once a port is in the forwarding state, there is no way to tell whether the port is root or designated. There is no difference in the operation of a port in blocking state and a port in listening state, since they both discard frames and do not learn MAC addresses. The real difference is in the role the spanning tree assigns to the port. RSTP decouples the role and the state of a port.

With RSTP, a role is assigned to a port. The root port and designated port roles are the same as with STP, while the blocking port role is split into the backup and alternative port roles. The Spanning Tree Algorithm (STA) determines the role of a port based on Bridge Protocol Data Units (BPDUs). The RSTP roles can be defined as follows:

- Root port: The port receiving the best BPDU on a bridge (lowest-cost path to the root bridge) is the root port.
- Designated port: The port that has the best path to the root bridge on a given segment is the designated port. The bridges connected to a given segment listen to each other's BPDUs and agree on the bridge sending the best BPDU as the designated bridge for the segment. The corresponding port on that bridge is the designated port.
- Alternative port: An alternative port is a port blocked by receiving more useful BPDUs from another bridge. It becomes the root port if the active port fails.
- Backup port: A backup port is a port blocked by receiving more useful BPDUs originating from the same bridge. It becomes the designated port if the existing designated port fails.

Ports on the switch can also be classified as edge ports and non-edge ports. Access ports or edge ports are those that attach to devices such as workstations or printers. Non-edge ports are those that connect to other switches. If a non-edge port transitions to a forwarding state, a TC BPDU will be generated. On the other hand, when an edge ports transitions to the forwarding state, such as after a computer boots up or a device is connected to the port, no TC BPDU is generated.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify spanning tree

References:
Cisco > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Technology Information > Technology White Paper > Understanding Rapid Spanning Tree Protocol (802.1w)

QUESTION 3
Which of the following statements best describes the purpose of ARP with respect to CEF?

A. ARP is used to build the FIB.
B. ARP is used to reindex the routing table.
C. ARP is used to build the adjacency table.

D. ARP is used to decrease the amount of time spent searching for an entry within a routing table.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Address Resolution Protocol (ARP) is used by Cisco Express Forwarding (CEF) to build the adjacency table. CEF is the switching method used by Catalyst switches. Unlike traditional multilayer switching (MLS), which merely caches Layer 3 information received when traffic passes through a switch, CEF attempts to optimize the routing process by reindexing the routing table and then building an adjacency table based on the routing table information. The type of MLS performed by CEF is called topology-based switching; traditional MLS is known as route caching, demand-based switching, and flow-based switching.

The routing table is reindexed by using a binary search method. The reindexed routing table is called the forwarding information base (FIB). Reindexing the routing table reduces the amount of time spent searching for an entry within a routing table.

After the FIB is created, an adjacency table is created to map the appropriate Layer 2 next-hop address or addresses to each FIB entry. ARP is used to retrieve the Layer 2 address information. If multiple Layer 2 next-hop addresses are available for an entry in the FIB, then CEF can employ load balancing for packets headed to that destination.

The final result is a single database of routing information (FIB) is built for the switching hardware.

Two extremely useful commands for verifying CEF are:
- show ip cef network address - displays entries in the forwarding information base (FIB)
- show adjacency detail | begin adjacency address - shows information about a specific adjacency in the adjacency table

Both commands are shown below with explanations.

SwitchA# show ip cef 192.168.6.0
192.168.6.0/24, version 302, cached adjacency 192.168.166.5, 0 packets, 0 bytes
Via 192.168.166.5, VLAN 185, 0 dependencies
Next-hop 192.168.166.5, VLAN 185
Valid cached adjacency

Above it can be determined that there is a valid CEF entry for the destination network 192.168.6.0 and that there is a valid cached adjacency to the 192.168.166.5 next hop IP address.

In the command output below, it can be determined that 005565946856 is the MAC address of the 192.168.166.5 next-hop address:

SwitchA# show adjacency detail | begin 192.168.166.5

IP VLAN 185 192.168.166.5(6) 0 packets, 0 bytes
005565946856

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify switch administration

References:
Cisco > Cisco IOS IP Switching Configuration Guide, Release 12.4 > Part 1: Cisco Express Forwarding > Cisco Express Forwarding Overview > Cisco Express Forwarding Adjacency Tables Overview
Cisco > Cisco IOS IP Switching Command Reference > show adjacency through show ipv6 cef with source >

show adjacency
Cisco > Cisco IOS IP Switching Command Reference > show adjacency through show ipv6 cef with source > show ip cef

QUESTION 4
You made changes to a VLAN, but the changes were not propagated to the other switches in the VTP domain. You enter a show vtp command at the switch where the changes were made, which displays the following output:

```
Switch1# show vtp
VTP version: 1
Configuration revision: 4
Maximum VLANs supported locally: 1005
Number of existing VLANs: 3
VTP domain name : Mobile
VTP password :
VTP operating mode : Transparent
VTP pruning mode : Enabled
VTP traps generation : Enabled
Configuration last modified by: 10.1.1.34 at 00-00-0000 00:00:00
```

What should you do to solve this problem?

A. Disable VTP pruning.
B. Change the VTP operating mode to server.
C. Upgrade the VTP version to version 2.
D. Upgrade the VTP version to version 3.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The output of the show vtp command shows that the VTP operating mode is transparent mode. This means that you can make VLAN changes on the switch, but they will only affect that switch. Changes will not be propagated to other switches in the Layer 2 network. You will need to change the operating mode to server if you want to VLAN changes to be propagated to other switches.

To change the VTP operating mode to server, you would enter the vtp server global command as shown:

switch1#(config) vtp server

You should not disable VTP pruning. This will have no effect on the propagation. You must change the mode of the switch.

You should not upgrade the VTP version to version 2 or version 3. This will have no effect on the propagation. You must change the mode of the switch.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Cisco IOS LAN Switching Command Reference > udld through vtp v2-mode > vtp server

QUESTION 5
Which Catalyst 6500 feature provides network-security enforcement based on Layer 2, Layer 3, and Layer 4 information on a VLAN?

A. NAM
B. SPAN
C. VACL
D. 802.1X

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

VLAN access control lists (VACLs) provide network-security enforcement based on Layer 2, Layer 3, and Layer 4 information on a VLAN.

VACLs can be used to provide security based on MAC address, source and destination IP address, Layer 4 protocols, or port numbers. The VACL will act on all traffic of a select VLAN whether bridged or switched. The actions performed on a packet can include permit, redirect, or deny. The VACL entries are checked in sequence, which is similar in concept to route-map structures. The following procedure is used to create VACLs:

Define a VLAN access map:
switch(config)# vlan access-map name [seq#]

Configure a match clause:
switch(config-access-map)# match {ip address {1-99 | 1300-2699 | acl_name} | mac address acl_name}

Configure an action clause:
switch(config-access-map)# action {drop | forward | redirect}

Apply the map to a VLAN:
switch(config)# vlan filter map_name vlan-list list

Once created, you should verify the VACLs using the following commands:

switch# show vlan access-map map_name
switch# show vlan filter

In the sample configuration shown below, all VLAN traffic in VLANS 1 through 3 that match access list SAFE will be forwarded. All other traffic will be dropped.

switch(config)# vlan access-map cisco 10
switch(config-access-map)# match ip-address SAFE
switch(config-access-map)# action forward
switch(config)# vlan filter cisco vlan-list 1-3

If access list cisco were configured as shown below, for example, traffic with a source address of 172.16.10.8 would be dropped.

Switch# show ip access-list cisco 10
Extended ip access list cisco 10
10 permit 10.0.0.0 255.255.255.0 any

Objective:
Infrastructure Security

Sub-Objective:
Configure and verify switch security features

References:
Cisco > Home > Support > Product Support > End-of-Sale and End-of-Life Products > Cisco Catalyst 6000 Series Switches > Configure > Configuration Examples and Technotes > Securing Networks with Private VLANs and VLAN Access Control Lists
Cisco > Cisco IOS LAN Switching Command Reference > vlan access-map
Cisco > Cisco IOS LAN Switching Command Reference > match (vlan access-map)

QUESTION 6
Which characteristics apply to multilayer switching? (Choose three.)

A. Uses CPU-based packet forwarding
B. Performs collision detection
C. Provides isolation of the collision domain
D. Provides Network-layer and Transport-layer access controls
E. Determines the forwarding path based on the Network layer address

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Multilayer switching characteristics include determining the forwarding path based on the Network layer address (Layer 3), providing isolation of the collision domain (Layer 2); and providing Network-layer and Transport-layer access controls (Layers 3 and 4).

Multilayer switching combines the functionalities of Layer 2 switching and Layer 3 switching. Layer 3 switching is routing performed by hardware, specifically by utilizing application-specific integrated circuits (ASICs). The Layer 3 switch can perform all of the basic operations of traditional routers, including the following:
- Path selection based on the packet's Layer 3 protocol information
- Layer 3 packet validation
- Flow accounting (Layers 3 and 4)
- Layer 3-based access controls and security

In contrast to Layer 2 switches, which provide the benefits of bridging, Layer 3 switches offer another high-performance packet switching solution.

CPU- based packet forwarding and collision detection are not unique characteristics of multilayer switching. CPU-based packet forwarding is not a concept used by routers or switches. Collision detection is a characteristic of Ethernet, which is not unique to multilayer switching.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify switch administration

References:
Cisco > Home > Support > Configuring IP MLS > Understanding How IP MLS Works

QUESTION 7
Which IOS command do you use to remove Layer 2 configurations and return an interface to Layer 3 mode?

A. vlan
B. no vlan

C. switchport
D. no switchport

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Use the no switchport command to remove Layer 2 configurations and return an interface to Layer 3 mode. The syntax of the command is:

switch(config-if)# no switchport

The enhanced multilayer switch image must be installed on the switch to use this command.

The switchport command without the no keyword converts the port back to a Layer 2-switched interface.

switch(config-if)# switchport

The vlan vlan-id configuration command is used to configure VLAN characteristics for a specific VLAN. Use the no keyword without additional parameters to delete a VLAN.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify switch administration

References:
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport
Catalyst 3560 Switch Command Reference, Rel. 12.2(25)SEE > Catalyst 3560 Switch Cisco IOS Commands - shutdown through vtp > switchport

QUESTION 8
Which command do you use on a switch to put an interface that is in Layer 3 mode into Layer 2 mode?

A. vlan
B. no vlan
C. switchport
D. no switchport

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Use the switchport command to put an interface that is in Layer 3 mode into Layer 2 mode.

switch(config-if)# switchport

Use the no switchport command to remove Layer 2 configurations and return an interface to Layer 3 mode.

switch(config-if)# no switchport

The enhanced multilayer switch image must be installed on the switch to use this command.

The vlan vlan-id configuration command is used to configure VLAN characteristics for a specific VLAN. Use the no keyword without additional parameters to delete a VLAN.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify switch administration

References:
Catalyst 3560 Switch Command Reference, Rel. 12.2(25)SEE > Catalyst 3560 Switch Cisco IOS Commands - shutdown through vtp > switchport
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport

QUESTION 9
What information is displayed by the command switch# show ip interface brief?

A. a summary of the IP addresses and subnet mask on the interface
B. a summary of the IP addresses on the interface and the interface's status
C. the IP packet statistics for the interfaces
D. the IP addresses for the interface and the routing protocol advertising the network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command show ip interface brief displays a summary of the IP address on the interface and the interface's status. The status means whether the interface is up. This command is useful whenyou are connected a router or switch with which you are not familiar, because it allows you to obtain the state of all interfaces or switch ports. Sample output is shown below:

```
Switch88# show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/1 unassigned YES manual down down
FastEthernet0/2 unassigned YES manual down down
FastEthernet0/3 unassigned YES manual down down
FastEthernet0/4 unassigned YES manual down down
FastEthernet0/5 unassigned YES manual down down
FastEthernet0/6 unassigned YES manual down down
FastEthernet0/7 unassigned YES manual down down
FastEthernet0/8 unassigned YES manual up up
FastEthernet0/9 unassigned YES manual down down
FastEthernet0/10 unassigned YES manual d own down
```

This command does not display subnet mask information. Use other commands, such as show ip interface or show run interface, to verify the subnet mask.

IP statistics about the interface are displayed with the command show ip interface. Adding the brief keyword tells the switch to leave out everything but the state of the interface and its IP address.

To view the routing protocol advertising an interfaces network, you would use the command show ip protocol.

Objective:
Infrastructure Security
Sub-Objective:

Configure and verify switch security features

References:
Cisco > Cisco IOS IP Addressing Services Command Reference > show ip interface

QUESTION 10
Which VTP mode and version should be configured on a switch so that its VLAN database can be separately maintained while it forwards all VTP advertisements it receives?

A. Server mode and version 1
B. Client mode and version 1
C. Server mode and version 2
D. Client mode and version 2
E. Transparent mode and version 2
F. Transparent mode and version 1

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A switch configured in VTP transparent mode allows the administrator to maintain the switch VLAN configuration information and not advertise its database to other switches in the network. A switch configured in VTP transparent mode using version 1 will only forward VTP advertisements it receives if the version used to send the update is also version 1. Using version 2 it will forward advertisements it receives without checking the version number.

There are two versions of VTP: version 1 and version 2. VTP version 1 is the default. The two versions are not interoperable. To support version 2, all of the switches in a network need to be configured to run in VTP version 2.

To enable, or revert back to, VTP version 1 at the configuration prompt, use the following command:

switch(config)# no vtp v2-mode

VTP version 2 offers some features that are not available in version 1.
- Token Ring support: Version 2 provides the ability to support Token Ring LAN parameters, such as ring numbers and hop counts, used in Token Ring LAN switching and VLANs.
- Unrecognized type, length, value (TLV) support: A version 2-enabled switch in server or client modes will propagate configuration changes to its other trunks, even for TLVs it is not able to parse.
- Version-independent transparent mode: In version 1, a transparent mode switch checks the domain name and the version of a received VTP advertisement before forwarding it. Using version 2, it ignores the version when forwarding the advertisement.
- Consistency checks: With version 2, the switch performs consistency checks of VLAN information, such as names and values, when new information is entered through the CLI or using SNMP. It does not do this when updating with information from a new advertisement.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)
Cisco > Cisco IOS LAN Switching Command Reference > udld through vtp v2-mode > vtp

QUESTION 11
Which IOS interface configuration commands are required to configure a switch port to actively negotiate to be an 802.1Q trunk port that, when active, will send packets destined for VLAN 3 untagged? (Choose three.)

A. switchport mode trunk
B. switchport trunk dot1q 3
C. switchport native vlan 3
D. switchport trunk mode dot1q
E. switchport mode dynamic auto
F. switchport trunk native vlan 3
G. switchport trunk encapsulation dot1q

Correct Answer: AFG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Entering the IOS commands switchport mode trunk and switchport trunk encapsulation dot1q in interface configuration mode will allow a switch port to actively negotiate to be an 802.1Q trunk port. Setting the trunk native VLAN to 3 with the command switchport trunk native vlan 3 will allow VLAN 3 traffic to be sent and received untagged over the trunk port.

