300-420

Number: 300-420
Passing Score: 800
Time Limit: 120 min
File Version: 1

300-420

Exam A

QUESTION 1
What command would display a single line of information for each virtual gateway or virtual forwarder on a switch?

A. switch# show glbp
B. switch# show glbp brief

C. switch# show standby
D. switch# show standby brief

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A brief single line view of virtual forwarder and virtual gateway information is provided with the command show glbp brief. Virtual forwarders and virtual gateways are terms used for GLBP groups. A brief output of GLBP information is provided with the brief key word. This output includes the interface, priority, state, and address of GLBP interfaces on the switch.

The command show glbp displays detailed information about GLBP groups on the switch. This information includes the GLBP groups the switch is a member of, whether this is the active switch, the virtual IP address, and whether preemption is enabled.

The command show standby brief is used to display a summary of the HSRP groups to which the switch belongs. The summary information it provides includes the group number, priority, state, active device address, standby address, and group address. This command is for HSRP only.

The command show standby can be used to display detailed information about HSRP groups to which a switch belongs. This command is for HSRP only.

Objective:

Infrastructure Services Sub-Objective:
Configure and verify first-hop redundancy protocols

References:
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring GLBP
Cisco > Cisco IOS IP Application Services Command Reference > show glbp

QUESTION 2
Which command enables GLBP on an interface?

A. glbp
B. glbp 10 ip 192.168.1.1
C. standby mode glbp
D. switchport mode glbp

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The glbp ip interface configuration command enables Group Load Balancing Protocol (GLBP). The syntax for this command is as follows:

```
switch(config-if)# glbp group-number ip ip-address
```

The following example activates GLBP for group 5 on Fast Ethernet interface 1/0. The virtual IP address to be used by the GLBP group is set to 10.5.5.5. The default gateway of each host should be set to the virtual IP address.

```
switch(config)# interface FastEthernet 1/0 switch(config-
if)# ip address 10.5.5.1 255.255.255.0 switch(config-if)#
glbp 5 ip 10.5.5.5
```

GLBP is a Cisco-designed protocol that provides for the dynamic use of redundant routers in a broadcast network. It differs from HSRP and VRRP in that it is not necessary to configure multiple groups to fully use redundant paths or routers. GLBP has a configurable load-balancing mechanism that will distribute the use of redundant gateways servicing a broadcast network such as an Ethernet LAN. When a host issues an ARP to resolve its gateway's MAC address, the active virtual gateway (AVG) will respond with the virtual MAC address of a selected active virtual forwarder (AVF). The AVG will perform load balancing by varying which virtual MAC it selects to use in the response. The AVF will own that assigned virtual MAC as long as the gateway is active. If an AVF becomes unable to provide service as gateway, then another AVF can assume ownership of the virtual MAC.

Objective:
Infrastructure Services Sub-
Objective:

Configure and verify first-hop redundancy protocols

References:
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring GLBP

QUESTION 3
What command disables 802.1x authentication on a port and permits traffic without authentication?

A. dot1x port-control disable
B. dot1x port-control force-unauthorized
C. dot1x port-control auto
D. dot1x port-control force-authorized

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command dot1x port-control force-authorized is used to disable 802.1x on a port and permit traffic without authentication. Dot1x ports are in one of two states, authorized or unauthorized. Authorized ports permit user traffic to flow through the port. This state usually follows successful authentication. Unauthorized ports only permit authorization traffic to flow through the port. Usually a port begins in the unauthorized state. A user is then allowed to exchange AAA authentication traffic with the port. Once the user has been authenticated successfully, the port is changed to the authorized state and the user is permitted to use the port normally.

Normal use of 802.1x has the port configured with the dot1x port-control auto statement. This places the port in the unauthorized state until successful authentication. After successful authentication, the port is changed to the authorized state.

When 802.1x is initially configured, the default port control of the ports is force-authorized. This forces the port to be in the authorized state without successful authentication. This setting disables the need for authentication and permits all traffic.

The force-unauthorized keyword configures the port as an unauthorized port regardless of authentication traffic. A port configured with this key word would not permit user traffic, not even authentication traffic.

The command dot1x port-control disable is not a valid command due to incorrect syntax.

Objective:
Infrastructure Security Sub-
Objective:
Describe device security using Cisco IOS AAA with TACACS+ and RADIUS

References:
Cisco > Catalyst 6500 Series Release 15.0SY Software Configuration Guide > Security > IEEE 802.1X Port-Based Authentication
Cisco > Catalyst 4500 Series Switch Cisco IOS Command Reference, 12.2(52)SG > aaa accounting dot1x default start-stop group radius through instance > dot1x port-control
Cisco > Catalyst 4500 Series Switch Cisco IOS Command Reference, 12.2(52)SG > aaa accounting dot1x default start-stop group radius through instance > dot1x port-control

QUESTION 4
What command would be used to display detailed information regarding VRRP groups on the switch?

A. switch# show vrrp
B. switch# show standby
C. switch# show vrrp detail
D. switch# show standby detail

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command that would display detailed information regarding VRRP groups on the switch is show vrrp. The information provided for each VRRP group by this command includes the status, virtual IP and MAC addresses, whether preemption is enabled, priority of the switch, and the address of the group master.

The command show vrrp detail does not exist on a Cisco device. The detail view is provided by the command show vrrp.

The command show standby can be used to display detailed information about HSRP groups to which a switch belongs. This command is for HSRP only.

The command show standby detail provides the same output as show standby. It can be used to display detailed information about HSRP groups a switch is a member of. This command is for HSRP only.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Cisco > Cisco IOS IP Application Services Command Reference > show vrrp

QUESTION 5
Assuming that preempt is not configured, when does a router in an HSRP group assume the role of the active router for the group?

A. A router in standby status will become the active router if it has a higher priority than the active router.
B. A router in standby status will become the active router when it does not detect three consecutive hello messages from the active router.
C. A router in standby status will become the active router when it does not detect any hello messages from the active router within the configured holdtime.
D. A router in listening status will become the active router when it does not detect any hello messages from the active router within the configured holdtime.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A router in standby status will become the active router when it does not detect any hello messages from the active router within the configured holdtime.

There are two ways for a router to become the HSRP active router. On startup, the router with the highest priority or IP address will become the active router. If the active router fails, the HSRP standby router is a candidate to become the next active HSRP router. Failure of the active router is detected by the loss of hello messages for a configurable amount of time referred to as holdtime. By default, hellos are sent every three seconds (hello time) and the holdtime is 10 seconds.

A router with the highest priority will be selected as the active router during the startup election process. If the active router fails and the standby router is promoted to be the active router, the first router will not immediately resume being the active router even if it has higher priority. This characteristic can be overridden with the configuration option of preempt. The router with the highest priority can initiate a coup to become the active router in the group if it has preempt enabled in the configuration. By default, all routers have an HSRP priority of 100. The range of values that can be assigned is 1 - 255.Other default values are: ▪ Standby holdtime is 10 seconds
▪ Standby track interface priority is 10

To illustrate these concepts, consider the following example. Router A is configured with a priority of 150 and Router B is configured with a priority of 100. Neither router is configured to preempt. If both routers were shut down and Router 5 was rebooted first, then Router B would become the active router. If Router A was then rebooted, it would not become the active router even though it has a higher priority than Router B, because it was NOT configured with the preempt command to allow it to assume the active role with a higher priority.

The six HSRP states are defined as follows:
▪ Initial state: All routers start in this state.
▪ Learn state: The router is in the learn state when it has not communicated with the active router. It does not know which router is the active router and does not know the IP address of the virtual router (if no HSRP IP address configured in the router).

- Listen state: Once the router hears from the active router and knows the virtual IP address, it enters the listen state. It is not the active or standby router.
- Speak state: After a router learns the IP address of the virtual router, it enters the speak state. It participates in the active and standby router election. It sends hello messages to the active router.
- Standby state: When the active router has been elected, the second router enters the standby state. This is the standby router and it will become the active router if the active router fails.

- Active state: The router is in active state when it is forwarding packets. It receives packets via the virtual IP address.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

QUESTION 6

You have configured three routers in HSRP group 10 to provide gateway redundancy for VLAN 56. Your intention was for Router 1 to be the active router in the group and for Router 3 to be the standby router. Furthermore, in the event that Router 1 became unavailable, resulting in Router 3 becoming active, you intended for Router 1 to resume its role as active when it came back online. However, you discover that in practice, Router 1 does NOT resume the active role when it comes back online.

What command should be executed on Router 1?