The command switchport mode trunk instructs DTP to actively negotiate to be a trunk if the other side is set to trunk, desirable, or auto.

Use the following steps to configure a port as an 802.1Q trunk:

1. Enter the interface configuration.
switch(config)# interface interface-id

2. Configure the port to using 802.1Q encapsulation.
switch(config-if)# switchport trunk encapsulation dot1q

3. Configure the port as a trunk port.
switch(config-if)# switchport mode trunk

4. (Optional) Set the native VLAN number.
switchport trunk native vlan number

If the native VLAN is changed as above, it must be changed on both ends of the link. Failure to do so will cause the link to not be successfully built because the native VLAN numbers must match. When left to the default (VLAN 1) the issue takes care of itself. If a native VLAN mismatch occurs, it will be reflected in the debug command output of one of the switches, as shown below.

2009 Aug 11 16:36:11 %SPNTREE-2-RX_IQPVIDERR:Rcvd pvid_inc BPDU on 1Q port 0/2 vlan3
2009 Aug 11 16:36:11 %SPNTREE-2-TX_BLKPORTPVID:Block 0/2 on xmitting vlan 1 for inc peer vlan
2009 Aug 11 16:36:11 %SPNTREE-2-RX_BLKPORTPVID:Block 0/2 on rcving vlan 3 for inc peer vlan 1

Note: Trunking modes can be configured as access, dynamic desirable, dynamic auto, trunk, and nonegotiate. If both sides are set to auto, no negotiations will occur.

The switchport allowed vlan command is also valid for configuring dot1q trunks, but is not required. By default, all VLANs are allowed on the trunk.

Objective:

Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Home > Support > Product Support > Switches > Cisco Catalyst VST 2950 Series Switches > Configure > Configuration Examples and Technotes > Configuring EtherChannel and 802.1Q Trunking Between Catalyst L2 Fixed Configuration Switches and a Router (InterVLAN Routing)
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport trunk
Cisco > Cisco IOS Interface and Hardware Component Command Reference > I through K > interface

QUESTION 12
In which VTP modes can you create and delete local VLANs? (Choose two.)

A. User
B. Host
C. Client
D. Server
E. Transparent

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

There are three modes in VTP: server, client, and transparent. The main differentiator among the three modes is whether a switch can create or delete VLANs. You can create local VLANs in server and transparent VTP modes. However, VLANs created on a switch in transparent mode apply only to that switch, and information about these VLANs is not propagated throughout the VTP domain.

VTP server mode sends or forwards VTP advertisements, synchronizes VLAN configuration information with other switches, and saves the VLAN in NVRAM. To propagate VLAN information, the switch must be configured with a VTP domain name.

VTP transparent mode forwards VTP advertisements and saves the VLAN configuration in NVRAM. It does not synchronize VLAN configuration information. A switch in transparent mode can create, delete, and modify VLANs, but changes are not transmitted to other switches in the domain. Changes only affect the local switch.

VTP client mode sends or forwards VTP advertisements and synchronizes VLAN configuration information with other switches. It does not save VLAN information in NVRAM. In client mode, VTP clients only can receive VLAN information from VTP servers. A Catalyst switch can create, modify, and delete VLANs in server or transparent modes, but not in client mode.

VTP user and host modes do not exist.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)

QUESTION 13
How is a VLAN best described?

A. subnet
B. segment
C. collision domain
D. broadcast domain

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A VLAN can best be described as a broadcast domain. A broadcast domain is a group of devices such that when one device in the group sends a broadcast, all the other devices in the group will receive that broadcast. Switching can segment a flat network into many smaller collision domains, but all stations must process all broadcasts. VLANs solve this problem by creating separate broadcast domains.

A subnet is an IP-addressing division where one subnet's broadcasts are isolated to only that subnet, and no broadcast traffic crosses the subnet divisions without being routed. While in most cases each VLAN may be its own subnet, this is not always the case.

A LAN segment is a general term for a subnet or broadcast domain.

A collision domain is a domain where two or more devices in the domain could cause a collision by sending frames at the same time. Each port on a switch will host a collision domain.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify VLANs

References:
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Configure > Configuration Examples and Technotes > Creating Ethernet VLANs on Catalyst Switches

QUESTION 14
In what mode does an LWAPP-enabled access point operate?

A. lightweight mode
B. autonomous mode
C. WGB
D. ad hoc mode

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Lightweight access point protocol (LWAPP)-enabled access points operate in lightweight mode. LWAPP is a protocol used to allow centralized management of APs. The management components are removed from the APs, and a WLAN controller provides a single point of management. This controller coordinates WLAN access, managing the load on the APs and user movement between APs. Upon starting, an LWAPP-enabled access point must obtain an IP address. It can then discover the controller using DHCP, DNS, or a subnet broadcast. When multiple wireless controllers are detected by an AP, it chooses to associate with the controller that has the fewest existing associated APs.

Individually configured APs that operate without central management are operating in autonomous mode. This would be the opposite of lightweight mode, which is made possible by LWAPP. Autonomous access points can be upgraded to lightweight. If they are upgraded, they will only function in conjunction with a WLAN controller. Moreover, when an autonomous access point is upgraded to lightweight, the console port only provides read access to the unit.

Characteristics that autonomous and lightweight access points have in common:
- Both support Power over Ethernet (PoE)
- Both can use a Cisco Secure Access Control server (ACS) for security

A wireless gateway bridge (WGB) is used to connect a computer without a wireless network card to a wireless network, but not separate WLANs. The WGB can connect up to eight computers to a WLAN. The WGB connects to the root AP through a wireless interface.

Ad hoc is a WLAN mode used for peer-to-peer connectivity. Ad hoc mode allows wireless-enabled computers to communicate with each other without having an AP involved.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify other LAN switching technologies

References:
Cisco > Support > Product Support > Wireless > Cisco Aironet 1200 Series > Reference Guides > Technical References > Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode
Cisco > Support > Technology Support > Wireless/Mobility > Wireless, LAN (WLAN) > Design > Design Technotes > Cisco Wireless Devices Association Matrix

QUESTION 15
Which command produced the following output?

```
VLAN0100
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     00d0.00b8.41a3
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     00d0.00b8.41a3
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa2/4            Desg FWD 200000    128.196  P2p
Fa2/5            Back BLK 200000    128.197  P2p
```

A. switch# show spanning-tree vlan 100
B. switch# show vlan 100
C. switch# show spanning-tree summary
D. switch# show interface vlan 100
E. switch# show spanning-tree inconsistentports

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

The command show spanning-tree vlan 100 was used to provide the output in the exhibit. This output helps to identify the state of each port on the switch that is a member of VLAN 100. It is also used to identify the root bridge in the spanning tree.

The command show vlan 100 will provide basic information about VLAN 100, such as what ports are assigned to it, but will not display the STP information about the VLAN as the exhibit shows.

The command show spanning-tree summary can be used to verify the enabling of the extended system ID. This command is not used to provide the output in the exhibit.

The command show interface vlan 100 displays the same kind of information as would be displayed for any other interface, including the IP address configuration and whether the interface is up. It does not provide STP information about the switch as displayed in the exhibit.

The command show spanning-tree inconsistent port is used to identify inconsistent ports on a switch. This can occur as a result of implementing the Root Guard feature on a switch. Root Guard can be implemented on a port to prevent the reception of superior BPDUs from causing a new root bridge from being elected. This can sometimes occur when a new switch is introduced with an unknown bridge ID. When a port is configured with Root Guard and it receives a superior BPDU, it will block the port, discard the BPDU, and assign a state of inconsistent to the port.

Below is an example of the partial output of the show spanning-tree inconsistent ports command:

```
Switcha# show spanning-tree inconsistentports

Name Interface Inconsistency
-------------------------------------------------
VLAN0010 fastethernet0/1 Root Inconsistent
VLAN0010 fastethernet0/2 Root Inconsistent
VLAN0030 fastethernet0/1 Root Inconsistent
VLAN0030 fastethernet0/2 Root Inconsistent
Number of inconsistent ports (segments) in the system :4
```

The output shows that devices connected to ports Fa0/1 and Fa0/2 are sending superior BPDUs (perhaps from a new switch). Because of this, no traffic will be forwarded across the ports. Once these superior BPDUs are stopped by changing the priority of the new switch, the interfaces will recover and resume normal operation.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify spanning tree

References:
Cisco > Cisco IOS LAN Switching Command Reference > set port flowcontrol through show udld > show spanning-tree

QUESTION 16
You want to create a VTP domain named myvtpdomain and define this switch as one that can be configured with VLANs and advertises VLAN changes to other switches.

What commands should you use? (Choose two.)

A. switch(config)# vtp mode server
B. switch(config)# vtp domain myvtpdomain
C. switch(config)# vtp domain server
D. switch(config)# vtp server myvtpdomain

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

To create a VTP domain and configure the switch so it can configure and advertise VLANs (server mode), use the global configuration commands vtp mode server and vtp domain myvtpdomain. The VTP domain is created with the command switch(config)# vtp domain {domainname}. The mode of the switch is defined with the command switch(config)# vtp mode {mode}. The possible modes are server, client, and transparent. Server means that the switch can be used to create, delete, and modify VLANs; and send and receive advertisements about VLAN changes. Client means that the switch cannot be used to create or change VLANs, but only send and receive advertisements, adjusting its own database to match advertisements that it hears. Transparent means that the switch can be used to create, delete, and modify VLANs; but does not advertise those changes to other switches. Any advertisements that a transparent switch receives are forwarded on to other switches, but not applied by the switch.

The commands vtp domain server and vtp server myvtpdomain are not valid due to incorrect syntax.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)
Cisco > Cisco IOS LAN Switching Command Reference > udld through vtp v2-mode > vtp
Cisco > Cisco IOS LAN Switching Command Reference > udld through vtp v2-mode > vtp domain

QUESTION 17
Which parameters are found in VTP advertisements? (Choose three.)

A. Password
B. VTP mode
C. IP address
D. Switch name
E. Revision number
F. Management domain name

Correct Answer: AEF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The management domain name, password, and revision number are all checked before the VTP frame is processed. To propagate VTP information between switches, both switches must have a trunk port configured and must have a matching native VLAN, which is VLAN 1 by default.

VTP advertisements are flooded throughout the management domain every five minutes or whenever there is a change. These advertisements are originated from a switch that is in server mode and are propagated by switches that are in either client or transparent mode. Before a client or another server accepts or incorporates the information sent in the advertisement, it checks the management domain name and password (if defined) against its own configuration. The revision number is checked. If the revision number is higher than the last

value store in the receiving switch, the receiving switch will overwrite its VLAN database with the information in the advertisement.

A VTP switch in transparent mode will receive and forward VTP advertisements. It will not use the contents of the advertisement to synchronize with its own VLAN database.

The VTP mode, IP address, and switch name are not found in VTP advertisements.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)

QUESTION 18
Which of the following commands configures a port with a VLAN?

A. vlan
B. vlan database
C. switchport access vlan
D. switchport mode access

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The switchport access vlan command configures a port with a virtual local area network (VLAN). The syntax for the switchport access vlan command is as follows:

switchport access vlan {vlan-id | dynamic}

If the vlan-id parameter is specified, then a static VLAN will be configured. If the dynamic keyword is specified, then dynamic VLAN assignment by a VLAN Membership Policy Server (VMPS) will occur. Static VLAN configuration is easy to configure, secure and works well in networks where moves, additions, and changes are rare. In environments where this not the case, dynamic VLANs may be preferable.

The vlan command is used to add VLANs to the VLAN database and to configure VLAN settings.

The vlan database command is issued to enter VLAN configuration mode. The following commands can be issued from VLAN configuration mode:

- abort - exits without applying changes
- apply - applies changes and bumps the revision number
- exit - applies changes, bumps the revision number and exits VLAN configuration mode
- no - negates a command
- reset - discards changes and rereads the VLAN database
- show - displays information
- vlan - configures the VLAN database
- vtp - configures VLAN Trunking Protocol (VTP) settings

The switchport mode access command disables trunking for a port. The syntax for the switchport mode command is as follows:

switchport mode {access | trunk | dynamicdesirable | dynamicauto}

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify VLANs

References:
Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport access

QUESTION 19
A new switch that contains a configuration consisting of only VLAN 5 was just added to the network. Now users assigned to VLANs 9 and 10 are complaining of communication problems.
Using the show vlan command, you discover that only VLAN 5 and the default VLANs exist on all your switches.

What could have caused this problem?

A. The new switch had the default password set.
B. The domain name on the new switch did not match the rest of the network.
C. The new switch was configured in server mode and the revision number was lower than the current number in the network.
D. The new switch was configured in server mode and the revision number was higher than the current number in the network.
E. The new switch was configured in transparent mode and the revision number was higher than the current number in the network.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Adding a switch that is configured in VTP server mode and has a revision number higher than the current number in the network could cause the communication problem in the scenario. If the new switch was configured in server mode and the revision number was higher than the revision number on existing switches, it could cause the rest of the switches to update with the information contained in that new advertisement.

VTP advertisements are flooded throughout the management domain every five minutes or whenever a change occurs in the network. These advertisements are originated from a switch that is in server mode, and are propagated by switches that are in either client or transparent mode. Before a client or another server accepts or incorporates the information sent in the advertisement, it checks the domain name and password (if defined) against its own configuration. Next, the revision number is checked to see if it is higher than the last value stored in the receiving switch. If the revision number is higher, the receiving switch will overwrite its VLAN database with the information in the advertisement.

A VTP switch in transparent mode will receive and forward VTP advertisements. It will not use the contents of the advertisement to synchronize with its own VLAN database.

The password, domain name, and VTP mode will not cause the switch to overwrite the other switches. This is a revision number issue.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify VLANs

References:
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol

(VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)

QUESTION 20
How long does it take for a port to transition from the STP blocking state to the forwarding state by default?

A. 2 seconds
B. 10 seconds
C. 25 seconds
D. 50 seconds
E. 70 seconds

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

It usually takes 50 seconds for a port to transition from the blocking state to the forwarding state in STP. This delay is a function of the default settings for the forward-delay and max-age settings. The max-age delay is 20 seconds by default, and is used to transition from the blocking to the listening state. The forward-delay setting is 15 seconds by default. This timer is used in the transition from the listening to learning states, and again for the transition from the learning to the forwarding state. These timers give STP time to gather the correct information about the network topology. While they can be modified to make convergence more efficient, the default settings work for most networks. To change the timers on all switches in the VTP domain, change the timer settings on the root bridge and the changes will be forwarded to the other switches.

To prevent switching loops, spanning tree transitions each port through several states whenever there is a change in the network topology. Each state is briefly defined as follows:

- Blocking: In the blocking state, a port does not forward frames, learn information, or send information. A forwarding port is placed in the blocked state when the port senses an absence of BPDUs, which are sent in the interval defined by the hello timer (two seconds by default). If the blocked port does not detect a BPDU for the length of time defined in the max-age setting (20 seconds by default), the port will transition into the listening state.
- Listening: In the listening state, a port receives traffic but does not send information. This is the first transitional state after the blocking state. No user data is forwarded at this time, but the switch is very busy. It is during this stage that the switch participates in the election of the root bridge, the designation of root ports on the non-root bridges, and the selection of designated ports on each segment. Ports that are designated or root ports will transition to the learning state after the time defined in the forward delay (15 seconds by default) has elapsed.
- Learning: In the learning state, a switch port can add the MAC addresses that it has learned into its address table, but cannot forward user data. The switch port will remain in this state until the amount of time defined in the forward-delay setting has elapsed (15 seconds by default), at which time it will transition into the forwarding state.
- Forwarding: In the forwarding state, a port is actively forwarding packets. It will remain in the forwarding state until it does not detect a BPDU within the defined hello time, at which time the port is placed in the blocking state and the process starts again.

NOTE: One of the issues that can adversely affect the operation of STP is a duplex mismatch between the NICs on either end of a link between two switches. While this causes more of a performance problem than a loss of the link, the intermittent nature of the outage can cause one of the other links on the switch to transition into a forwarding state, as it may interpret this as a loss of connectivity. If one of the other links switches to forwarding and the link with the duplex mismatch comes back online (which could happen quickly), it can create a switching loop.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify spanning tree

References:
Cisco > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Design > Design Technotes > Understanding and Tuning Spanning Tree Protocol Timers > Document ID: 19120
Cisco > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Design > Design Technotes > Spanning Tree Protocol Problems and Related Design Considerations > Document ID: 10566

QUESTION 21
Which of the following is true about CDP?

A. It can be used to discover the network topology
B. It is used to generate a denial of service attack
C. It can be used as part of a MAC address flooding attack
D. It is used to generate a MAC spoofing attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Cisco Discovery Protocol (CDP) is a Cisco proprietary protocol used by Cisco devices to obtain information about directly connected devices that are also made by Cisco. Since this information includes name, device type and capabilities, IP address, and other identifying information, if these packets are captured they can be used to map the network topology. Since the first step in the hacking process (Discovery, Penetration, and Control) is discovery, this can be a security threat.

CDP is not used to generate a DoS (denial-of-service) attack, which is an attack designed to overwhelm a device with work requests that make it unavailable for its normal jobs.

CDP is not used as part of a MAC address flooding attack. This is performed by a hacker creating packets with unique MAC addresses and flooding the switch's CAM table with these packets. When the CAM buffer is full, the switch will start sending packets out all interfaces enabling the hacker to capture packets from all switch ports, which is normally not possible on a switch, where each port is its own collision domain. CDP plays no role in this process.

CDP is not used to generate a MAC spoofing attack. This type of attack involves the creation of a packet using the MAC address of a known host in the network for the purpose of redirecting traffic to the hacker's machine instead. CDP plays no role in this process.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify Layer 2 protocols

References:
Cisco > Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(37)SG > Configuring CDP

QUESTION 22
Which of the following standards describes the details of RSTP?

A. 802.1d
B. 802.1w
C. 802.1s
D. 802.1x

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

Rapid Spanning Tree Protocol (RSTP) is described in the IEEE 802.1w standard. It has several enhancements over Spanning Tree Protocol (STP), which uses 802.1d. The result of these enchantments is a more rapid convergence when topology changes occur. The two protocols can coexist in the network.

If a switch running RSTP receives an 802.1d Bridge Protocol Data Unit (BPDU), on a port it will begin to use 802.1d rules on that port. However, the IEEE 802.1d standard describes STP and not RSTP.

The IEEE 802.1s standard describes Multiple Spanning Tree Protocol (MST). This enhancement allows for multiple instances of STP. Unlike Common Spanning Tree Protocol (802.1q) and Per-VLAN Spanning Tree Protocol Plus (PVST+), which allow for a single instance of STP or an instance for every VLAN, respectively, MST allows the administrator to map several VLANs to the same instance, without committing them all to the same instance.

IEEE 802.1x describes a standard for port-based access control. It is not related to VLANs or their management.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify spanning tree

References:
Cisco > Home > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Technology Information > Technology White Paper > Understanding Rapid Spanning Tree Protocol (802.1w)

QUESTION 23
The following commands have been issued on a Catalyst switch:

```
switchport trunk allowed vlan all
switchport trunk allowed vlan remove 1,101-4094
switchport trunk allowed vlan except 3001-4094
switchport trunk allowed vlan 1
switchport trunk allowed vlan add 101-200
```

Which of the following VLANs is allowed on the trunk?

A. VLAN 1 and VLANs 101 through 200
B. VLANs 101 through 200
C. VLANs 1 through 3000
D. VLANs 1 through 4094

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Virtual local area network (VLAN) 1 and VLANs 101 through 200 are allowed on the trunk. The switchport trunk allowed vlan command configures a trunk to carry one or more VLANs. The syntax for the switchport trunk

allowed vlan command is switchport trunk allowed vlan {vlan-list | all | {add | except | remove} vlan-list}. VLANs specified in the vlan-list parameter should be separated by commas. However, if a contiguous group of VLANs is specified, the starting and ending VLAN numbers can be separated by a hyphen.

If no keywords are specified with the switchport trunk allowed vlan command, then only the VLANs contained within the vlan-list parameter will be allowed on the trunk. The all keyword specifies that all VLANs from 1 through 4094 should be allowed on the trunk. The add keyword specifies the VLANs that should be added to the list of VLANs that are already allowed by the trunk. The except keyword specifies that all VLANs from 1 through 4094 are allowed except the listed VLANs. The remove keyword specifies the VLANs that should be removed from the list of VLANs that are already allowed by the trunk.

In this scenario, the first command issued is switchport trunk allowed vlan all, which allows VLANs 1 through 4094. The second command issued is switchport trunk allowed vlan remove 1,101-4094, which removes VLAN 1 and VLANs 101-4094. Therefore, VLANs 2 through 100 are allowed. The third command issued is switchport trunk allowed vlan except 3001-4094, which specifies that all VLANs should be allowed except VLANs 3001 through 4094. Therefore, VLANs 1 through 3000 are allowed. The fourth command issued is switchport trunk allowed vlan 1, which specifies that only VLAN 1 should be allowed. The fifth command issued is switchport trunk allowed vlan add 101-200, which adds VLANs 101 through 200 to the list of allowed VLANs. Therefore, VLAN 1 and VLANs 101 through 200 are allowed on the trunk.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport trunk

QUESTION 24
Which of the following statements best describes the result of issuing the instance 3 vlans 7 command?

A. VLAN 7 is mapped to MST instance 3.
B. VLAN 7 is mapped to switchport 3.
C. VLAN 7 is mapped to three MST instances.
D. Seven VLANs are mapped to MST instance 3.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

When the instance 3 vlans 7 command is issued, the virtual local area network (VLAN) 7 is mapped to Multiple Spanning Tree (MST) Protocol instance 3. MST, which is defined by the 802.1s standard, maps a distinct group of VLANs to one STP instance. Multiple STP instances can be used with MST. The Cisco implementation of MST supports 256 instances. However, each instance must support a different group of VLANs because each VLAN can only be mapped to one instance.

To map one or more VLANs to an MST instance, issue the instance instance-ID vlans vlan-range command, where ID is the number of the MST instance and vlan-range is the VLAN or VLANs that should be mapped to the instance. For example, the command instance 1 vlans 14-16,99 maps VLANs 14 through 16 and VLAN 99 to MST instance 1.

The instance 3 vlans 7 command will not map VLAN 7 to switchport 3. The instance vlans command cannot be used to map multiple instances to a single VLAN. Each VLAN can only be mapped to one instance. When the instance 3 vlans 7 command is issued, only a single VLAN will be mapped to MST instance 3.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify spanning tree

References:
Cisco IOS LAN Switching Command Reference > bridge-domain through instance (VLAN) > instance (VLAN)
Cisco > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Technology Information > Technology White Paper > Understanding Multiple Spanning Tree Protocol (802.1s) > Document ID: 24248

QUESTION 25
Which IOS commands are entered in interface configuration mode to configure a switch port to actively negotiate to be an 802.1Q trunk port? (Choose two.)

A. switchport trunk dot1q
B. switchport mode dynamic auto
C. switchport trunk allowed vlan
D. switchport mode trunk
E. switchport trunk encapsulation dot1q

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Entering the IOS commands switchport mode trunk and switchport trunk encapsulation dot1q in interface configuration mode will allow a switch port to actively negotiate to be an 802.1Q trunk port. This allows Dynamic Trunking Protocol (DTP) to actively negotiate to be a trunk if the other side is set to trunk, desirable, or auto.

Use the following steps to configure a port as an 802.1Q trunk:

1. Enter the interface configuration.
switch(config)# interface interface-id

2. Configure the port to use 802.1Q encapsulation.
switch(config-if)# switchport trunk encapsulation dot1q

3. Configure the port as a trunk port.
switch(config-if)# switchport mode trunk

Note: Trunking modes can be configured as dynamic desirable, dynamic auto, trunk, access, and nonegotiate. If both sides are set to auto, no negotiations will occur.

Verification of the configuration can be done by executing the show run command on both switches. An example partial output for two switches is shown below:

```
<output omitted>
hostname switcha
interface fastethernet 0/1
switchport mode dynamic auto
switchport trunk encapsulation dot1q
switchport trunk native vlan 5
<output omitted>
hostname switchb
interface fastethernet0/2
switchport mode dynamic desirable
switchport trunk encapsulation dot1q
```

In the above partial output, the following can be determined:
- Since it is configured as dynamic desirable, SwitchB will send DTP packets to SwitchA
- Since the two switches are set to dynamic desirable and dynamic auto, they will form a trunk. When one end is set to desirable, the other must be set to trunk, desirable, or auto for a trunk link to form.
- The native VLAN for SwitchA is VLAN 5 as indicated in the last line of its output. SwitchB is set to the default, which is VLAN 1. This configuration would result in a failure of the switches to form a trunk since the native VLANs do not match.

The switchport allowed vlan command is also valid for configuring dot1q trunks, but is not required. By default, all VLANs are allowed on the trunk.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco IOS Master Command List, Release 12.4T>switchport mode

QUESTION 26
Which redundancy mode for supervisor engine modules exhibits all of the following characteristics?
- Static routes are maintained during a switchover
- The Forwarding Information Base (FIB) is cleared during a switchover
- Dynamic route information is cleared during a switchover
- Route engine is initialized and switch modules are loaded

A. RPR
B. RPR+
C. SSO
D. NSF

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Redundant supervisor engine modules can be configured in several modes. In route processor redundancy plus (RPR+) mode, the backup module is booted up and the supervisor and route engines initialize. However, no Layer 2 or Layer 3 functions are started, which means it will be necessary to start them after a failover. This also means the routing protocols must re-converge and the FIB table must be rebuilt, since it is derived from

the routing table. The static routes are maintained in the running configuration, so they are not lost in the failover.

In route processor redundancy (RPR) mode, the module is booted, but the supervisor and route engines are not initialized.

In stateful switchover (SSO) mode, all functionality provided by RPR+ is available at failover, and the FIB table is not

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify other LAN switching technologies

References:
Cisco > Catalyst 6500 Release 12.2SX Software Configuration Guide > RPR Supervisor Engine Redundancy
Cisco > Catalyst 6000/6500 Series Switches with Redundant Supervisor Engines Software Image Upgrade Configuration Guide (4.5) > Background Information> Supervisor Engine Redundancy

QUESTION 27
Which Cisco switch feature enables IP phones to be assigned IP addresses from a different subnet than the workstation attached to the same port?

A. Auxiliary VLAN
B. 802.1P
C. 802.1Q
D. in-line power

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Auxiliary VLANs can assist in the deployment of Cisco IP telephones by allowing a Catalyst switch access port to support the data device on one VLAN and have the IP telephone assigned to a different VLAN. The auxiliary VLAN ID is not required to match the native VLAN associated with the access port of the switch. Therefore, the two port attached devices (the phone and the workstation) can be on two different broadcast domains or IP subnets. Some Cisco Catalyst switches provide the auxiliary VLAN feature that provides the automatic assignment of an IP telephone to a VLAN. This auxiliary VLAN feature is also known as the voice VLAN feature.

IP telephones typically have a built in 3-port 10/100 hub. One port internally attaches to the phone, one port is attached to the switch access port, and the last port is used to connect to the workstation. The switch uses CDP on a port on which an auxiliary VLAN has been configured to advertise 802.1Q and 802.1P information. The attached IP telephone can use the advertised information to learn which VLAN ID and priority tag to use. The default Class of Service (CoS) value for incoming traffic is 0.

Having the telephone and the data device use different frame types and belong to different VLANs allows the administrator to place the telephones on their own subnet. Voice traffic on a separate VLAN is less likely to contend with the data devices.

To configure the interface on the switch to support auxiliary VLANs, use the following commands:
- switchport voice vlan VVID: This command is used to enable the access port to forward 802.1Q packets received tagged with the ID of the voice VLAN (VVID) to the VLAN defined as the voice VLAN. By default, 802.1Q packets are sent by IP phones with a QoS priority of 5.
- switchport voice vlan dot1p: This command is used to instruct the attached IP telephone to send packets using the VLAN ID of the port's native VLAN with a dot1p priority of 5.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify VLANs

References:
Cisco > Cisco Catalyst 6500 Series Switches > Data Sheets > Cisco Catalyst 6500 Series 10/100-10/100/1000-MBPS Ethernet Interface Modules Data Sheet
Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport voice vlan

QUESTION 28
What IOS VLAN commands would create a new VLAN and assign it to a port? (Choose two.)

A. switch(config)# vlan 10
B. switch(config-if)# switchport access vlan 10
C. switch(config)# vlan database 10
D. switch(config-if)# switchport vlan 10 enable

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The commands necessary to create a VLAN and assign it to a port are switch(config)# vlan 10 and switch (config-if)# switchport access vlan 10. The global configuration mode is used to create VLANs with the command vlan {vlan_id}. VLANs can be removed with the no form of the command.

Ports are assigned as members of VLANs in the interface configuration mode with the command switchport access vlan {vlan_id}. At this point, if the port is in access mode, it will participate as a member of the VLAN. The mode of the port can be forced to be access in the interface configuration mode with the command switchport mode access.

The command vlan database 10 is not a valid command, but it is similar to a valid command. An optional, but not recommended, way to create a VLAN is in VLAN database mode. This is accessed from global configuration mode with the command vlan database. The prompt would be switch(vlan)#. At this prompt, a VLAN can be created with the command vlan 10. The problem with VLAN database mode is that the configurations issued here have to be applied with either the apply or exit commands. Using CTRL-Z to exit would cancel the changes made in this mode.