A. router1(config)# interface VLAN 56router1(config-if)# standby 10 preempt
B. router1(config)# interface VLAN 10router1(config-if)# standby 56 preempt
C. router1(config)# standby 10 preempt
D. router1(config)# standby 56 preempt

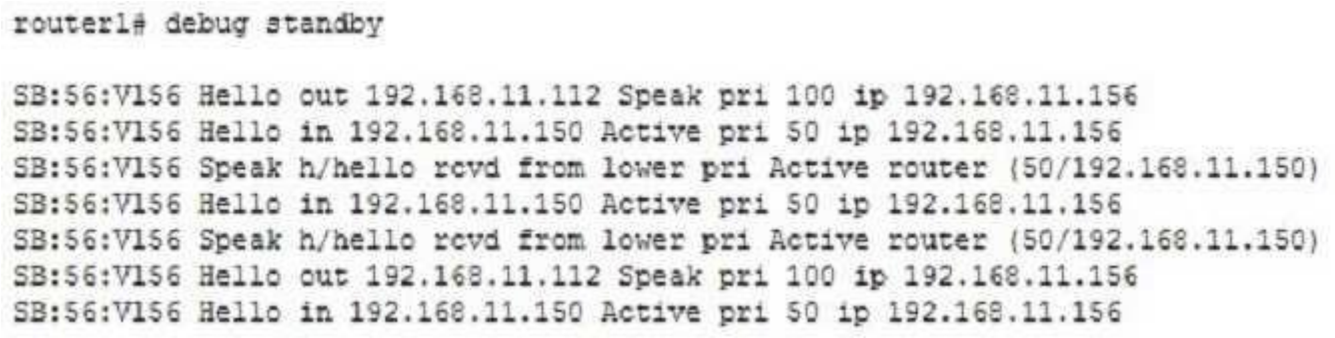
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

For Router 1 to resume its role as active when it comes back online, it must be configured to preempt the router with a lower priority. In this scenario, Router 3 must have been configured with a lower priority than Router 1, or else it would have been the active router to begin with. To allow Router 1 to take back over as active, it must be configured with the following commands that will allow it to preempt the router with the lower priority:

router1(config)# interface VLAN 56 router1(config-if)# standby 1 preempt

This condition can be illustrated by executing the debug standby command on Router 1 as shown in the partial output below. The IP address of Router 1 is 192.168.11.112. The IP address of Router 3 is 192.168.11.150. The virtual IP address of the HSRP group is 192.168.11.156.



```
router1# debug standby

SB:56:Vl56 Hello out 192.168.11.112 Speak pri 100 ip 192.168.11.156
SB:56:Vl56 Hello in 192.168.11.150 Active pri 50 ip 192.168.11.156
SB:56:Vl56 Speak h/hello rcvd from lower pri Active router (50/192.168.11.150)
SB:56:Vl56 Hello in 192.168.11.150 Active pri 50 ip 192.168.11.156
SB:56:Vl56 Speak h/hello rcvd from lower pri Active router (50/192.168.11.150)
SB:56:Vl56 Hello out 192.168.11.112 Speak pri 100 ip 192.168.11.156
SB:56:Vl56 Hello in 192.168.11.150 Active pri 50 ip 192.168.11.156
```

Router 1 sends a hello in line 1 of the output and receives its hello in line 2. Line 1 shows that Router 1 has a priority of 100. Line 2 shows that Router 3 (192.168.11.150) has a priority of 50. Although Router 1 has a higher priority, it is not configured to preempt, so it will not be able to take the active role back from Router 3. If Router 1 were configured to preempt, there would be a series of output as shown below:

```
SB:56:Vl56 Hello in 192.168.11.112 Active pri 100 ip 192.168.11.156
SB:56:Vl56 Active router is 192.168.11.112, was local
```

If the HSRP router is the only HSRP router on the segment, then the output will show the router sending out hello packets with no hellos coming back.

The commands below are incorrect because the VLAN is 56, not 10, and the group number is 10, not 56:

router1(config)# interface VLAN 10 router1(config-if)# standby 56 preempt

The command below is incorrect because it is not executed under the VLAN 56 interface:

router1(config)# standby 10 preempt

The command below is incorrect because it is not executed under the VLAN 56 interface and the HSRP number is incorrect:

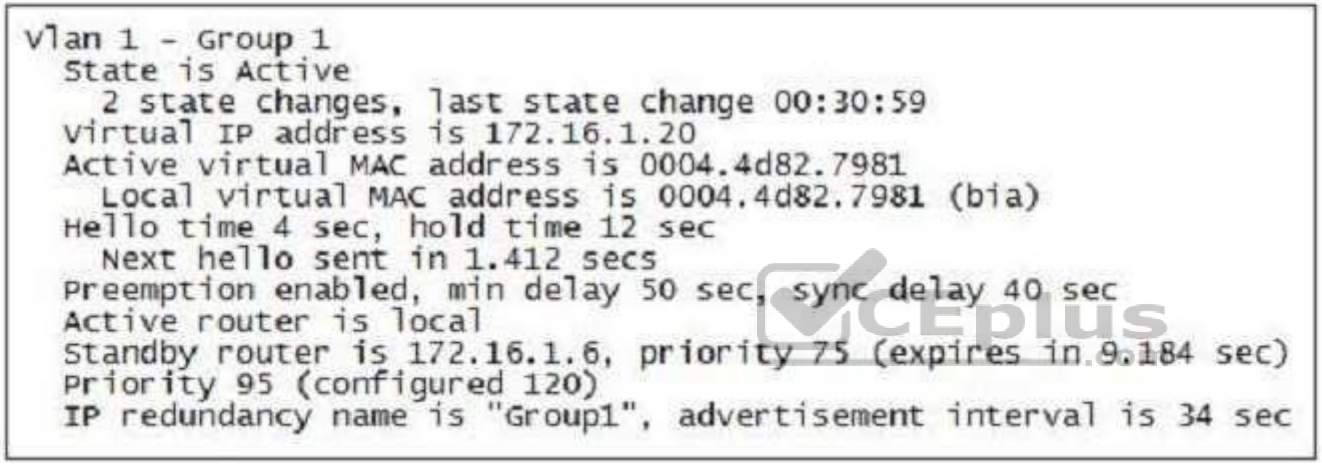
router1(config)# standby 56 preempt

Objective:

Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing
Cisco > Cisco IOS IP Application Services Command Reference > standby preempt through weight > standby preempt

QUESTION 7
The partial output displayed in the exhibit is a result of what IOS command? (Click on the Exhibit(s) button.)



```
Vlan 1 - Group 1
  State is Active
    2 state changes, last state change 00:30:59
  Virtual IP address is 172.16.1.20
  Active virtual MAC address is 0004.4d82.7981
    Local virtual MAC address is 0004.4d82.7981 (bia)
  Hello time 4 sec, hold time 12 sec
    Next hello sent in 1.412 secs
  Preemption enabled, min delay 50 sec, sync delay 40 sec
  Active router is local
  Standby router is 172.16.1.6, priority 75 (expires in 9.184 sec)
  Priority 95 (configured 120)
  IP redundancy name is "Group1", advertisement interval is 34 sec
```

A. switch# show running-config
B. switch# show standby vlan1 active brief
C. switch# show hsrp 1
D. switch# show standby

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command show standby produces the output displayed in the exhibit. This command displays information about HSRP on all configured interfaces and for all HSRP groups. Important information in the exhibit includes that this router is the active router, the virtual IP address for the HSRP group is 172.16.1.20, the address of the standby router is 172.16.1.6, and the router is configured to preempt.

The command show running-config will display the complete configuration of the device, including the configuration of HSRP, but will not display the current status of HSRP on the switch.

The command show standby vlan 1 active brief provides a summary display of all HSRP groups on the switch that are in the active state. This output would provide basic information, not nearly the detail indicated in the exhibit. The following is an example of output for show standby vlan 1 active brief:

```
Interface Grp Prio P State Active addr Standby addr Group addr
Vlan1 0 120 Active 172.16.1.5 Unknown 172.16.1.20
```

The command show hsrp 1 is not valid due to incorrect syntax.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Cisco > Cisco IOS IP Application Services Command Reference > show ip sockets through standby name > show standby
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

QUESTION 8

You have been assigned to create a plan to implement HSRP on the router connecting your company's network to the Internet. The router should be the active router in the HSRP group. On the active router, the following conditions should be met:
▪ Enable preemption with no delay
▪ Set Hello timer to 10 seconds and hold time to 25 seconds ▪
Set the priority to 150

Which of the following commands should be included in the plan to meet the given requirements? (Choose all that apply.)

A. standby 1 preempt delay minimum 10
B. standby 1 preempt
C. standby 1 priority 150
D. standby 1 timers 10 25
E. standby 1 timers 25 10
F. standby track interface S0/1

Correct Answer: BCD

Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following commands should be included in the implementation plan to meet the given requirements:

```
standby 1 preempt
standby 1 priority 150
standby 1 timers 10 25
```

The standby 1 preempt command configures the preempt settings on the router. This command allows preemption without any delay. The standby 1 priority 150 command sets the priority of the router to 150. The default priority of HSRP routers is 100. This implies that this router becomes the active router if there are no other routers in the group with a higher priority. The standby 1 timers 10 25 command sets the Hello timer and the hold time on the local router. The first value, 10, specifies the Hello timer, and the second value, 25, indicates the hold time.