The command switchport vlan 10 enable is not correct due to invalid syntax.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify VLANs

References:
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Configure > Configuration Examples and Technotes > Creating Ethernet VLANs on Catalyst Switches
Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport access
Cisco > Cisco IOS LAN Switching Command Reference > udld through vtp v2-mode > vlan

QUESTION 29

Which devices are required to provide connectivity between VLANs? (Choose two.)

A. hub
B. router
C. bridge
D. multilayer switch
E. DSU/CSU

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Routing between different VLANs can be accomplished using VLAN-capable multilayer switches or routers.

Devices within a single VLAN can communicate without the aid of a Layer 3 device, but as a rule, devices in different VLANs require a Layer 3 device for communication. The only situation where two computers in different VLANs located on different switches can ping one another is if they have addresses in the same subnet, and if the link between the two switches is an access port rather than trunk port.

Since traffic is sent untagged in an access link, if the link between the switches is an access link and the computers are in the same subnet, they will be able to ping one another. The following steps can be used to configure inter-VLAN routing on a multilayer switch:

1. Enable IP routing.
switch(config)# ip routing

Note: Routing must be enabled on a Layer 3 switch for interVLAN routing to occur. This can be verified by examining the output of the show run command executed on the switch. The example below is output from the show run command executed on a switch that has IP routing enabled, as can be seen in the third line (ip routing):

```
hostname SwitchA
!
ip subnet-zero
ip routing
!
vtp domain Cisco
vtp mode transparent
<output omitted>
```

2. Specify an IP routing protocol, such as RIP.
switch(config)# router rip

3. Specify a VLAN interface.
switch(config)# interface vlan vlanid

4. Assign an IP address to the VLAN.
switch(config-if)# ip address address subnet-mask

Hubs operate at the Physical layer (Layer 1) and do not have the ability to route.

Bridges operate at the Data Link layer (Layer 2) and do not have the ability to route.

CSU/DSUs convert signals from a LAN to a type necessary for the telco. They do not have the ability to route.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Home > Support > Technology Support > LAN Switching > Layer-Three Switching and Forwarding > Configure > Configuration Examples and Technotes > Configuring InterVLAN Routing with Catalyst 3750/3560/3550 Series Switches

QUESTION 30
What attack technique attempts to fill a switching table so the attackers can capture traffic passing through a switch?

A. VLAN hopping
B. MAC spoofing
C. Rogue device
D. MAC flooding

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

MAC flooding is an attack technique in which frames with unique, but invalid, source MAC addresses flood the switch and exhaust the CAM table space. Eventually no more MAC addresses can be added because the table is full. When this occurs, any packets destined for a MAC address not in the table will be flooded to all other ports. This would allow the attacker to see the flooded traffic and capture information. The switch would be essentially functioning as a hub in this case.

Two methods of mitigating these attacks are:
- Implementing port security
- Implementing VLAN access maps

VLAN hopping is an attack that allows an attacker to access network resources on a different VLAN without passing through a router. The attacker can create a packet with two 802.1Q VLAN headers on it (called double tagging) and send it to a switch. The switch port will strip off the first header and leave the second. The second header will be seen as the originating VLAN, allowing the attacker access to a VLAN they are not connected to. Executing the switchport mode access command on all non-trunk ports can help prevent this attack. Pruning the native VLAN from a trunk link can also help.

VLAN hopping is a security concern because it can be accomplished without the packet passing through a router and its security access lists. For this reason, private VLANs and VACLs should be used to secure access between VLANs. Techniques to prevent these attacks are:
- Prevent automatic trunk configurations by explicitly turning off Dynamic Trunking Protocol on all unused ports
- Place unused ports in a common unrouted VLAN

MAC spoofing is an attack that allows an attacking device to receive frames intended for a different host by changing an assigned Media Access Control (MAC) address of a networked device to a different one. Changing the assigned MAC address may allow the device to bypass access control lists on servers or routers, either hiding a computer on a network or allowing it to impersonate another computer.

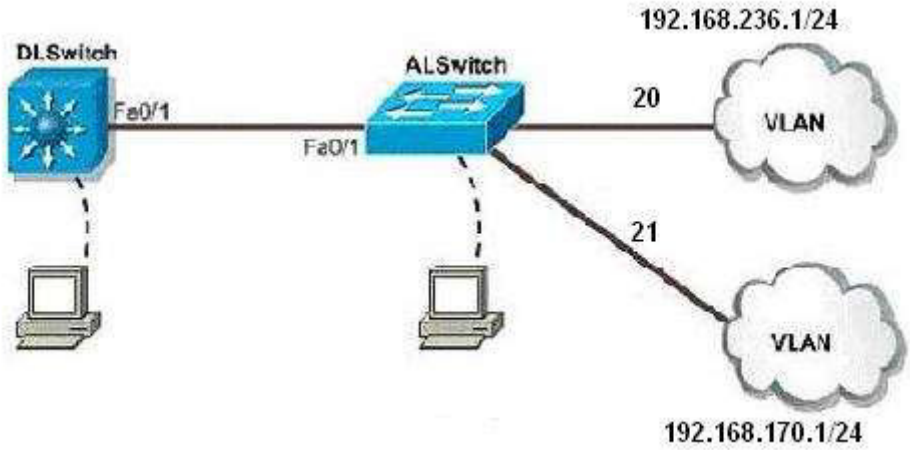
A rogue device is a device attached to the network that is not under the control of the organization. This term is

normally used to mean a wireless device, perhaps an access point that is not operating as a part of the company's infrastructure. Employees may bring their own access points and connect them to the network so they can use their computer wirelessly. This creates a security gap since the device is probably not secured to protect the traffic. An attacker could connect a rogue access point to a company's network and capture traffic from outside the company's premises.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify switch administration

References:
Cisco > Products and Services > Switches > Cisco Catalyst 6500 Series Switches > Product Literature > White Papers > Cisco Catalyst 6500 Series Switches > VLAN Security White Paper > MAC Flooding Attack

QUESTION 31
A company has a following network infrastructure. Refer to the exhibit:



To enable inter-VLAN routing on the distribution layer switch, which of the following commands should be used?

A. dlswitch# switchport mode access
B. dlswitch (config) # switchport mode trunk
C. dlswitch(config-if) # switchport mode trunk
D. dlswitch(config-if) # switchport mode access

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

You should use switchport mode trunk command at the interface configuration prompt to enable inter-VLAN routing. This command sets the port as a trunk port. Trunks carry traffic from all VLANs to and from the switch by default, and can be configured to carry specific VLAN traffic as well.

A port on a Cisco switch is either an access port or a trunk port. An access port only carries traffic for the VLAN of which it is a member and does not tag or mark the frame with a VLAN ID. A trunk port carries traffic from multiple VLANs and tags or marks each frame with a VLAN ID so it can be determined where it goes when it gets to the other switch.

You can enable inter-VLAN routing by enabling trunking using the following command:

switchport mode trunk

You would not use the dlswitch# switchport mode access command to enable inter-VLAN routing. This command sets the port as an access port, which is capable of carrying only the traffic a single VLAN. Moreover, even if that were the intent, the command must be executed in interface mode and not global configuration mode.

You would not use the dlswitch (config) # switchport mode trunk command to enable inter-VLAN routing. This is the correct command, but is shown being executed in global configuration mode instead of interface mode.

You would not use the dlswitch(config-if)# switchport mode access command to enable inter-VLAN routing. This is both the wrong command and is being executed at an incorrect prompt.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco Press > Articles > Network Technology > General Networking > VLANs and Trunking
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport mode trunk

QUESTION 32
Which IOS commands should you enter in interface configuration mode to configure a switch port as an access port and assign it to VLAN 25? (Choose two.)

A. trunk on
B. switchport mode access
C. vlan-membership static 25
D. switchport access vlan 25

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Use the following steps to assign ports to a VLAN:

1. Enter the interface to be added to the VLAN.
switch(config)# interface interface-id

2. Configure the port as a Layer 2 access port.
switch(config-if)# switchport mode access

3. Assign the port to a VLAN.
<fon

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify VLANs

References:
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport access vlan

QUESTION 33
What Cisco switch feature allows IP phones to be automatically placed into a separate VLAN from data traffic?

A. marking
B. AutoQoS
C. private VLANs
D. auxiliary VLANs

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Auxiliary VLANs allows IP phones to be automatically placed into a separate VLAN from data traffic. The information the phones need regarding this voice VLAN is provided by the switch. This allows the data and voice traffic to use the same physical topology but remain logically separate. The following is an example of the commands that should be executed on the switch to instruct it to provide this information to the IP phone by CDP:

Switch> (enable) set port auxiliaryvlan 2/1-3 222

This command creates the auxiliary VLAN 222 and adds ports 2/1 to 2/3 to the VLAN.

Private VLANs are not used for voice traffic. Private VLANs are secondary VLANs created by an administrator that are not accessible by other secondary VLANs.

Marking is the process of setting the Class of Service (CoS), IP precedence, or DSCP of a packet to a specific value that will provide appropriate QoS throughout the network. It is not involved in separating voice and data traffic.

Auto QoS is a method of configuring commonly used QoS features on a Cisco switch with a single command. It is not involved in separating voice and data traffic.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify VLANs

References:
Cisco > Catalyst 4500 Series Software Configuration Guide, 8.1 > Configuring VLANs > Configuring Auxiliary VLANs

QUESTION 34
Which IOS command configures a switch for VTP client mode?

A. vtp mode client
B. no vtp v2-mode
C. no vtp mode
D. vtp terminal

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

To configure a switch to operate as a VLAN Trunk Protocol (VTP) client, simply enter the vtp mode client command at the global configuration prompt:

switch(config)# vtp mode client

When a switch is in VTP client mode, you cannot change its VLAN configuration. The switch will receive VTP updates from a VTP server in the VTP domain and then modify its configuration accordingly.

For added security, you can specify the VTP domain to which the client belongs and a password used to connect to the domain when configuring a switch for VTP client mode. The password is the same for all devices in the VTP domain. The commands to configure a VTP password are as follows:

switch(config)# vtp domain domain-name
switch(config)# vtp password password

The no vtp v2-mode command reverts the VTP version to version 1 (the default version). Use the vtp v2-mode command to set the VTP mode to version 2.

The no vtp mode command reverts the VTP mode back to its default state, which is server mode. To set the VTP mode of a VTP client back to server mode, you can use either the no vtp mode command or the vtp server command.

vtp terminal is not a valid command.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)
Cisco > Cisco IOS LAN Switching Command Reference > udld through vtp v2-mode > vtp

QUESTION 35
Which IOS commands do you enter in interface configuration mode to configure a switch port to actively negotiate to be an ISL trunk port if possible? (Choose two.)

A. switchport trunk isl
B. switchport mode dynamic auto
C. switchport trunk allowed vlan
D. switchport mode dynamic desirable
E. switchport trunk encapsulation isl

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Entering the IOS commands switchport mode dynamic desirable and switchport trunk encapsulation isl in interface configuration mode will allow a switch port to actively negotiate to be an ISL trunk port if possible.

Use the following steps to configure a port as an ISL trunk:

1. Enter the interface configuration.

switch(config)# interface interface-id

2. Configure the port to use ISL encapsulation.
switch(config-if)# switchport trunk encapsulation isl

3. Configure the port as a trunk port.
switch(config-if)# switchport mode dynamic desirable

Note: Trunking modes can be configured as trunk, dynamic auto, dynamic desirable, nonegotiate, and access.

This allows DTP to actively negotiate to be a trunk if the other side is set to trunk, desirable , or auto. If one side is set to auto and the other side is also set to auto, no negotiations will occur.

The switchport allowed vlan command is also valid for configuring dot1q trunks, but is not required. By default, all VLANs are allowed on the trunk.

The other commands use incorrect syntax.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport trunk
Cisco > Cisco IOS Interface and Hardware Component Command Reference > I through K > interface

QUESTION 36
What information is displayed by the command switch# show ip interface brief?

A. a summary of the IP addresses and subnet mask on the interface
B. a summary of the IP addresses on the interface and the interface's status
C. the IP packet statistics for the interfaces
D. the IP addresses for the interface and the routing protocol advertising the network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command show ip interface brief displays a summary of the IP address on the interface and the interface's status. The status means whether the interface is up. This command is useful when you are connected to a router or switch with which you are not familiar, because it allows you to obtain the state of all interfaces or switch ports. Sample output is shown below:

```
Switch88# show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/1 unassigned YES manual down down
FastEthernet0/2 unassigned YES manual down down
FastEthernet0/3 unassigned YES manual down down
FastEthernet0/4 unassigned YES manual down down
FastEthernet0/5 unassigned YES manual down down
FastEthernet0/6 unassigned YES manual down down
FastEthernet0/7 unassigned YES manual down down
FastEthernet0/8 unassigned YES manual up up
FastEthernet0/9 unassigned YES manual down down
FastEthernet0/10 unassigned YES manual d own down
```

This command does not display subnet mask information. Use other commands, such as show ip interface or show run interface, to verify the subnet mask.

IP statistics about the interface are displayed with the command show ip interface. Adding the brief keyword tells the switch to leave out everything but the state of the interface and its IP address.

To view the routing protocol advertising an interfaces network, you would use the command show ip protocol.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify VLANs

References:
Cisco > Cisco IOS IP Addressing Services Command Reference > show ip interface

QUESTION 37
At which OSI layer does STP operate?

A. Physical
B. Network
C. Transport
D. Data Link

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Spanning Tree Protocol (STP) operates at the Data Link layer (Layer 2) of the OSI model.

Switches and bridges running the spanning-tree algorithm communicate by exchanging multicast messages called bridge protocol data units (BPDUs) at regular intervals. BPDUs are used to build and maintain the spanning tree, ensuring a stable loop-free topology.

BPDU exchange facilitates the following:
- Election of a root switch (only one per spanning tree)
- Election of a designated switch for each switched segment
- Removal of loops by placing redundant switch ports in a backup (non-forwarding) state

STP is implemented on bridges and switches in order to prevent loops in the network. STP should be used in situations where redundant links are used.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify spanning tree

References:
Cisco > Home > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Configure > Configuration Examples and Technotes > Spanning Tree Protocol > Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches
Cisco > Support > Configuring Spanning Tree Protocol > How STP Works

QUESTION 38
Which feature can you enable on a switch to prevent potential bridging loops caused by invalid configurations on PortFast-configured interfaces?

A. UDLD
B. Root Guard
C. BPDU Guard
D. Loop Guard

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

BPDU Guard prevents bridging loops caused by an invalid configuration on a PortFast-configured interface by shutting down the interface when it receives BPDUs.