The most essential steps to configure HSRP on routers are as follows:

- Assign IP addresses to the interfaces using the ip address command
- Enable HSRP on the interfaces and assign the virtual IP address using the standby ip command
- Set the HSRP priority of the interfaces using the standby priority command
- Configure HSRP preempt settings on the interfaces using the standby preempt command
- Set the Hello timers using the standby timers command
- Enable interface tracking for other HSRP-enabled interfaces using the standby track command

The standby 1 preempt delay minimum 10 command should not be included in the implementation plan. This command causes the router to preempt the active router after a minimum of 10 seconds. However, the requirement states that there should be no delay in preemption (a delay of 0 seconds), which is the default behavior.

The standby 1 timers 25 10 command should not be included in the implementation plan. This command sets the Hello timer to 25 seconds and the hold time to 10 seconds. However, the requirement is to set the Hello timer to 10 seconds and the hold time to 25 seconds.

The standby track interface S0/1 command should not be included in the implementation plan. This command enables tracking of the S0/1 interface on the local router. However, there is no requirement in the scenario to track an interface. Tracking can be used to decrement the priority of an HSRP router when the interface goes down. Using the default decrement value, if S0/1 were to go down, the priority of the router would be reduced by 10.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:

Home > Support > Configuring HSRP > How to Configure HSRP
Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing > Configuring HSRP

QUESTION 9
Which statement best describes the function of Hot Standby Router Protocol (HSRP)?

A. HSRP specifies a single IP address that all routers in the group must use.
B. HSRP defines a set of routers that represent one virtual, fault-tolerant router.

C. HSRP provides a round-robin gateway selection process to increase fault tolerance.
D. HSRP defines a frame-tagging scheme that allows end stations to use any router as a gateway.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Hot Standby Router Protocol (HSRP) is specified by RFC 2281. The primary function of HSRP is to define a set of routers that work together to represent one virtual, fault-tolerant router. Thus, redundancy is provided in the event that any one of the routers fails. HSRP can be configured on the following interface types:
- Routed ports
- Switched virtual interfaces (SVI) ▪
Etherchannel port channels

HSRP does use a single IP address to represent a group of routers, but this does not fully describe the function of HSRP.

HSRP does not provide round-robin gateway selection. HSRP uses router priority to select a primary and standby router.

HSRP does not define a frame-tagging scheme that allows end stations to use any router as a gateway. End stations use the virtual IP address of a group of HSRP routers as the default gateway.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

QUESTION 10

Which of the following statements best describes the result of issuing the command standby 44 timers 3 1 on an HSRP router?

A. The holdtime will be set to a value of 3, and the hellotime will be set to a value of 1.
B. The status of the standby router will be displayed as unknown expired.
C. The role of active router will be passed repeatedly from one router to another.
D. The router will be configured to reassume the role of active router in the event that the router fails and is subsequently restarted.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

When the command standby 44 timers 3 1 is issued on a Hot Standby Routing Protocol (HSRP) router, the role of active router will be passed repeatedly from one router to another. This behavior occurs when the timers are set incorrectly. The syntax for the standby timers command is standby [group-number] timers [hellotime holdtime].

The hellotime variable is the number of seconds between hello messages and is set to a value of 3 by default.

The holdtime variable is the number of seconds that the HSRP standby router will wait before assuming that the active router is down; if the standby router believes the active router to be down, it will assume the role of active router.

The holdtime is set to a value of 10 by default. The holdtime should be set to a value at least three times the value of the hellotime. Otherwise, the active router might not be able to respond before the standby router assumes that the active router is down and becomes the new active router.

Because the command standby 44 timers 3 1 sets the hellotime to a value of 3 and the holdtime to a value of 1, the role of active router will be passed from one standby router to the next. To set the holdtime to a value of 3 and the hellotime to a value of 1, the command standby 44 timers 1 3 should be issued. To reset the timer values to their default values, the command no standby group-number timers should be issued.

The status of the standby router will be displayed as unknown expired if a Physical layer problem exists. The unknown expired status can also be displayed if only one HSRP router is configured for the subnet.

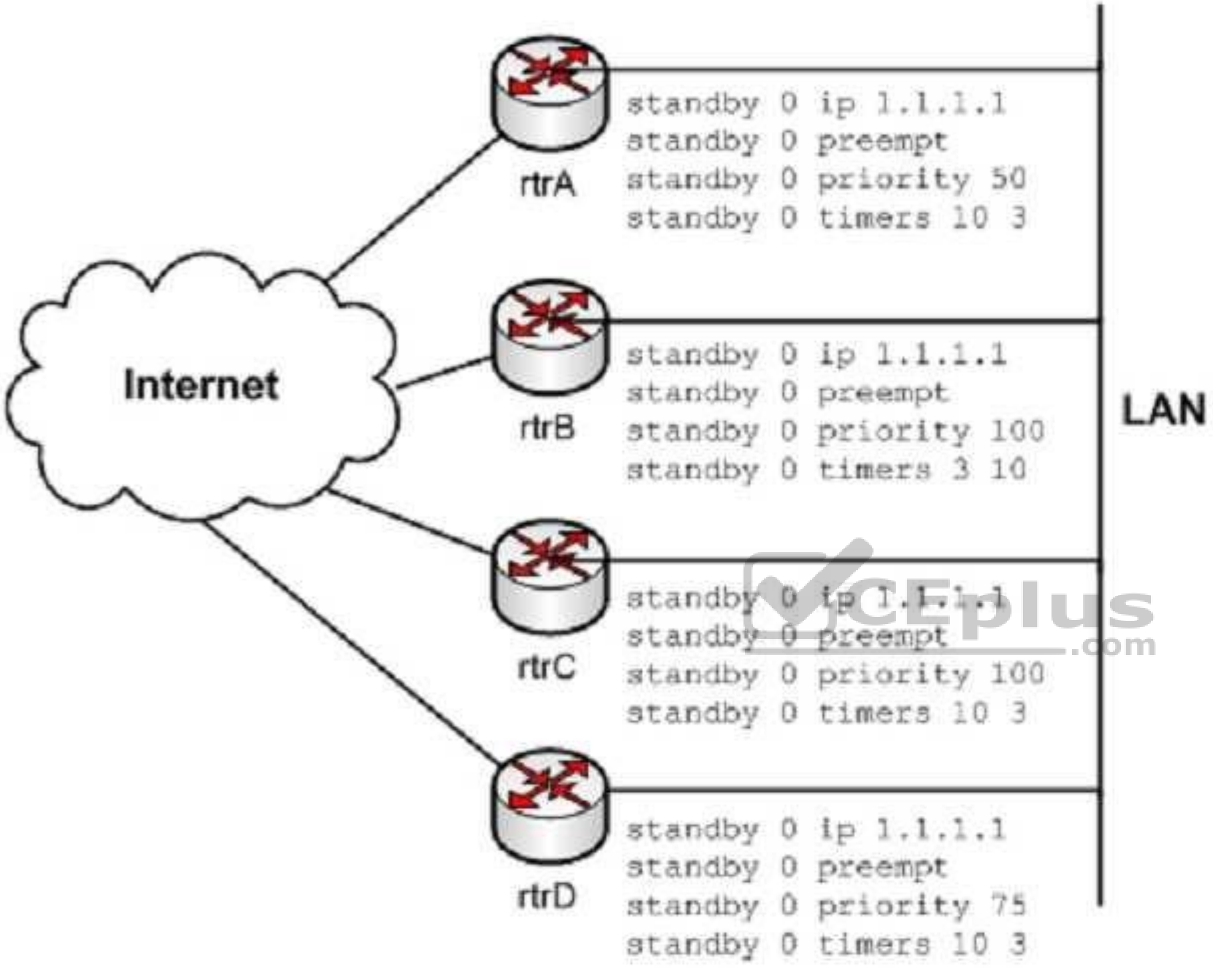
To configure an HSRP router to reassume the role of active router in the event that the router fails and is subsequently restarted, the command standby groupnumber preempt should be issued. When the HSRP active router fails or is shut down, the standby router assumes the role of active router. By default, when the original HSRP active router is restarted, it does not take the role of active router away from the original standby router, even if the original active router has a higher priority value. The command standby group-number preempt changes this default behavior.

The holdtime will not be set to a value of 3, and the hellotime will not be set to a value of 1. On the contrary, the hellotime will be set to a value of 3 and the holdtime will be set to a value of 1.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Cisco IOS IP Application Services Command Reference > show vrrp through synguard (virtual server) > standby timers
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

QUESTION 11
Refer to the following exhibit:



rtrA

```
standby 0 ip 1.1.1.1
standby 0 preempt
standby 0 priority 50
standby 0 timers 10 3
```

rtrB

```
standby 0 ip 1.1.1.1
standby 0 preempt
standby 0 priority 100
standby 0 timers 3 10
```

rtrC

```
standby 0 ip 1.1.1.1
standby 0 preempt
standby 0 priority 100
standby 0 timers 10 3
```

rtrD

```
standby 0 ip 1.1.1.1
standby 0 preempt
standby 0 priority 75
standby 0 timers 10 3
```

You have configured the routers in the diagram for HSRP, resulting in the displayed configurations.