PortFast-configured interfaces should not receive BPDUs in a valid configuration because only end devices should be connected to the PortFast interfaces (only switches and bridges send BPDUs). However, if a switch were improperly connected to the PortFast-configured interface, it would begin to receive BPDUs from the switch at the other end of the link. The port would immediately go into the spanning-tree blocking state and the port would begin to send BPDUs, which could cause a bridging loop. BPDU Guard can prevent this situation by providing a secure response to BPDUs received on PortFast-configured interfaces. When enabled, BPDU Guard shuts down a PortFast-configured interface when it receives BPDUs. When BPDU Guard brings down an interface, the interface stays down until an administrator manually puts it back into service.

The following command enables BPDU Guard on an interface:

switch(config-if)# spanning-tree portfast bpduguard

To further enhance the ability of Root Guard to prevent the introduction of rogue switches in the network, PortFast can be used as well to shut down the port when a switch is connected to it. When you globally enable BPDU guard, STP shuts down ports that receive BPDUs. This is called STP PortFast BPDU Guard.

The following command enables STP PortFast BPDU Guard globally.

switch(config)# spanning-tree portfast bpduguard default

Unidirectional Link Detection (UDLD) improves the stability of Layer 2 networks by detecting and shutting down unidirectional links.

Root Guard provides a mechanism for enforcing root-bridge placement in the network. When enabled on a Layer 2 access port, it forces the port to become a designated port. Root Guard prevents the port from becoming an STP root port.

Loop Guard provides protection against Layer 2 forwarding loops in a physically redundant topology by moving

a non-designated port that has not received BPDUs as expected into the STP loop-inconsistent blocking state, preventing the port from cycling through the normal STP listening, learning, and forwarding states. It cannot be used to force a Layer 2 access port to become a designated port. Loop guard can be implemented on a switch either globally or per interface with the following commands.

Globally. the command would be:

switch(config)# spanning-tree loopguard default

Per interface, the commands would be:

switch(config)# interface fastethernet0/1
switch(config-if)# spanning-tree guard loop

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify spanning tree

References:
Cisco > Cisco IOS LAN Switching Command Reference > show vlan through ssl-proxy module allowed-vlan > spanning-tree portfast bpduguard default

QUESTION 39
Which parameters in VTP advertisements are checked before being accepted and processed? (Choose three.)

A. VLAN ID
B. Password
C. VTP mode
D. Switch name
E. Revision number
F. Management domain name

Correct Answer: BEF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The management domain name, password, and revision number are all checked before the VTP frame is processed.

VTP advertisements are flooded throughout the management domain every five minutes or whenever there is a change. These advertisements are originated from a switch that is in server mode and are propagated by switches that are in either client or transparent mode. Before a client or another server accepts or incorporates the information sent in the advertisement, it checks the management domain name and password (if defined) against its own configuration. The revision number is then checked. If the revision number is higher than the last value stored in the receiving switch, the receiving switch will overwrite its VLAN database with the information in the advertisement.

A VTP switch in transparent mode will receive and forward VTP advertisements. It will not use the contents of the advertisement to synchronize with its own VLAN database.

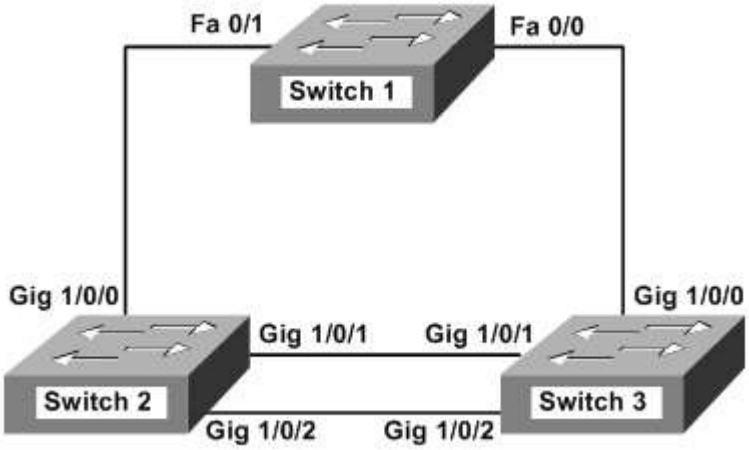
To set the VTP mode of a switch execute the following command at the global prompt. All switches are set to server mode by default; therefore, the command is only necessary to set a switch to client or transparent mode. The command syntax is:

switch(config)# vtp mode {transparent | client}

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Configure > Configuration Examples and Technotes > All Transparent VTP Domain to Server-Client VTP Domain Migration Configuration Example
Cisco > Cisco IOS LAN Switching Command Reference > udld through vtp v2-mode > vtp

QUESTION 40
You have three switches connected as shown in the diagram below: S1, S2, and S3.



You instructed your assistant to configure the switches so that the following requirements would be met:
- Switch 1 should be the root bridge for VLAN A
- VLAN C should forward over the Gig 1/0/1 link between Switch 2 and Switch 3
- VLAN B should forward over the Gig 1/0/2 link between Switch 2 and Switch 3

However, after your assistant performs the configuration, you discover that:
- Switch 2 is the root bridge for VLAN A
- VLAN C is forwarding over the Gig 1/0/2 link between Switch 2 and Switch 3
- VLAN B is forwarding over the Gig 1/0/1 link between Switch 2 and Switch 3

When you execute the show spanning tree command on Switch 2, you determine that all link costs and priorities are set at the defaults.

Which of the following actions performed on Switch 2 would enable the desired configuration? (Choose three. Each correct answer is part of one solution.)

A. switch2(config)# spanning-tree vlan a priority 61440
B. switch2(config)# spanning-tree vlan a priority 1
C. switch2(config)# int G1/0/2switch2(config-if)# spanning-tree vlan b cost 1
D. switch2(config)# int G1/0/2switch2(config-if)# spanning-tree vlan b cost 19
E. switch2(config)# int G1/0/1switch2(config-if)# spanning-tree vlan c port-priority 64
F. switch2(config)# int G1/0/1switch2(config-if)# spanning-tree vlan c port-priority 128

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The commands that will achieve the desired results are:

switch2(config)# spanning-tree vlan a priority 61440
switch2(config)# interface G1/0/2
switch2(config-if)# spanning-tree vlan b cost 1
switch2(config)# interface G1/0/1
switch2(config-if)# spanning-tree vlan c port-priority 64

The first command raises the bridge priority for Switch 2 with respect to VLAN A, which will cause Switch 1 to be the root bridge for VLAN A. By default, the bridge priorities for Switch 2 and Switch 3 will set to 32769.

The second command will lower the cost of G1/0/2 with respect to VLAN B. Since the cost for G1/0/1 is the default cost of 4, this will cause interface G1/0/2 to become the root port for VLAN B, which will in turn cause it to forward instead of block for VLAN B.

The third command will lower the port priority for G1/0/1 with respect to VLAN C. Since the port priority of G1/0/2 will remain set at the default of 128, this will result in switching the ports that are blocking and forwarding. The end result will be that VLAN C will start forwarding over the Gig 1/0/1 link between Switch 2 and Switch 3.

The other commands will have no effect because they change the cost and port priority to the defaults, which are how the links are currently set.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify spanning tree

References:
Cisco IOS LAN Switching Configuration Guide, Release 12.4 > EtherSwitch Network Module > Configuring Spanning Tree on a VLAN > VLAN Root Bridge and VLAN Bridge Priority

QUESTION 41
You have executed the following set of commands on a Layer 3 switch:

```
switchA(config)# ip routing
switchA(config)# vlan 5
switchA(config-vlan)# name Finance
switchA(config-vlan)# exit
switchA(config)# interface Fa0/1
switchA(config-if)#no switchport
switchA(config-if)# ip address 10.55.5.1 255.255.255.0
switchA(config-if)# switchport mode access
switchA(config-if)# switchport access vlan 5
switchA(config-if)# no shutdown
switchA(config-if)# interface Fa0/2
switchA(config-if)# ip address 10.55.5.1 255.255.255.0
switchA(config-if)# switchport mode trunk
switchA(config-if)# switchport trunk encapsulation dot1q
switchA(config-if)# no shutdown
switchA(config-if)# exit
switchA(config)# interface vlan 5
switchA(config-if)# ip address 10.33.3.1 255.255.255.0
switchA(config-if)# no shutdown
```

You have verified that the configuration on all the physical and logical interfaces is correct. All the Layer 2 interfaces configured on the switch are in the up/up state.

What is the state of the VLAN and the line protocol when you execute the show interfaces vlan 5 command?

A. administratively down/down
B. down/down
C. up/up
D. up/down

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The VLAN and the line protocol are in the up/up state when you execute the show interfaces vlan 5 command. You can view the state of the VLAN and the line protocol using the show interfaces vlan command, which is as follows:

switchA# show interfaces vlan 5
Vlan5 is up, line protocol is up
Hardware is Ethernet SVI, address is 031B.70A2.166F (bia 031B.70A2.166F)
Internet address is 10.33.3.1/24
<output omitted>

As you can see in the given output, the text Vlan5 is up, line protocol is up indicates that VLAN 5 and the Layer 2 line protocol both are in the up state. Both the VLAN and line protocol are in the up/up state if the following conditions are true:

The VLAN is configured on the switch and is enabled in the VLAN database

The VLAN is not in the administratively down state

The VLAN has at least one Layer 2 (access or trunk) port in the up state

The VLAN and the line protocol will not be in the administratively down/down state. An interface is in the administratively down state only when the shutdown command is used on that interface. In this case, the no shutdown command is used on the VLAN 5 interface, not the shutdown command. The no shutdown command enables the VLAN 5 interface.

The VLAN and the line protocol will not be in the down/down state. An interface is the down state when there is some Layer 1, Layer 2, or Layer 3 problem such as incorrect cabling used or an incorrect IP address assigned. Interfaces can also be in the down state if the either of the interfaces at the end of a link is in down state due to erroneous configuration. However, in this case, the configuration is correct and the VLAN 5 is in the up state because of the no shutdown command.

The VLAN and the line protocol will not in the up/down state. An interface is the down state when there are some Layer 1, Layer 2, or Layer 3 problems such as incorrect cabling used or an incorrect IP address assigned. In Layer 3 switches, line protocol will be in the down state if all of the Layer 2 ports in the VLAN are in the down state. In this case, the configuration is correct and all the ports in VLAN 5 are in the up state. This implies that that the line protocol cannot be in the down state.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify VLANs

References:
Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(37)SG > Configuring Layer 3 Interface > Configuring VLANs as Layer 3 Interfaces
Home > Articles > Network Technology > Routing & Switching > Cisco LAN Switching Fundamentals: Configuring Switches > Configuring the Access Layer
Home > Support > Technology Support > LAN Switching > Layer-Three Switching and Forwarding > Configure > Configuration Examples and Technotes > How to Configure InterVLAN Routing on Layer 3 Switches > Configure InterVLAN Routing

QUESTION 42
Consider the following commands executed on a Layer 3 switch named switchA:

```
switchA(config)# ip routing
switchA(config)# vlan 10
switchA(config-vlan)# name Finance
switchA(config-vlan)# exit
switchA(config)# interface Fa0/1
switchA(config-if)# ip address 10.1.1.1 255.255.255.0
switchA(config-if)# switchport mode access
switchA(config-if)# switchport access vlan 10
switchA(config-if)# no shutdown
switchA(config)# interface Fa0/2
switchA(config-if)# ip address 10.2.2.2 255.255.255.0
switchA(config-if)# switchport mode access
switchA(config-if)# switchport access vlan 10
switchA(config-if)# switchport autostate exclude
switchA(config-if)# no shutdown
switchA(config)# interface Fa0/3
switchA(config-if)# ip address 10.3.3.3 255.255.255.0
switchA(config-if)# switchport mode access
switchA(config-if)# switchport access vlan 10
switchA(config-if)# switchport autostate exclude
switchA(config-if)# no shutdown
switchA(config-if)# interface Fa0/4
switchA(config-if)# ip address 10.4.4.4 255.255.255.0
switchA(config-if)# switchport mode access
switchA(config-if)# switchport access vlan 10
switchA(config-if)# no switchport autostate exclude
switchA(config-if)# no shutdown
switchA(config-if)# interface vlan 10
switchA(config-if)# ip address 10.66.66.1 255.255.255.0
switchA(config-if)# no shutdown
```

Which of the following physical interfaces do NOT affect the uplink state of VLAN 10? (Choose two.)

A. Fa0/1
B. Fa0/2
C. Fa0/3
D. Fa0/4

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The Fa0/2 and Fa0/3 physical interfaces of switchA do not affect the uplink state of VLAN 10. This is because the switchport autostate exclude command is used on the Fa0/2 and Fa0/3 interfaces. This command causes the exclusion of an interface from the determination of the uplink state of the VLAN (SVI interface) to which the interface belongs.

An SVI or switch virtual interface is a logical interface that allows you to enable inter-VLAN routing on Layer 3 switches. SVIs are configured as VLAN interfaces and have at least one physical interface assigned to the VLANs. An SVI is up and running when all of the following conditions are met:

- It is configured on the switch and is enabled in the VLAN database
- It is not in the administratively down state
- It has at least one Layer 2 (access or trunk) interface in the up state

When an SVI services multiple interfaces (the switch ports in the VLAN to which the SVI connects) and all of

them go down, the SVI also goes down by default. When any of the interfaces comes up, the SVI also comes up. By default, all interfaces assigned to the SVI are involved in determining its uplink state. However, if you do not want a particular interface to participate in this determination, use the switchport autostate exclude command on that interface.

You can use the switchport autostate exclude command on any Layer 2 access or trunk interface. This command applies to all VLANs to which the interface belongs. If the excluded interface of an SVI is in the up state and all the other interfaces of the SVI are in the down state, the SVI remains in the down state. The state of the SVI does not change to up.

The Fa0/1 and Fa0/4 interfaces of switchA affect the uplink state of VLAN 10 because all the interfaces assigned to an SVI contribute towards the uplink state determination of the SVI by default.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify VLANs

References:
Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(37)SG > Configuring Layer 3 Interfaces > Configuring VLANs as Layer 3 Interfaces > Understanding SVI Autostate Exclude
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport autostate exclude

QUESTION 43
Inter-VLAN routing has been operating successfully for several months. Users who connect to a newly installed switch report that they are unable to communicate with the rest of the company's networks. You decide to ensure that the switch is properly connected to the VTP domain before taking any other troubleshooting steps.

What command would be best used to verify this?

A. switch# show vlan
B. switch# show ip route
C. switch# show interfaces trunk
D. switch# show vtp status
E. switch #show interface

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command show vtp status would be the best command to verify the switch's connection to the company's VTP domain. This command displays the version of VTP, the VTP domain the switch is a member of, the VTP mode of the switch, and other configuration settings relating to VTP.

The command show vlan will display the VLANs that exist and the ports that are members of the VLANs, but will not identify whether switch is a member of the VTP domain. If the VLANs that are displayed with this command are the same as those in the VTP domain, it does not necessarily mean the switch is a member of the domain. This data needs to be verified with the show vtp status command.

The command show ip route is used to verify the routing table, but it does not provide any VTP information. This command is used to verify routes to other networks discovered or configured on the switch. It will display the routing protocol used to discover each route, and the next hop used to forward traffic to the destination network.

The command show interfaces trunk is used to verify which VLANs are being forwarded to another device, but does not indicate whether the switch is a member of the VTP domain.

The command show interfaces would not allow you to verify the switch's connection to the company's VTP domain. This command would allow you to determine the following features of the switch:

- Port state
- Port speed
- Input errors
- Collisions

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.1(13)EW > Understanding and Configuring VTP
Cisco > Cisco IOS LAN Switching Command Reference > show vlan through ssl-proxy module allowed-vlan > show vtp

QUESTION 44
Consider the following output from the show interfaces trunk command:

```
Port Mode Encapsulation Status Native VLAN
gi0/1 desirable isl trunking 1

Port Vlans allowed on trunk
gi0/1 1-43,45-4094

Port Vlans allowed and active in management domain
gi0/1 1-17,40,43,101-172

Port Vlans in spanning tree forwarding state and not pruned
gi0/1 1-12,16,40,101-172
```

Which two of the following statements can be confirmed regarding the trunking configuration on the switch? (Choose two.)

A. VLAN 44 is allowed on the trunk.
B. VLAN 46 is not allowed on the trunk.
C. VLAN 45 is configured for the VTP domain.
D. VLAN 41 is not configured for the VTP domain.
E. VLAN 43 is pruned or is not in the spanning-tree forwarding state.
F. VLAN 41 is not pruned.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Virtual local area network (VLAN) 41 is not configured for the VLAN Trunking Protocol (VTP) domain, and VLAN 43 is pruned or is not in the spanning-tree forwarding state. The show interfaces trunk command can be used to determine which VLANs are allowed, which VLANs are configured for the VTP domain, and which VLANs are in the spanning-tree forwarding state and are not pruned.

The VLANs listed under the Vlans allowed on trunk section are allowed on the trunk. Therefore, VLANs 1 through 43 and 45 through 4094 are allowed on the trunk. VLAN 44 is not allowed on the trunk; VLAN 46 is

allowed on the trunk.

The VLANs listed under the Vlans allowed and active in management domain section are allowed on the trunk and configured for the VTP domain. In this scenario, this section includes VLANs 1 through 17, VLAN 40, VLAN 43, and VLANs 101 through 172. Because VLANs 41 and 45 are allowed on the trunk, but are not listed under the Vlans allowed and active in management domain section, VLANs 41 and 45 must not be configured for the VTP domain. VLANs 18 through 43, VLANs 45 through 100, and VLANs 173 through 4094 are not configured for the VTP domain.

VLANs 1 through 12, VLAN 16, VLAN 40, and VLANs 101 through 172 are listed under the Vlans in spanning tree forwarding state and not pruned section. Because VLAN 43 is allowed and is in the spanning-tree forwarding state, but is not listed under the Vlans in spanning tree forwarding state and not pruned section, VLAN 43 must be pruned or must not be in the spanning-tree forwarding state. This is also true of VLANs 13 through 15 and VLAN 17. As stated previously, VLAN 41 is allowed on the trunk but is not configured for the VTP domain. Therefore, it cannot be confirmed whether VLAN 41 has or has not been pruned manually. If VLAN 41 were in the spanning-tree forwarding state, but were not listed under the Vlans in spanning tree forwarding state and not pruned section, then it could be confirmed that VLAN 41 were being pruned.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Cisco IOS Interface and Hardware Component Command Reference > show hw-module slot tech-support through show interfaces vg-anylan > show interfaces trunk

QUESTION 45
What protocol allows for centralized management of multiple wireless access points?

A. WPA
B. WEP
C. ad hoc
D. LWAPP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Lightweight access point protocol (LWAPP) is a protocol used to allow centralized management of access points (APs). The management components are removed from the APs and centralized into a wireless LAN controller. This controller can coordinate WLAN access, managing the load on the APs and user movement between APs. A lightweight AP receives control and configuration from the WLAN controller.

LWAPP defines the following activities:
- Packet encapsulation, fragmentation, and formatting
- Access point certification and software control
- Access point discovery, information exchange, and configuration

The processing of 802.11 data and the handling of management protocols and access point capabilities is distributed between the lightweight access point and the WLAN controller. For example, the AP handles the transmission of beacon frames and responses to probe request frames and the controller handles authentication. The WLC enhances:
- Mobility
- Authentication
- Security management

When lightweight APs are used, the data path from one wireless station to another includes the AP and its controller.

Wi-Fi protected access (WPA) is an encryption and authentication protocol for wireless access. It supports 802.1x authentication and EAP on a wireless client. The AP would function as the authenticator.

WEP is a wireless encryption protocol that uses static keys and no authentication.

Ad hoc is a WLAN mode used for peer-to-peer connectivity. Ad hoc allows wireless-enabled computers to communicate with each other without having an AP involved.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify other LAN switching technologies

References:
Cisco > Support > Product Support > Wireless > Cisco Aironet 1200 Series > Product Literature > Solution Overviews > Cisco Unified Wireless Network Overview

QUESTION 46
What feature allows the administrator to put phones into a separate logical network from the data network while keeping both in the same physical network?

A. auxiliary VLANs
B. queuing
C. 802.1Q
D. marking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Auxiliary VLANs allows the data and voice traffic to use the same physical topology but remain logically separate. The information the phones need regarding this voice VLAN is provided by the switch. Auxiliary VLANs allows IP phones to be automatically placed into a separate VLAN from data traffic.

Queuing is the process of placing traffic in appropriate queues depending on the class of traffic.

Marking is the process of setting the CoS, IP precedence, or DSCP of a packet to a specific value that will provide appropriate QoS throughout the network.

802.1Q is a trunking protocol used to allow traffic from multiple VLANs to pass through a single link and still be logically separate.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify VLANs

References:
Cisco > Catalyst 4500 Series Software Configuration Guide, 8.1 > Configuring VLANs > Configuring Auxiliary VLANs

QUESTION 47

Which port will the spanning-tree algorithm select as a bridge's root port?

A. The first port on the root bridge to receive an STP packet
B. The port through which the root bridge can be reached with the lowest-cost path
C. The port through which the root bridge can be reached with the lowest-value interface identifier
D. The port through which the root bridge can be reached with the highest-value interface identifier

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Root ports are ports that are in the forwarding state and provide connectivity to the root bridge. The port through which the root bridge can be reached with the lowest-cost path is the root port. All the ports on the root bridge (the bridge with the lowest bridge ID) are in the forwarding state and are referred to as designated ports.

Bridges and switches use the Spanning-Tree Protocol (STP) to prevent network loops. Without a loop-avoidance service on the network, Layer 2 devices, in certain situations, will endlessly flood broadcasts. An STP-enabled device recognizes a loop in the topology and blocks one or more redundant paths, preventing the loop. STP allows the switches to continually explore the network so that the loss or addition of a switch or bridge is also quickly discovered. STP is enabled by default on Catalyst switches.

For example, if two switches have an active connection between them that is forwarding traffic and a second link is connected between the same two switches, one of the two switch ports will go into a blocking state when BPDUs are received on the link. This helps to ensure that a loop does not form using the redundant connections. In some situations, heavy traffic may prevent the reception of BPDUs when the second link is put in place, and in that case, a loop may still form.

The root port is not selected based on the first port to receive an STP packet on the root bridge. Neither is it based on the lowest or highest interface identifier values.

Note: In some situations, there may be two ports with equal cost to the root bridge. When this occurs, the port with the lowest port number becomes the root port.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify spanning tree

References:
Catalyst 6500 Release 12.2SXF and Rebuilds Software Configuration Guide > Configuring STP and IEEE 802.1s MST > Creating the Spanning Tree Topology
Cisco > Support > Configuring Spanning Tree Protocol > How STP Works

QUESTION 48
Which IOS command sets the native VLAN to VLAN3?

A. switchport mode trunk 3
B. switchport native vlan 3
C. switchport trunk native vlan 3
D. switchport trunk allowed vlan 3
E. switchport default native vlan 3

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

The IOS command switchport trunk native vlan 3 sets the native VLAN to VLAN3.

Use the following command to configure the native VLAN on an 802.1Q trunk:

switch(config-if)# switchport trunk native vlan vlan_id

The 802.1Q native VLAN is the VLAN from which or to which Layer 2 frames are transmitted untagged on the 802.1Q trunk port. The default native VLAN on an 802.1Q is VLAN 1. The native VLAN IDs should be set to the same value for both sides of an 802.1Q trunk.

The command switchport trunk allowed vlan 3 is used to assign VLANs whose frames are allowed to be passed over the trunk.

The other options are incorrect due to invalid syntax.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport trunk

QUESTION 49
What command is used to enable CEF on a Cisco switch?

A. ip cef
B. ip cef distributed
C. ip route-cache cef
D. ip cef enable

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command to enable Cisco Express Forwarding (CEF) on a Cisco switch is ip cef. This enables CEF support on the entire switch. All interfaces that are configured to use CEF will be able to. The no form of this command will disable CEF support, including support on interfaces that have CEF configured on them.

Cisco Express Forwarding allows a Layer 3 switch to determine the next-hop destination MAC address of the first frame in a transmission made of many frames, and then utilizes the much faster switching process for all the remaining frames. This requires that routing be enabled on the switch, since the route to the initial frame must be determined.

The output of the show ip interface vlan id command can be used to determine whether IP routing is enabled. Partial output of the show ip interface vlan id command for two switches is shown below. The first (Switch A) has IP routing enabled and the second (Switch B) does NOT have IP routing enabled. The second switch is missing the section about CEF, since CEF cannot be enabled unless IP routing is enabled.

```
Switcha# show ip interface vlan 2<output omitted>IP flow switching is disabledIP CEF switching is enable
IP CEF Fast Switching turbo vector
IP multicast fast switching is enabled

Switchb# show ip interface vlan 2
<output omitted>
IP flow switching is disabled
IP multicast fast switching is enabled
```

The command ip cef distributed is used to enable distributed CEF (dCEF), not the CEF mentioned in the scenario.

The command ip route-cache cef is a valid command to enable CEF on an individual interface, but the command is only valid in interface configuration mode.

The command ip cef enable is an invalid command due to incorrect syntax.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify switch administration

References:
Cisco > Cisco IOS IP Switching Command Reference > ip cef

QUESTION 50
In the following partial output of the show run command, which MAC address or addresses will be removed from the list of secure addresses after 240 seconds?

```
<output omitted>

interface Fastethernet0/1
      switchport mode access
      switchport port-security
      switchport port-security maximum 10
      switchport port-security aging time 4
      switchport port-security aging static
      switchport port-security mac-address sticky
      switchport port-security mac-address 0000.0000.aaaa
      switchport port security mac-address sticky 0000.0000.bbbb
```

A. 0000.0000.aaaa
B. 0000.0000.bbbb
C. 0000.0000.aaaa and 0000.0000.bbbbb
D. none of the MAC addresses will be removed after 240 seconds

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The only address that will be removed or aged out of the secure MAC address list will be 0000.0000.aaaa. When port security is used on an interface, not only can you set a maximum number of MAC addresses that can use the interface, but you can also set the amount of time that an address can reside in the secure list.

When the switchport port-security command is used, you can specify whether the command applies to statically

assigned MAC addresses or dynamically learned MAC addresses, called sticky addresses. In this scenario, line 6 of the output specifies that the command applies to static addresses. Since 0000.0000.aaaa is the only statically assigned MAC address (assigned in line 8 of the output), it is the only address that will age out. The amount of time is configured in terms of minutes and is done on line 5 with the switchport port-security aging time 4 command.

The MAC address 0000.0000.bbbb will not age out because it is a sticky secure address. The aging command only applies to static MAC addresses.

Objective:
Infrastructure Security
Sub-Objective:
Configure and verify switch security features

References:
Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(20)EWA > Configuring Port Security
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport port-security

QUESTION 51
In which VTP modes can you propagate VTP advertisements and create or delete local VLANs? (Choose two.)

A. User
B. Server
C. Client
D. Private
E. Transparent

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

You can propagate VTP advertisements and create or delete local VLANs on a switch when it is in server mode or transparent mode.

There are three modes in VTP: server, client, and transparent. The main differentiator among the three modes is whether a switch can create or delete VLANs. You can create local VLANs in server and transparent VTP modes. However, VLANs created on a switch in transparent mode apply only to that switch, and information about these VLANs is not promulgated throughout the VTP domain.

VTP server mode sends or forwards VTP advertisements, synchronizes VLAN configuration information with other switches, and saves the VLAN in NVRAM.

VTP transparent mode forwards VTP advertisements and saves the VLAN configuration in NVRAM. It does not synchronize VLAN configuration information. A switch in transparent mode can create, delete, and modify VLANs, but changes are not transmitted to other switches in the domain. Changes only affect the local switch.

VTP client mode sends or forwards VTP advertisements and synchronizes VLAN configuration information with other switches. It does not save VLAN information in NVRAM. In client mode, VTP clients only can receive VLAN information from VTP servers. A Catalyst switch can create, modify, and delete VLANs in server or transparent modes, but not in client mode.

VTP user mode and private mode do not exist.

Objective:
Layer 2 Technologies

Sub-Objective:
Configure and verify trunking

References:
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)

QUESTION 52
With RSTP hello timers set to the default interval, how quickly can a non-edge port discover that its neighbor is down?

A. 20 seconds
B. 10 seconds
C. 6 seconds
D. 5 seconds

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

With Rapid Spanning Tree Protocol (RSTP) hello timers set at the default interval, a non-edge port can discover that its neighbor is down in 6 seconds. One of the advantages of RSTP over STP is quicker convergence when changes occur in the topology. After a non-edge port fails to receive three Bridge Protocol Data Units (BPDUs) from its neighbor, it will assume the neighbor to be down and will age out all information regarding the neighbor. Since hellos are sent at 2-second intervals in RSTP, it will take only 6 seconds for this to occur, as compared to 20 seconds for STP.

All other options are incorrect values for the default convergence time for RSTP.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify spanning tree

References:
Cisco > Home > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Technology Information > Technology White Paper > Understanding Rapid Spanning Tree Protocol (802.1w)

QUESTION 53
Which IOS commands are entered in interface configuration mode to configure a switch port to unconditionally be an 802.1Q trunk port and not generate DTP packets? (Choose two.)

A. trunk dot1q
B. switchport trunk dot1q
C. switchport nonegotiate
D. switchport trunk allowed vlan
E. switchport trunk encapsulation dot1q

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Entering the IOS commands switchport nonegotiate and switchport trunk encapsulation dot1q in interface configuration mode will only allow a switch port to be an 802.1Q trunk port. This disables the generation of dynamic trunking protocol (DTP) negotiation packets. Since DTP also negotiates encapsulation type, the encapsulation type must be identified (for example, dot1q).