Which of the following routers were configured with the default HSRP values for each command?

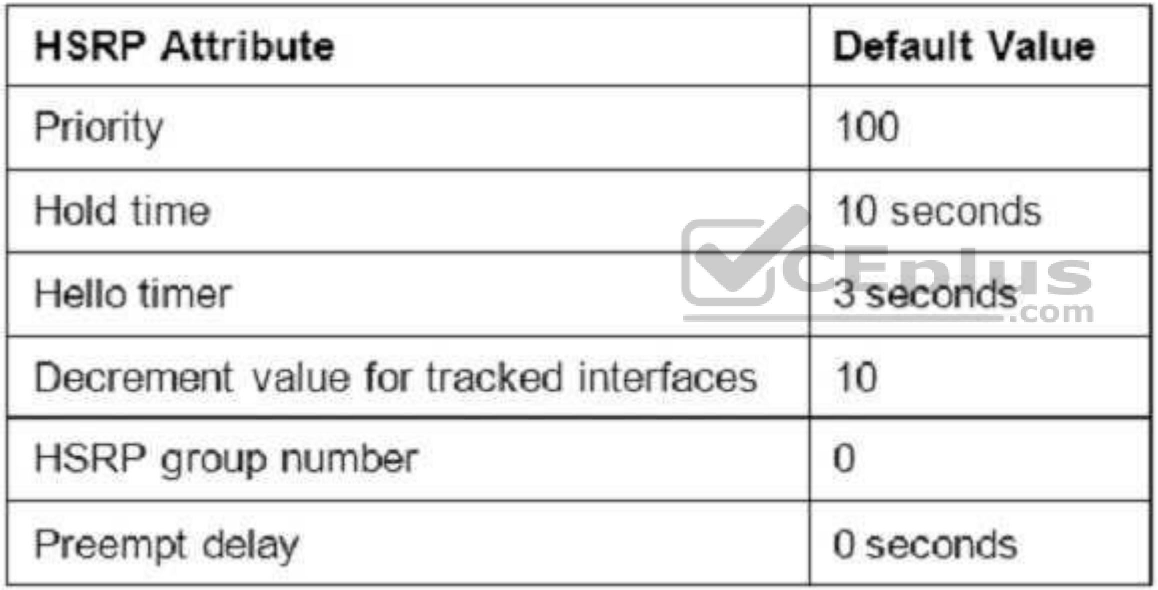
A. rtrA
B. rtrB
C. rtrC

D. rtrD

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Only rtrB has the default HSRP settings. The default values for some of the important parameters for an HSRP-enabled router are listed in the following table:



HSRP Attribute	Default Value
Priority	100
Hold time	10 seconds
Hello timer	3 seconds
Decrement value for tracked interfaces	10
HSRP group number	0
Preempt delay	0 seconds

In this case, the routers have the default group number 0. The two routers rtrB and rtrC have the default priority value of 100, srtrB also has the default timer values, which are 3 seconds for the Hello timer and 10 seconds for the hold time.

The rtrA router is not configured with the default settings because the priority is set to 50, which is not the default value. In addition, the Hello timer is set to 10 seconds (default is 3 seconds) and the hold time is set to 3 seconds (default is 10 seconds)

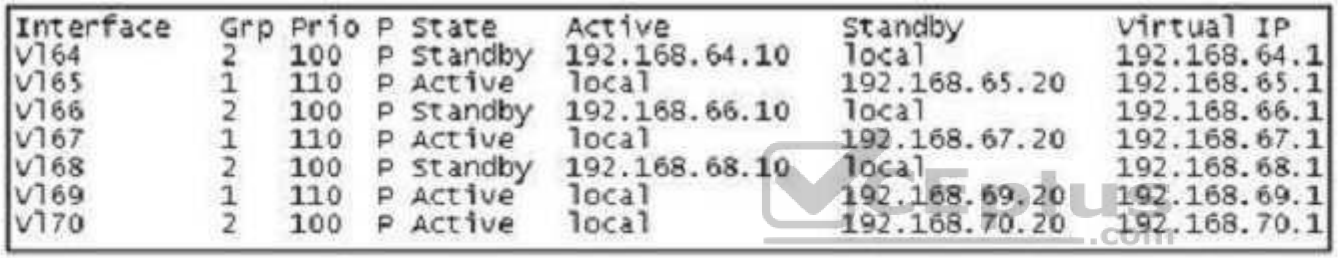
The rtrC router is not configured with the default settings. Although the priority is 100, which is the default, the Hello timer is set to 10 seconds (default is 3 seconds) and the hold time is set to 3 seconds (default is 10 seconds).

The rtrD router is not configured with the default settings. It has a priority of 75 and the default is 100.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Home > Support > Configuring HSRP > How to Configure HSRP
Cisco IOS Master Command List, Release 12.4>show lnm station through system (ERM policy) > standby track
Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing > Configuring HSRP

QUESTION 12
What command would provide the output displayed in the exhibit? (Click on the Exhibit(s) button.)



```
Interface     Grp Prio P State    Active          Standby         Virtual IP
Vl64          2   100  P Standby  192.168.64.10   local           192.168.64.1
Vl65          1   110  P Active   local           192.168.65.20   192.168.65.1
Vl66          2   100  P Standby  192.168.66.10   local           192.168.66.1
Vl67          1   110  P Active   local           192.168.67.20   192.168.67.1
Vl68          2   100  P Standby  192.168.68.10   local           192.168.68.1
Vl69          1   110  P Active   local           192.168.69.20   192.168.69.1
Vl70          2   100  P Active   local           192.168.70.20   192.168.70.1
```

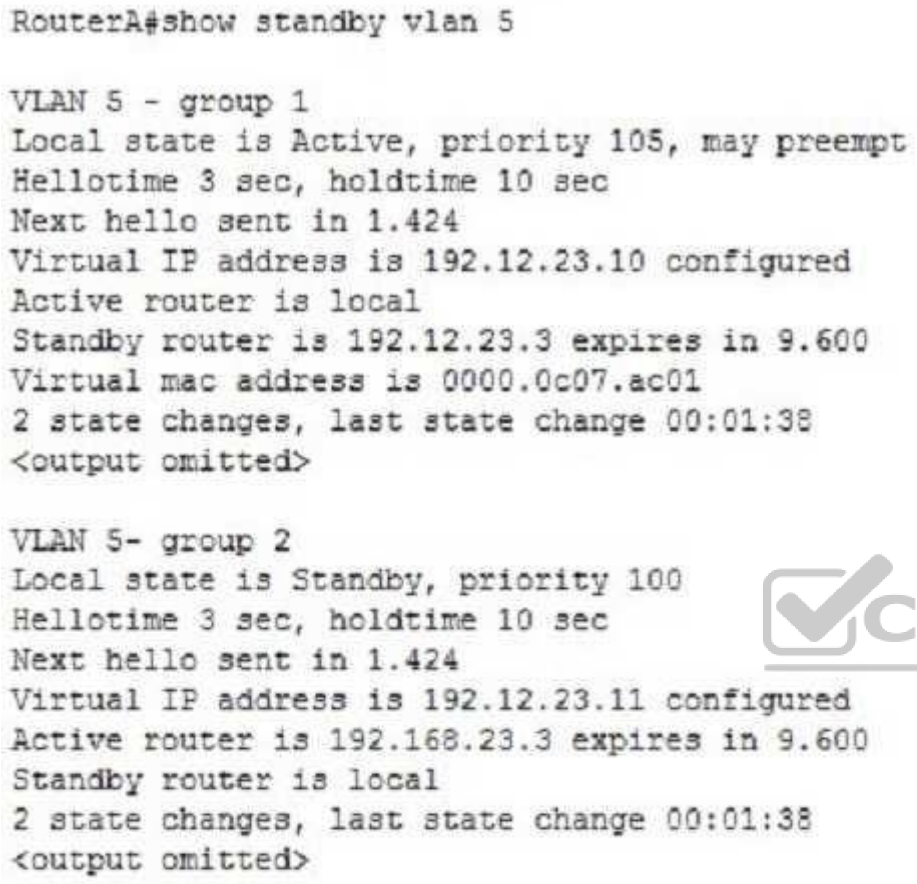
A. switch# show hsrp
B. switch# show standby
C. switch# show interface vlan
D. switch# show standby brief

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
Explanation:

The command show standby brief displays the output in the exhibit. It is used to display a summary of the HSRP groups of which the switch is a member. The summary information it provides includes the group number, priority, state, active device address, standby address, and group address. In the exhibit, the interface VLAN 64 is a member of HSRP group 2. Its priority in the group is 100 and it is currently the standby switch. Since preemption is configured (as indicated by the P following the priority), we know that the priority of this switch must be lower than the priority of the active device. The active device has an IP address of 192.168.64.10 and the group IP address is 192.168.64.1.