Use the following steps to configure a port as an 802.1Q trunk:

1. Enter the interface configuration:
switch(config)# interface interface-id

2. Configure the port to using 802.1Q encapsulation:
switch(config-if)# switchport trunk encapsulation dot1q

3. Configure the port as a trunk port:
switch(config-if)# switchport nonegotiate

Note: Trunking modes can be configured as trunk, dynamic auto, dynamic desirable, nonegotiate, and access.

The switchport allowed vlan command is also valid for configuring dot1q trunks, but is not required. By default, all VLANs are allowed on the trunk.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport trunk
Cisco > Cisco IOS Interface and Hardware Component Command Reference > I through K > interface

QUESTION 54
What command configures a port with a voice VLAN using 802.1Q?

A. switch(config-if)# switchport voice vlan 10
B. switch(config-if)# switchport voice vlan 10 q
C. switch(config-if)# switchport voice vlan 10 802.1q
D. switch(config-if)# switchport voice vlan 10 dot1p

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command that configures a port with a voice VLAN using 802.1Q is switchport voice vlan 10. This configuration uses 802.1Q as a default. 802.1P is configured with the command switchport voice vlan 10 dot1p . These are the only two valid commands to configure voice VLANs on a switch port.

The following is an example of voice VLAN configuration and QoS:

switch(config)# mls qos
switch(config)# interface fastethernet 0/10
switch(config-if)# switchport voice vlan 100
switch(config-if)# switchport access vlan 1
switch(config-if)# switchport priority extend trust
switch(config-if)# mls qos trust cos

switch(config-if)# mls qos trust device cisco-phone

In this example, the mls qos command enables QoS on the switch. The interface command moves the administrator into interface configuration mode. The switchport voice vlan 100 command configures the voice VLAN to be 100 using 802.1Q. If you wanted 802.1P, the command would have been switchport voice vlan 100 dot1p .

The VLAN for data traffic is defined with the fourth command, switchport access vlan 1 . The switchport priority extend trust command instructs the port to trust the CoS of the data traffic being passed from a PC connected to the IP phone. The mls qos trust cos command tells the port to use the CoS value of traffic passed to it from the phone or PC to classify traffic. (It is included here for illustration purposes only, as this command is not necessary when using the switchport priority extend trust command since the CoS value of the PC will be trusted anyway.) The mls qos trust device cisco-phone command tells the port to trust the QoS information provided from the IP phone if it is a Cisco phone.

The other options are incorrect due to invalid syntax.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify VLANs

References:
Cisco > Catalyst 3750-E and 3560-E Switch Software Configuration Guide, 12.2(46)SE > Configuring Voice VLANs
Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport voice vlan
Cisco > Cisco IOS Quality of Service Solutions Command Reference > mls qos (global configuration mode) through mpls experimental > mls qos (interface configuration mode)

QUESTION 55
What commands can be used to verify the trunking configuration of a router performing inter-VLAN routing? (Choose all that apply. Each correct answer is a complete solution.)

A. router# show trunk
B. router# show vlans
C. router# show vtp status
D. router# show ip interface brief
E. router# show ip route

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command show vlans verifies the trunking configuration of a router performing inter-VLAN routing. This command will indicate what subinterfaces are associated with what VLANs, the trunking protocol being used, and the IP addresses that the router is using on each of the VLANs. Below is sample output of the show vlans command:

```
RouterA# show vlans
Virtual LAN ID: 2 (Inter Switch Link Encapsulation)
VLAN Trunk Interface: Fa0/1.1
Protocols Configured: Address: Received: Transmitted:
IP 10.1.1.1 14 16
Virtual LAN ID: 3 (Inter Switch Link Encapsulation)
VLAN Trunk Interface: Fa0/1.2
Protocols Configured: Address: Received: Transmitted:
IP 10.2.2.1 13 19
```

The show ip route command can also be used to determine the correct configuration of inter-VLAN routing. If routing is configured correctly, there should be a route to each VLAN displayed in the output. If a route to a VLAN is missing, most likely the router is missing the command to assign an IP address to the VLAN in VLAN configuration mode. Below is output of the command on the same router as in the previous sample output, showing a route to both VLANs. If an IP address is not configured for a VLAN, a route to the VLAN will not be present.

```
RouterA# show ip route

Gateway of last resort is not set

10.0.0.0/8 is subnetted, 2 subnets

C 10.1.1.0 is directly connected, Fasthethernet0/1.1
C 10.2.2.0 is directly connected, Fasthethernet0/1.2
```

The command show trunk is not a valid command to issue on a router. Routers do not understand trunking in the same way switches do. Routers must be configured with a unique subinterface representing each VLAN, mimicking how the router normally connects different network with physical interfaces.

The command show ip interface brief is not used to verify trunking on a router. This command is useful in identifying IP addresses assigned to interfaces, and the state of the interfaces. No VLAN or trunking information is included in the output.

The command show vtp status is not a valid command on a router. The router does not use or understand VTP.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Cisco IOS LAN Switching Command Reference > show vlan through ssl-proxy module allowed-vlan > show vlans

QUESTION 56
You must add a new switch to the existing network using VTP to maintain the VLAN databases.

Which mode should be configured on this switch so that VLANs can be separately maintained on this switch?

A. None

B. Client
C. Server
D. Transparent

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Adding a switch configured in VTP transparent mode allows the administrator to maintain the switch VLAN configuration information and not advertise its database to other switches in the network.

A VTP transparent mode switch will receive and forward VTP advertisements. The VTP transparent mode switch will not use the contents of the advertisement to synchronize with its own VLAN database.

VTP advertisements are flooded throughout the management domain every five minutes or whenever there is a change. These advertisements originate from a switch that is in server mode and are propagated by switches that are in either client or transparent mode. Before a client or another server accepts or incorporates the information sent in the advertisement, it checks the domain name and password (if defined) against its own configuration. Next, the revision number is checked to see if it is higher than the last value stored in the receiving switch. If the revision number is higher, the receiving switch will overwrite its VLAN database with the information in the advertisement.

The VTP server mode sends or forwards VTP advertisements, synchronizes VLAN configuration information with other switches, and saves the VLAN in NVRAM.

The VTP client mode sends or forwards VTP advertisements and synchronizes VLAN configuration information with other switches. It does not save VLAN information in NVRAM. In client mode, VTP clients only can receive VLAN information from VTP servers.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)

QUESTION 57
Which are valid configurable VLAN ID numbers for 802.1Q networks?

A. 0-1005
B. 1-4094
C. 0-4095
D. 1-1001

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

IEEE 802.1Q supports configuring VLAN IDs 1 through 4094.

The 802.1Q standard specifies support for a maximum of 4,094 VLANs. (IDs 0 and 4095 are reserved.) Therefore, ID values of 1-4094 are assignable. In contrast, the valid range of configurable ISL VLANs is 1-1001. The following is a summary of VLAN IDs:

- 0 and 4095: Reserved
- 1: Cisco default management
- 2-1001: Available for Ethernet VLANs
- 1002-1005: Defaults for FDDI and Token Ring VLANs
- 1006-4094: Extended range available for Ethernet VLANs (802.1Q only)

Recognizing the differences between supported VLAN ID ranges highlights several issues in constructing a network of both ISL and 802.1Q VLAN networks. Ethernet VLAN IDs above the supported ISL range must be mapped to IDs within the range supported by ISL. Among other limitations, you are limited to eight mappings. This process of mapping 802.1Q to ISL VLAN IDs will further restrict and define which IDs are available to be used.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify VLANs

References:
Cisco Nexus 5000 Series Switch CLI Software Configuration Guide > Configuring Access and Trunk Interfaces

QUESTION 58
When provisioning bandwidth for an IP telephony network, which elements are unique to an IP telephony call? (Choose two.)

A. voice stream
B. IGMP packets
C. call-control signaling
D. routing protocol packets
E. speed of the segment to the telephone

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Bandwidth provisioning for an IP telephony call consists of the voice stream traffic and the call control traffic. These elements are unique to an IP telephony call.

The network infrastructure should be examined to see if the required bandwidth exists to support the voice and call-control applications. The sum of the bandwidth necessary for each major application, including voice, video, and data, should not exceed 75% of the total available bandwidth for each link. Voice traffic can be characterized as:

- Smooth
- Benign
- Drop sensitive
- Delay sensitive

Voice packets are typically around 60 to 120 bytes in size. For good voice quality, packet loss should be less than 1 percent and delay should be no more than 150 ms.

The IP telephony voice call-control procedures also generate traffic. The call control procedures are in the areas of call setup, maintenance, redirect, and tear down. There are special protocols such as H.323 and Media Gateway Control Protocol (MGCP) that handle these procedures.

Voice applications are delay-sensitive. Speech is sampled by voice processors referred to as a codec (coder/ decoder). Then the digitized voice-sample outputs of the codecs are sent into the network towards the receiver at regular intervals in real-time transport protocol (RTP) packets. If these packets containing the voice samples are delayed for any reason behind other data traffic, the quality of the voice conversation suffers.

The transportation of these voice applications in RTP packets through the IP network handled by H.323 protocols and devices is referred to as Voice over IP (or VoIP for short).

The following are other network and design considerations besides bandwidth relating to IP telephony infrastructure support:
- Determine if the cabling plant can support the IP telephony equipment.
- Determine if the switch hardware can supply power to attached IP telephony equipment or if additional hardware is required.
- Ensure that infrastructure supports priority end-to-end VLANs and QoS networking.

Internet Group Management Protocol (IGMP) is used for managing the membership of IP multicast groups and is not an element unique to an IP telephony call.

Routing protocol packets (RIP, OSPF, and EIGRP) are used by routers to share routing information, and are not elements unique to an IP telephony call.

The speed of the segment to the telephone is important to VoIP, but that is not an element unique to an IP telephony call.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify VLANs

References:
Cisco > Support > Technology Support > Voice > Telephony Signaling

QUESTION 59
What occurs when an untagged frame is received by an 802.1Q trunk port?

A. It discards the frame.
B. It tags the frame with the identified native VLAN value.
C. It forwards the frame out each port of the switch not assigned to a VLAN.
D. It forwards the frame to a port belonging to the same VLAN as the native VLAN.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

IEEE 802.1Q supports configuring native VLANs. A native VLAN is the VLAN a port is in when not in trunking mode. Native VLAN packets are sent untagged. If an 802.1Q trunk receives an untagged frame, it will forward that frame to a port that belongs to the same VLAN as the identified native VLAN. The frame is treated as if it were tagged with the same VLAN ID as the native VLAN. Frames received through ports having the same membership as the identified native VLAN of the trunk will be forwarded untagged out of the trunk.

It is important that the native VLAN settings on each end of an 802.1Q trunk match.

The 802.1Q standard specifies support for a maximum 4094 VLANs (IDs 0 and 4095 are reserved). Therefore, ID values of 1-4094 are assignable. In contrast, the valid range of configurable ISL VLANs is 1-1001. The following is a summary of VLAN IDs:
- 0 and 4095: Reserved

- 1: Cisco default management
- 2-1001: Available for Ethernet VLANs
- 1002-1005: Defaults for FDDI and Token Ring VLANs
- 1006-4094: Extended range available for Ethernet VLANs (802.1Q only)

Recognizing the difference in supported VLAN ID ranges highlights several issues in constructing a network of both ISL and 802.1Q VLAN networks. Ethernet VLAN IDs above the supported ISL range must be mapped to IDs within the range supported by ISL. Among other limitations, you are limited to eight total mappings. This process of mapping 802.1Q to ISL VLAN IDs will further restrict and define what IDs are actually available to be used.

Untagged frames are not discarded, but are sent to the native VLAN.

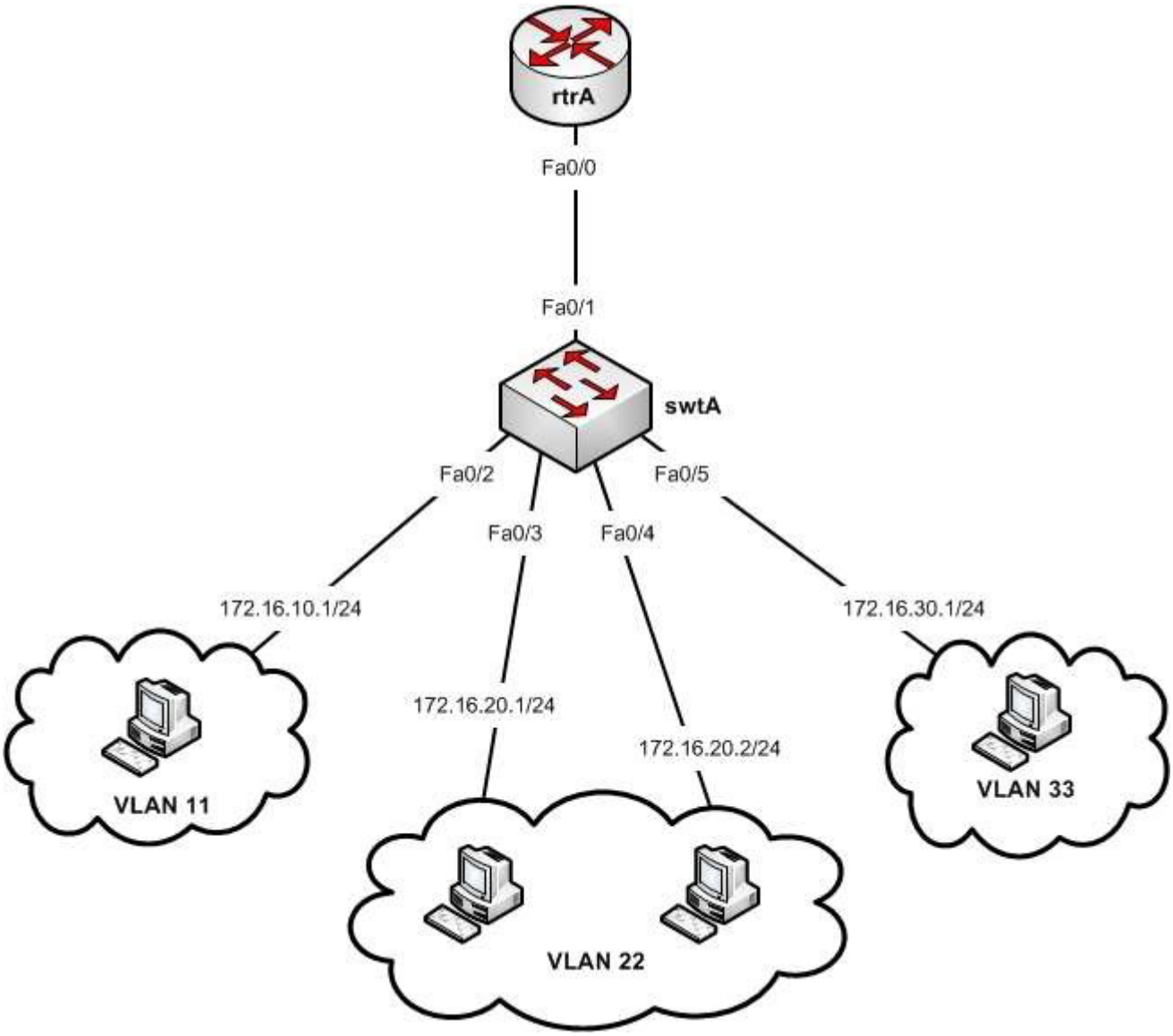
Untagged frames are not tagged with the tag of the native VLAN. They are simply forwarded to that VLAN. No packets in the native VLAN have tags.

Untagged frames are not forwarded out all ports not assigned to a VLAN. It will only be forwarded to the switchport where the destination MAC address resides.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Cisco Nexus 5000 Series Switch CLI Software Configuration Guide > Configuring Access and Trunk Interfaces
Cisco Press > Articles > Determining IP Routes

QUESTION 60
Refer to the following network diagram:



You executed the following commands on the swtA switch:

```
swtA(config)#vlan 11
swtA(config-vlan)#name Sales
swtA(config-vlan)#exit
swtA(config)#vlan 22
swtA(config-vlan)#name Administration
swtA(config-vlan)#exit
swtA(config)#vlan 33
swtA(config-vlan)#name Accounts
swtA(config-vlan)#exit
swtA(config)#interface fa0/1
swtA(config-if)#switchport trunk encapsulation dot1q
swtA(config-if)#switchport mode trunk
swtA(config-if)#switchport trunk allowed vlan 11,22,33
swtA(config)#interface fa0/2
swtA(config-if)#switchport mode access
swtA(config-if)#switchport access vlan 11
swtA(config)# interface fa0/3
swtA(config-if)# switchport mode access
swtA(config-if)# switchport access vlan 22
swtA(config)# interface fa0/4
swtA(config-if)# switchport mode access
swtA(config-if)# switchport access vlan 22
swtA(config)# interface fa0/5
swtA(config-if)# switchport mode access
swtA(config-if)# switchport access vlan 33
```

You executed the following commands on the rtrA switch:

```
rtrA(config)# interface fa0/0
rtrA(config-if)# no shutdown
rtrA(config)# interface fa0/0.1
rtrA(config-subif)# encapsulation dot1q 11
rtrA(config-subif)# ip address 172.16.10.2 255.255.255.0
rtrA(config-subif)# no shutdown
rtrA(config)# interface fa0/0.2
rtrA(config-subif)# ip address 172.16.20.3 255.255.255.0
rtrA(config-subif)# no shutdown
rtrA(config)# interface fa0/0.3
rtrA(config-subif)# encapsulation dot1q 33
rtrA(config-subif)# ip address 172.16.30.2 255.255.255.0
rtrA(config-subif)# no shutdown
```

Which of the following VLANs do(es) NOT participate in inter-VLAN routing through the rtrA router?

A. VLAN 11 only
B. VLAN 22 only
C. VLAN 33 only
D. VLAN 11 and VLAN 22
E. VLAN 22 and VLAN 33
F. VLAN 33 and VLAN 11

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

VLAN 22 is the only VLAN that does not participate in inter-VLAN routing through the rtrA router. The given network diagram and the commands reflect a router-on-a-stick (RoaS) configuration. In a RoaS configuration, inter-VLAN routing is achieved in two steps.

The first step sets up the switch:
- Configure the switch
- Configure the required VLANs
- Configure the switch port connecting to the router interface as a trunk port
- Enable dot1q or ISL encapsulation on the trunk port
- Configure the switch ports connecting to the VLANs as access ports
- Assign the access switch ports to respective VLANs

The second step sets up the router:
- Configure the router
- Enable the router interface connected to the trunk switch port
- Create separate subinterfaces on the trunk router interface for each VLAN
- Enable dot1q or ISL encapsulation on the subinterfaces
- Assign IP addresses to each subinterface in the same subnet as the VLAN of which the interface will be a member. Consequently, this address will become the default gateway for each host in that VLAN.

In the scenario, the subinterface created for VLAN 22 is not configured for inter-VLAN routing because the encapsulation command is missing. Without this command, the encapsulation type and the VLAN ID remain

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify trunking

References:
Home > Support > Configuring InterVLAN Routing > Configuring InterVLAN Routing on an External Cisco Router > Configuring IP InterVLAN Routing on an External Router
Home > Support > Configuring InterVLAN Routing > InterVLAN Routing Configuration Examples > InterVLAN Routing with an External Cisco 7505 Router Example

QUESTION 61
Which of the following capabilities does a multilayer switch possess that an Access layer switch does not? (Choose all that apply.)

A. the ability to make forwarding decisions based on MAC addresses
B. the ability to make forwarding decisions based on host names
C. the ability to make forwarding decisions based on IP addresses
D. the ability to make forwarding decisions based on UDP/TCP port numbers
E. the ability to make forwarding decisions based on NetBIOS names

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Multilayer switches are capable of making forwarding decisions based on IP addresses and UDP/TCP port numbers, while Access layer switches are not. The term multilayer describes the ability of the multilayer switch to utilize information that exists on more than one layer of the TCP model for forwarding decisions. This device combines the functionality of a switch and a router. Additionally, it possesses the ability to do something that neither a switch or router alone: perform Fast Switching, a process whereby the device can route the first packet in a traffic flow and then use hardware switching for the remaining packets in the flow. This process of

routing once, switching many, results in less routing (a slower process) and more switching (a faster process), with a net result of speeding traffic flow.

Multilayer switches usually operate in the Distribution and Core layers of the Cisco Enterprise Composite model. There are important considerations for each layer:

- Access layer - This is the layer where end-user stations should connect. It consists of Access layer or Layer 2 switches. VLANs, QoS, and protocol filtering operate at this layer.
- Distribution layer - This is the layer where routing is performed and where access lists are enforced. Devices in this layer operate in Layer 3 of the OSI model.
- Core layer - High-speed backbone switches exist on this layer. It should be designed with a low number of Layer 3 peers, switches that can efficiently forward traffic even when every uplink is at 100% capacity and the switches should have many high-speed ports.

When migrating to the Cisco Enterprise Composite model from earlier models, keep the following practices in mind:

- Add redundancy between the hierarchical layers
- Identify groups of end users as switch blocks
- Group common resources into switch blocks

Multilayer switches are also capable of making forwarding decisions based on MAC addresses, but access layer switches can do this as well.

Neither multilayer switches nor Access layer switches can make forwarding decisions based on host names or NetBIOS names. This function is performed by Domain Name Servers (DNS) and Windows Internet Naming (WINS), servers respectively.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify switch administration

References:
Cisco > Home > Support > Configuring IP MLS

QUESTION 62
What is the approximate amount of time it takes for a PortFast-enabled port to transition from blocking to forwarding?

A. Immediately
B. 15 seconds
C. 20 seconds
D. 30 seconds
E. 50 seconds

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Instead of waiting for STP to cycle through the blocking, learning, and listening states, PortFast will place the port in the forwarding state immediately.

When PortFast is enabled on a port, the attached end station can join the network almost immediately rather than waiting up to 50 seconds for spanning tree to converge. This feature is designed to enable the connections to workstations and servers to be put into the forwarding state as soon as possible after a spanning-tree reconvergence.

Bypassing the listening and learning states creates an exposure for spanning-tree loops. The default behavior of a PortFast-enabled port is to put the port immediately into a blocking state if a BPDU is received.

The following command enables PortFast:

switch(config-if)# spanning-tree portfast

You should only enable PortFast on a port that connects an end station. Enabling PortFast on a port that connects another switch could create a loop.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify spanning tree

References:
Catalyst 3750 Switch Software Configuration Guide, 12.2(40)SE > Configuring Optional Spanning-Tree Features > Understanding Port Fast

QUESTION 63
By default, which VLAN is the Cisco management VLAN?

A. 1
B. 0
C. 1001
D. 1005

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Cisco uses VLAN1 as the default management VLAN.

All ports are automatically assigned to VLAN1. Cisco Discovery Protocol (CDP) and VLAN Trunking Protocol (VTP) advertisements are transmitted on VLAN1. VLAN1 is the management VLAN and is used for administration. It cannot be deleted or pruned from a trunk line.

VLAN Ids that are implemented can vary based on whether the trunk implementation is Cisco's Inter-Switch Link (ISL) or the IEEE 802.1Q standard.

The following is a summary of the VLAN IDs:
0 and 4095 - Reserved
1 - Cisco default management
2-1001 - Available for Ethernet VLANs
1002-1005 - Defaults for FDDI and Token Ring VLANs
1006-4094 - Extended range available for Ethernet VLANs (802.1Q only)

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify VLANs

References:
Cisco > Support > Technology Support > LAN Switching > Layer-Three Switching and Forwarding > Configure > Configuration Examples and Technotes > How To Configure InterVLAN Routing on Layer 3 Switches

QUESTION 64
You are the network administrator in your company. You have executed the following commands on the Fa0/1 interface of a switch named swtA:

```
swtA(config)# interface Fa0/1
swtA(config-if)# switchport mode access
swtA(config-if)# switchport port-security
swtA(config-if)# switchport port-security maximum 4
swtA(config-if)# switchport port-security mac-address sticky
swtA(config-if)# switchport port-security mac-address 1111.1111.1111
swtA(config-if)# switchport port-security mac-address 3333.3333.3333
swtA(config-if)# exit
```

Over a period of time, different hosts are connected to the Fa0/1 switch port of swtA. The MAC addresses of the hosts that were connected to the Fa0/1 port and the order in which they connected are as follows:

```
1111.1111.1111
2222.2222.2222
4444.4444.4444
5555.5555.5555
3333.3333.3333
```

After a few days, you notice that the Fa0/1 port is in the shutdown state.

Which of the following MAC addresses causes the Fa0/1 port to shut down?

A. 2222.2222.2222
B. 3333.3333.3333
C. 4444.4444.4444
D. 5555.5555.5555

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The MAC address 5555.5555.5555 caused the Fa0/1 port to shut down because it violates the port security enabled on the port. The switchport port-security maximum 4 command allows at most four MAC addresses or hosts to be connected to the Fa0/1 switch port. Two secure MAC addresses, 1111.1111.1111 and 3333.3333.3333, are statically configured on the Fa0/1 port by using the switchport port-security mac-address command. This implies that these two MAC addresses are allowed to be connected to the Fa0/1 port.

The switchport port-security mac-address sticky command enables sticky learning of MAC addresses on the Fa0/1 port. With sticky learning, the dynamically learned MAC addresses are stuckto the port. The first MAC address that is connected to the port becomes the sticky secure address. In this case, 1111.1111.1111 and 3333.3333.3333 MAC addresses are statically configured as secure addresses. This implies that there can be at most two sticky secure MAC addresses for Fa0/1. The hosts w

Objective:
Infrastructure Security
Sub-Objective:
Configure and verify switch security features

References:
Cisco > Catalyst 6500 Series Release 15.0SY Software Configuration Guide > Security > Port Security

Cisco IOS Security Command Reference > show vlan group Through switchport port-security violation > switchport port-security mac-address
Cisco IOS Security Command Reference > show parameter-map type consent Through show users > show port-security

QUESTION 65
Refer to the following partial output of the show spanning-tree command.

```
SW1# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0A61.0015.4D02
             Cost        19
             Port        1(FastEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0F2C.08A1.330E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/2            Root FWD 3        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/5            Altn BLK 19        128.5    P2p

VLAN0121
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0F2C.08A1.330E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0F2C.08A1.330E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ----------------------------
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/6            Desg FWD 19        128.6    P2p
```

Which of the following statements are TRUE for the given output? (Choose all that apply.)

A. SW1 is the root bridge for VLAN0001
B. Fa0/2 is the root port for VLAN0001
C. The switch having the 0A61.0015.4D02 bridge ID is the root bridge for VLAN0001
D. The switch having the 0F2C.08A1.330E bridge ID is the root bridge for VLAN0001
E. The switch connected to the Fa0/6 port of SW1 is using its root port
F. The port Fa0/4 is in a blocking state for VLAN 0121
G. The STP protocol in use is RSTP

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following statements are correct about the given output:
- Fa0/2 is the root port for VLAN001
- The switch having the 0A61.0015.4D02 bridge ID is the root bridge for VLAN0001
- The switch connected to the Fa0/6 port of SW1 is using its root port

The value in the Role column in the output for VLAN0001 is Root for the Fa0/2 port of SW1. This implies that the Fa0/2 port is a root port. A root port is the port on a non-root bridge that has the least cost to reach the root bridge. Every non-root bridge must elect a root port. A root bridge does not have any root ports.

The output for VLAN0121 specifies Desg in the Role column for the Fa0/6 port of SW1. This implies that the Fa0/6 port is a designated port. This means that the switch on the other end is using its root port.

The switch having the 0A61.0015.4D02 bridge ID is the root bridge for VLAN0001. For VLAN0001, the bridge ID of the root and the local switch are different. The bridge ID of the local switch (SW1) is 0F2C.08A1.330E, while the bridge ID of the root bridge is 0A61.0015.4D02. The text Port 1 (FastEthernet0/2) in the Root ID section for VLAN0001 in the output indicates that the root bridge is connected to the Fa0/2 port of the local switch.

The options stating that SW1 is the root bridge for VLAN0001 and that the switch having the 0F2C.08A1.330E bridge ID is the root bridge for VLAN0001 are incorrect. The Bridge ID section in the output for VLAN0001 and VLAN0121 specifies the bridge ID of the local switch. In this case, the bridge ID of the local switch (SW1) is 0F2C.08A1.330E. SW1 is not the root bridge for VLAN001; however, SW1 is the root bridge for VLAN0121.

You can determine if a local switch is the root bridge by any of the following:
- The text This bridge is the root appears in the Root ID section of the output for VLAN0121.
- The bridge IDs in the Root ID and Bridge ID sections of the output are the same.
- All the ports of the local switch are Desg (designated) ports and in forwarding state.

The port Fa0/4 is NOT in a blocking state for VLAN 0121. As indicated in the STS column for Fa0/4 under the section on VLAN 0121, it states that is in an a FWD (forwarding) state.

The STP protocol in use is NOT Rapid Spanning Tree protocol (RSTP). If that were the case, the output would display Spanning tree enabled protocol rstp, rather than Spanning tree enabled protocol ieee. This indicates that IEEE 802.1d is in use.

Objective:
Layer 2 Technologies
Sub-Objective:
Configure and verify spanning tree

References:
Cisco Press > Articles > Network Technology > General Networking > CCNP Exam Prep: Traditional Spanning Tree Protocol
Cisco > Cisco IOS Bridging Command Reference > show spanning-tree