The command show standby can be used to display detailed information about HSRP groups of which a switch is a member. It does not provide the quick summary display of the exhibit. This command displays information about HSRP on all configured interfaces and for all HSRP groups. It also displays hello timer information and the expiration timer for the standby switch. The command syntax is show standby [type number [group]].

Below is an example of this command's output:



```
RouterA#show standby vlan 5

VLAN 5 - group 1
Local state is Active, priority 105, may preempt
Hellotime 3 sec, holdtime 10 sec
Next hello sent in 1.424
Virtual IP address is 192.12.23.10 configured
Active router is local
Standby router is 192.12.23.3 expires in 9.600
Virtual mac address is 0000.0c07.ac01
2 state changes, last state change 00:01:38
<output omitted>

VLAN 5- group 2
Local state is Standby, priority 100
Hellotime 3 sec, holdtime 10 sec
Next hello sent in 1.424
Virtual IP address is 192.12.23.11 configured
Active router is 192.168.23.3 expires in 9.600
Standby router is local
2 state changes, last state change 00:01:38
<output omitted>
```

In the above output, Router A is load-sharing traffic for VLAN 5. It is active for group 1 and standby for group 2. The router at address 192.168.23.3 is active for group 2 and standby for group 1. This allows traffic to be sent to both routers while still allowing for redundancy. Router A was also configured with the standby 1 preempt command (results seen in line 1), which allows it to resume its role as active for group 1 if it comes back up from an outage.

The command show interface vlan is not a complete command. A VLAN number must follow the command. When provided with a VLAN number, the output would display the status of the SVI, but no HSRP information.

The command show hsrp is not a valid command due to incorrect syntax.

Objective:
Infrastructure Services

Sub-Objective:
Configure and verify first-hop redundancy protocols

References:
Cisco > Cisco IOS IP Application Services Command Reference > show standby through show udp > show standby

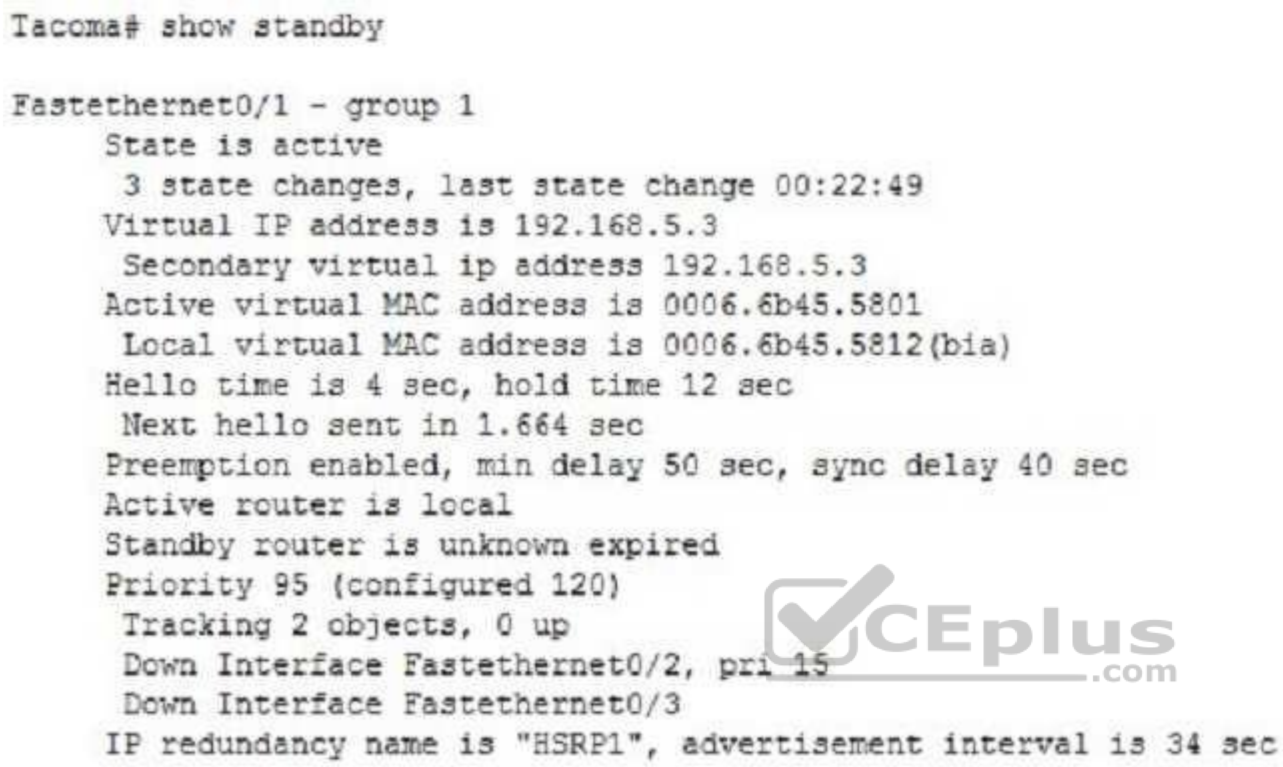
QUESTION 13
What command can be used on a Cisco switch to display the virtual MAC address for the HSRP groups of which the switch is a member?

A. switch# show standby mac
B. switch# show hsrp mac
C. switch# show standby
D. switch# show standby brief

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command show standby can be used to display the virtual MAC address for HSRP groups of which a switch is a member. This command displays information about HSRP on all configured interfaces and for all HSRP groups. It also displays hello timer information and the expiration timer for the standby switch. The standby switch will take over as the active switch if the timer expires before it hears a heartbeat from the active switch. Below is an example of the show standby command for the HSRP group 1:

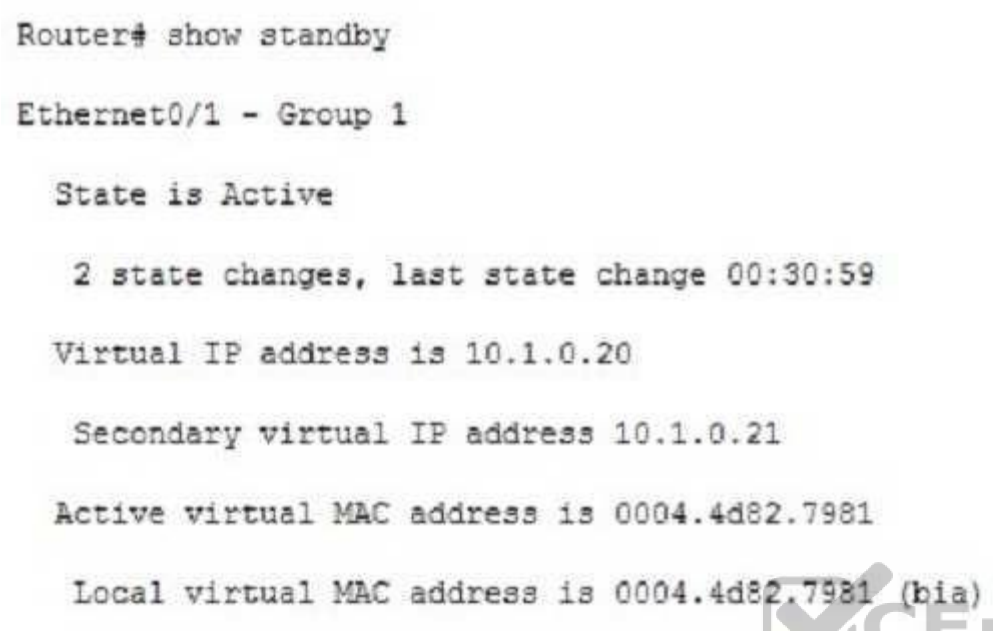


```
Tacoma# show standby

Fastethernet0/1 - group 1
     State is active
      3 state changes, last state change 00:22:49
     Virtual IP address is 192.168.5.3
      Secondary virtual ip address 192.168.5.3
     Active virtual MAC address is 0006.6b45.5801
      Local virtual MAC address is 0006.6b45.5812(bia)
     Hello time is 4 sec, hold time 12 sec
      Next hello sent in 1.664 sec
     Preemption enabled, min delay 50 sec, sync delay 40 sec
     Active router is local
     Standby router is unknown expired
     Priority 95 (configured 120)
      Tracking 2 objects, 0 up
      Down Interface Fastethernet0/2, pri 15
      Down Interface Fastethernet0/3
     IP redundancy name is "HSRP1", advertisement interval is 34 sec
```

In the above output, the following can be determined:

- The router is currently active for the group, as can be seen in line 2. The Active Virtual MAC address is 0006.6b45.5801, which includes the group number (1) in the last two positions, which is why the address is different from the routers actual MAC address shown on the next line. Special Note: Some router models (Cisco 2500, 4000 and 4500) WILL NOT use this altered MAC address format, but will instead use the real MAC address for the virtual MAC address and will display that MAC address as the virtual MAC address in the output of the show standby command. An example of the output of the show standby command on an older router such as the 2500 would be as follows:



```
Router# show standby

Ethernet0/1 - Group 1

  State is Active

   2 state changes, last state change 00:30:59

  Virtual IP address is 10.1.0.20

   Secondary virtual IP address 10.1.0.21

  Active virtual MAC address is 0004.4d82.7981

   Local virtual MAC address is 0004.4d82.7981 (bia)
```

These routers have Ethernet hardware that only recognize a single MAC address. In either case, if for some reason this router becomes the standby router, such as due to loss of interfaces, then when the interfaces come back up it will be able to recover the active role because it is set for preemption, as shown on line 10.

- The router is tracking two of its own interfaces. Because both interfaces are down, the router's priority has been reduced by 25 (15 for Fastethernet0/2 and 10 for Fastethernet0/3), from the configured value of 120 to 95. This data is shown on lines 13-16. The default is 10 if not otherwise specified, as is the case for Fastethernet0/3.
- If either of the two interfaces comes back up, the priority will be increased by the amount assigned to the interface. For example, if Fastethernet0/3 comes back up, the priority will become 105 (95 + 10).
- The standby router is unreachable, which can be determined because it is marked unknown expired in line 12. This could be due to either a physical layer issue or an HSRP misconfiguration.

The command show standby brief can be used to view summary information about HSRP groups of which the switch is a member. This information includes the group number, priority, state, active device address, standby address, and group address. It does not include the virtual MAC address.

The commands show standby mac and show hsrp mac are invalid due to incorrect syntax.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Cisco > Cisco IOS IP Application Services Command Reference > show standby
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

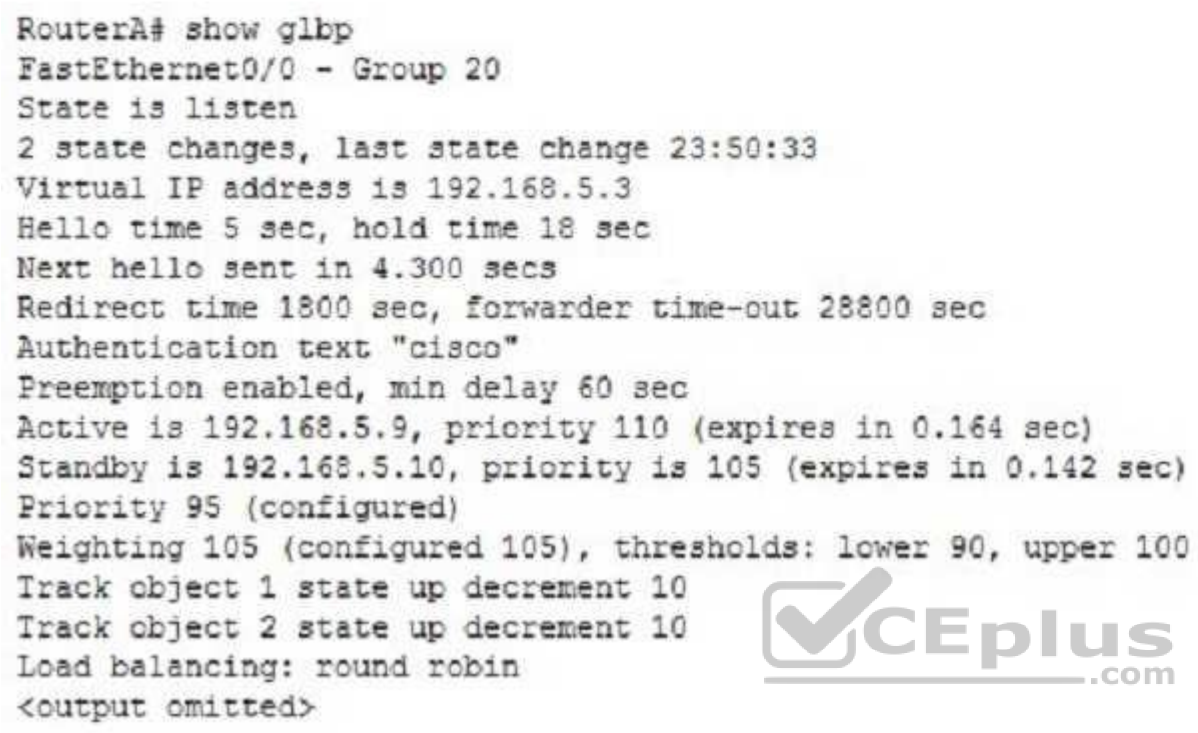
QUESTION 14
What command displays detailed information about the GLBP groups to which the switch belongs?

A. switch# show standby
B. switch# show glbp state
C. switch# show glbp
D. switch# show standby detail

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command show glbp displays detailed information about GLBP groups on the switch. This information includes the GLBP groups the switch is a member of, whether this is the active switch, the virtual IP address, and whether preemption is enabled. Below is an example of the command output.



```
RouterA# show glbp
FastEthernet0/0 - Group 20
State is listen
2 state changes, last state change 23:50:33
Virtual IP address is 192.168.5.3
Hello time 5 sec, hold time 18 sec
Next hello sent in 4.300 secs
Redirect time 1800 sec, forwarder time-out 28800 sec
Authentication text "cisco"
Preemption enabled, min delay 60 sec
Active is 192.168.5.9, priority 110 (expires in 0.164 sec)
Standby is 192.168.5.10, priority is 105 (expires in 0.142 sec)
Priority 95 (configured)
Weighting 105 (configured 105), thresholds: lower 90, upper 100
Track object 1 state up decrement 10
Track object 2 state up decrement 10
Load balancing: round robin
<output omitted>
```

The following can be learned from this output:

- This router is the active virtual forwarder (AVF). In line 3, the output indicates the state is listen. This is the state of the active AVF.
- As indicated in line 14, this router is configured with a weighting for tracking of 105. It also is configured with an upper limit of 100 and a lower limit of 90. When a tracked object goes down, the value of 105 will be reduced by the decrement value associated with that object. If this results in the weighting dropping below the lower limit (90), this router will give up its role as AVF.
- The router is tracking two objects, and both have decrement values of 10. This means that ONLY if both objects go down will this router relinquish its role as AVF. As there is another router to take the role of AVF, there will be no disruption of traffic, even if hosts were using the tracked interface that went down.

The show glbp state will only display the glbp state of the router (standby, listen etc). Detailed output is accomplished with the command show glbp.

The command show standby can be used to display detailed information about HSRP groups to which a switch belongs. This command is for HSRP only.

The command show standby detail provides the same output as show standby. It can be used to display detailed information about HSRP groups to which a switch belongs. This command is for HSRP only.

Objective:

Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring GLBP

QUESTION 15
Which next-hop router redundancy protocol provides backup for an assigned real IP address?

A. HSRP
B. GLBP
C. VRRP
D. CGMP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Using VRRP, the shared address of the next-hop router redundancy group can be the real address of a router interface.

Virtual Router Redundancy Protocol (VRRP) is defined in RFC 2338. VRRP enables a group of routers to form a single virtual router, known as a VRRP group. Routers are configured in VRRP groups to provide redundancy for an IP address shared among members of the VRRP group. This address can be the real address of a router interface or a virtual address (or addresses) shared by the group. Each group is comprised of a master and one or more backup routers. If the shared address is the real IP address of a router, that router will always be the master when the address is available. The master router is responsible for forwarding packets sent to the virtual router. The backup routers provide redundancy and stand ready to assume the role of the master router in the event that it is unable to forward packets.

The master virtual router owns the VRRP IP address and is responsible for handling all packets sent to the VRRP IP address. Backup VRRP routers monitor for hello activity from the master virtual router. The master router will advertise using IP 224.0.0.18 and MAC 0000.0c00.01xx (xx is the VRRP Group ID). The advertisements by default will be sent every second, and the master down interval is three seconds.

If the VRRP IP address is NOT the physical address of one of the VRRP routers, then the router with the highest priority will assume the role of the master. The configurable priority range is from 0 to 255, and the default value is 100. The higher the value is, the higher the priority is. If activity stops for the duration of the master router's down interval, the backup router with the highest priority will become the master router. When the old master router comes back online, it will assume the master role again if it still has the highest priority among all routers.

In the configuration shown below, Router A will be the master router unless it goes down, in which case B will take over. If A comes back up it will assume the master role again.

routerA(config-if)# vrrp 3 priority 130 routerB(config-
if)# vrrp 3 priority 110

Hot Standby Router Protocol (HSRP) defines a set of routers that work together to represent one virtual, fault-tolerant router. Thus, redundancy is provided in the event that any one of the routers fails. The shared address of the next-hop router redundancy group is not the real address of a router interface.

Gateway Load Balancing Protocol GLBP) is a Cisco-designed protocol that provides for the dynamic utilization of redundant routers in a broadcast network. The shared address of the next-hop router redundancy group is not the real address of a router interface. A virtual group address is used.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring VRRP

QUESTION 16
When executed on a HSRP group member named Router 10, what effect does the following command have?

Router10(config-if)# standby 1 track serial0 25

A. It will cause the router to increase its HSRP priority by 25 if the Serial0 interface on the standby router goes down
B. It will cause the router to shut down the Serial0 interface if 25 packets have been dropped
C. It will cause the router to notify Router 25 is serial 0 goes down
D. It will cause the router to decrement its HSRP priority by 25 if Serial 0 goes down

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

This command will cause the router to decrement its HSRP priority by 25 if Serial 0 goes down. Interface tracking can be configured in Hot Standby Routing Protocol (HSRP) groups to switch traffic to the standby router if an interface goes down on the active router. This is accomplished by having the active router track its interface. If that interface goes down, the router will decrement its HSRP priority by the value configured in the command. When properly configured, this will cause the standby router to have a higher HSRP priority, allowing it to become the active router and to begin serving traffic.

When the standby router in an HSRP group is not taking over the active role when the active router loses its tracked interface, it is usually a misconfigured decrement value, such that the value does not lower the HSRP priority of the active router far enough for the standby to have a superior priority value.

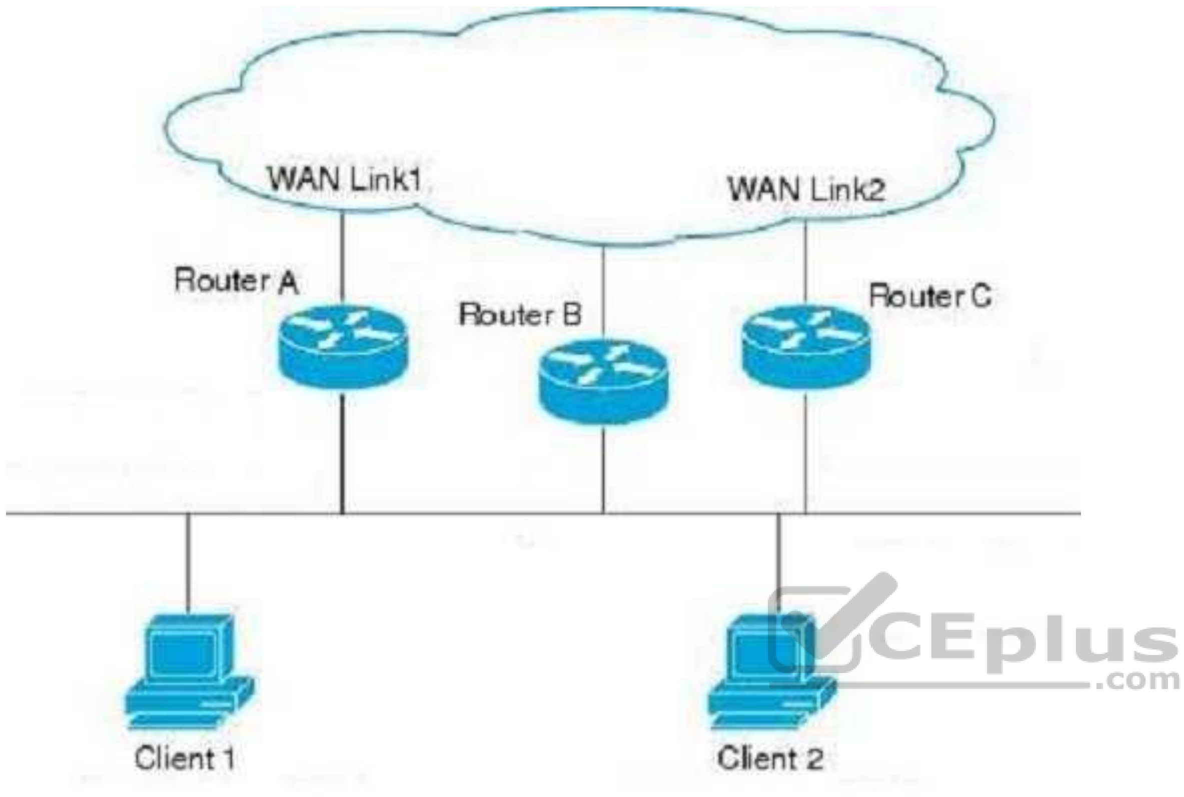
The command will not cause the router to increase its HSRP priority by 25 if the Serial0 interface on the standby router goes down. HSRP routers track their own interfaces, not those of another router.
The command will not cause the router to shut down the Serial0 interface if 25 packets have been dropped. It will only do this if the link becomes unavailable.

The command will not cause the router to notify Router 25 is serial 0 goes down. The number 25 in the command is the decrement value, not the ID of another router.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Cisco > Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > How to Use the standby preempt and standby track Commands

QUESTION 17
A company has the following network infrastructure. (Refer to the exhibit.)



Router A is a GLBP active virtual gateway with priority level set to 250. Routers B and C are configured with the default GLPB configurations. The configuration of the active virtual gateway needs to be changed such that if the AVG fails, Router C should be elected to be used as an active virtual gateway. As the network administrator, you have been asked to make corresponding changes to the configuration.

Which command would you use for this purpose on Router C, and where would the command be configured?

A. glbp 10 preempt (on Router B)
B. glbp 10 preempt (on Router C)
C. glbp 10 priority 200 (on Router B)
D. glbp 10 priority 200 (on Router C)

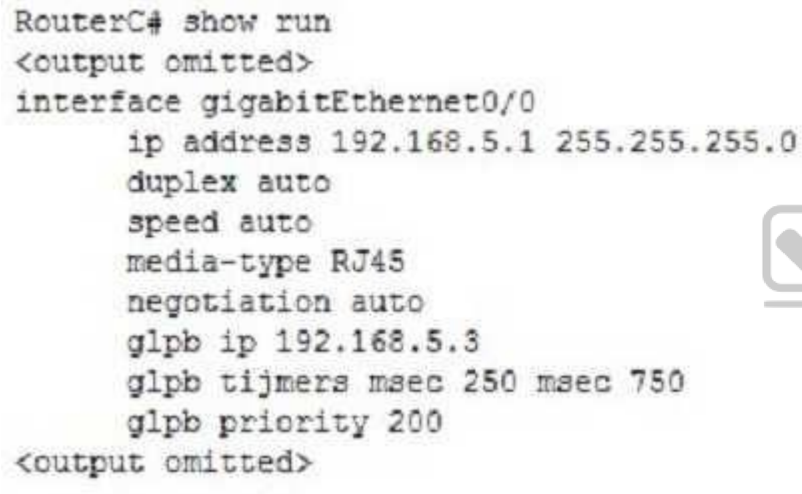
Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:

You would configure the glbp 10 priority 200 command on Router C to change the configuration as required. Gateway Load Balancing Protocol (GLBP) gateway priority determines the role that each GLBP gateway plays and what happens if the AVG fails. In the given scenario, Router A is used as an active virtual gateway. If the AVG in a LAN topology fails, an election process takes place to determine which backup virtual gateway should take over. When you configure this command on Router C, Router C will be elected when Router A fails as an AVG.

Once the configuration change is made, it can be verified by examining the output if the show run command as shown below:



```
RouterC# show run
<output omitted>
interface gigabitEthernet0/0
      ip address 192.168.5.1 255.255.255.0
      duplex auto
      speed auto
      media-type RJ45
      negotiation auto
      glpb ip 192.168.5.3
      glpb tijmers msec 250 msec 750
      glpb priority 200
<output omitted>
```

In the above output, it can be determined that the glpb priority 200 command has been applied to the gigabitEthernet0/0 interface on Router C. If the default priority of 100 had been applied, there would be no line in the output for priority. Because Router B is configured with the default configuration, it will have its priority set to the default level as 100.

You would not use the glbp 10 preempt command on Router B or the glbp 10 preempt command on Router C to change the configuration. You would use this command on a router to enable preemption. Preemption allows a virtual router that was once the AVG to assume its role as active virtual router when it comes back online if it has a higher priority than the current AVG. Alternatively, it can enable a new router with a higher priority to take the role of AVG from the current AVG if the new router has a higher AVG.

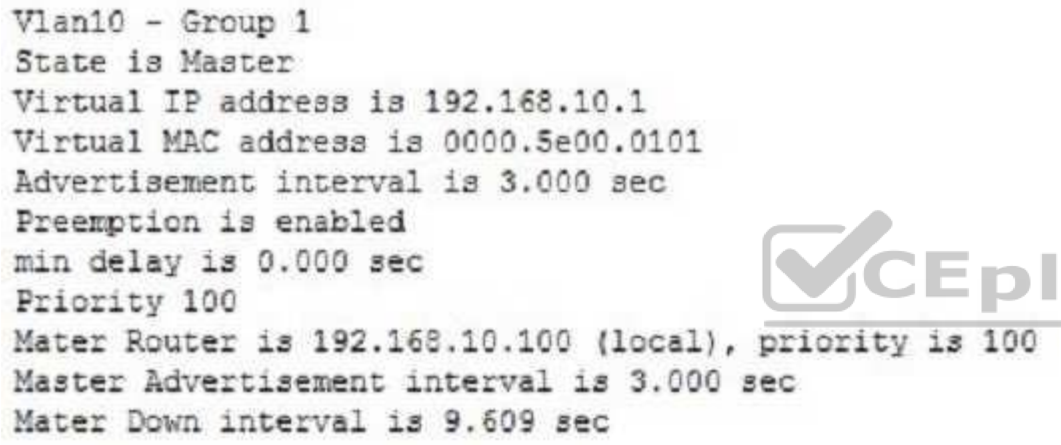
You would use not the glbp 10 priority 200 command on Router B to change the configuration. You would run this command if you needed Router B to be elected as the AVR instead of Router C, as running this command on Router B would configure it with higher priority than Router C.

Objective:

Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Cisco > Home > End-of-Sale and End-of-Life Products > Cisco IOS Software Releases > 12.2T > Product Literature > White Papers > GLBP - Gateway Load Balancing Protocol
Cisco > Cisco IOS IP Application Services Command Reference > glbp priority

QUESTION 18
What command provides the output shown below?



```
Vlan10 - Group 1
State is Master
Virtual IP address is 192.168.10.1
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3.000 sec
Preemption is enabled
min delay is 0.000 sec
Priority 100
Mater Router is 192.168.10.100 (local), priority is 100
Master Advertisement interval is 3.000 sec
Mater Down interval is 9.609 sec
```

A. switch# show vrrp brief
B. switch# show standby
C. switch# show glbpD. switch# show vrrp

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command that displays the output in the exhibit is show vrrp. This command displays detailed information regarding VRRP groups on the switch. The information provided for each VRRP group by this command includes the status, virtual IP and MAC addresses, whether preemption is enabled, priority of the switch, and the address of the group master.

The command show vrrp brief is used to display a summary of the VRRP groups to which the switch belongs. The summary information it provides includes the group number, priority, state, whether preemption is enabled, the Master IP address, and the group IP address.

The command show glbp displays detailed information about GLBP groups on the switch. This information includes the GLBP groups the switch is a member of, whether this is the active switch, the virtual IP address, and whether preemption is enabled.

The command show standby can be used to display detailed information about HSRP groups to which a switch belongs. This command displays information about HSRP on all configured interfaces and for all HSRP groups. This command is for HSRP only.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Cisco > Cisco IOS IP Application Services Command Reference > show vrrp

QUESTION 19
You need to create an implementation plan for providing Layer 3 redundancy in your switched network. You included Hot Standby Routing Protocol (HSRP) as the protocol to avoid first-hop router failure. However, your supervisor suggests including Virtual Router Redundancy Protocol (VRRP) instead of HSRP in the implementation plan.

Which of the following statements is TRUE about the reasons for the suggested change in the implementation plan? (Choose two.)

A. HSRP works only on Cisco routers and VRRP works on both Cisco and non- Cisco routers.
B. HSRP works on both Cisco and non-Cisco routers and VRRP works only Cisco routers.
C. HSRP-enabled routers need to be configured manually to preempt the active router and VRRP-enabled routers preempt it automatically.
D. HSRP-enabled routers automatically preempt the active router and VRRP-enabled routers need to be configured manually to preempt the active router.

Correct Answer: AC

Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following two statements are TRUE:

- HSRP works only on Cisco routers and VRRP works on both Cisco and non- Cisco routers.
- HSRP-enabled routers need to be configured manually to preempt the active router and VRRP-enabled routers preempt it automatically.

HSRP was developed by Cisco intended for only Cisco routers and VRRP was developed by IEFT intended as a standard for routers. HSRP was defined in RFC 2281 and VRRP was defined in RFC 2338. Both these protocols provide a fault tolerance solution by grouping several routers together but presenting them as a single router. One of the routers in the group acts as the active or master router. A second router is selected as the standby router. In case the active or master router fails, the standby router takes over the responsibilities of the active router.

The router with the highest priority is automatically selected as the active or master router. In HSRP, preempt settings have to be manually configured on every router in the group, even if the routers have a priority higher than that of the active router. However, in VRRP, the routers with higher priority automatically preempt the master router. Another advantage that VRRP has over HSRP is a faster Hello timer (1 second). HSRP has a Hello timer of 3 seconds

Two other protocols ICMP Router Discovery Protocol (IRDP) and Gateway Load Balancing Protocol (GLBP) provide redundancy for first-hop router failure. IRDP also allows the selection of a new router if the active router fails, while GLBP provides load balancing in addition to redundancy.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Home > Articles > Cisco Certification > CCDP > CCDP Self Study: Designing High-Availability Services
Cisco First Hop Redundancy Protocols Configuration Guide, Cisco Release 15MT

QUESTION 20
In which HSRP state is the router a candidate to become the next active router for the group?

A. Learn
B. Backup
C. Listen
D. Initial
E. Standby

Correct Answer: E

Section: (none)
Explanation

Explanation/Reference:
Explanation:

The HSRP router in standby state (the standby router) is a candidate to become the next active HSRP router should the current active router fail.

The six HSRP states are defined as follows:

- Initial state: All routers start in this state.
- Learn state: The router is in the learn state when it has not communicated with the active router. It does not know which router is the active router and does not know the IP address of the virtual router (if no HSRP IP address configured in the router).
- Listen state: Once the router hears from the active router and knows the virtual IP address, it enters the listen state. It is not the active or standby router. ▪ Speak state: After a router learns the IP address of the virtual router, it enters the speak state. It participates in the active and standby router election. It sends hello messages to the active router.
- Standby state: When the active router has been elected, the second router enters the standby state. This is the standby router and it will become the active router if the active router fails.
- Active state: The router is in active state when it is forwarding packets. It receives packets via the virtual IP address.

Backup is not a valid HSRP router state.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

QUESTION 21
Which routers comprise a VRRP group?

A. Host and client
B. Master and backup
C. Active and standby
D. Primary and secondary

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Virtual Router Redundancy Protocol (VRRP) enables a group of routers to form a single virtual router, known as a VRRP group. Routers are configured in VRRP groups to provide redundancy for a virtual IP address shared among members of the VRRP group. Each group is comprised of a master router and one or more backup routers. The physical IP address of the master router will be the virtual IP address of the group.

The master router is responsible for forwarding packets sent to the virtual router. The backup routers provide redundancy and stand ready to assume the role of the master router in the event that the master is unable to forward packets.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring VRRP

QUESTION 22
Which of the following is required to allow load balancing between three HSRP routers connected to the same LAN?

A. A single HSRP group with all three routers as active routers for the group
B. A single HSRP group with one active router for the group
C. Two HSRP groups, each with an active router
D. Two HSRP groups with one active router for both the groups
E. Three HSRP groups, each with an active router
F. Three HSRP groups with one active router for all groups

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

You should configure three HSRP groups on all three routers and select an active router for each of the groups. You can create up to 256 (0 to 255) groups. Each router should be the active router for one of the three groups and the standby router for the remaining two groups.

If you want to use HSRP on a Layer 3 switch, the switch ports must be one of the following: ▪
EtherChannel port Refers to a Layer 3 switch port used for EtherChannel
▪ Routed port Refers to a Layer 3 port on a switch used for routing and for inter-VLAN routing

- Switch virtual interface (SVI) Refers to a Layer 2 switch port used for inter-VLAN routing

Routed ports are the physical Layer 3 interfaces that allow you to configure a switch as a router. The no switchport command allows the port to be used purely as a Layer 3 port. SVIs are Layer 3 logical interfaces of a switch that allow you to enable inter-VLAN routing on Layer 3 switches. An SVI is configured as a VLAN interface and has at least one physical interface assigned to the VLANs.

Creating a single HSRP group with all three routers as active routers for the group is incorrect. An HSRP group cannot have multiple active routers; it can have only one active router at a time.

Creating a single HSRP group with one active router for the group is incorrect because it does not allow load balancing between the three routers. All traffic will be passed through the active router.

Creating two HSRP groups with an active router each is incorrect because it only allows load balancing between two of the routers and not three of them.

Creating two HSRP groups with one active router for both groups, or three HSRP groups with one active router for all groups, is incorrect. Doing so does not enable load balancing on all three routers. Only the active router will be used for traffic forwarding.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing > Configuring Multiple Hot Standby Groups > Load Sharing
Catalyst 3750 Switch Software Configuration Guide, 12.2(40)SE > Configuring HSRP > Configuring HSRP > HSRP Configuration Guidelines
Catalyst 3750 Switch Software Configuration Guide, 12.2(40)SE > Configuring HSRP > Configuring HSRP > Multiple HSRP

QUESTION 23
Which virtual router states are defined in the GLBP protocol? (Choose two.)

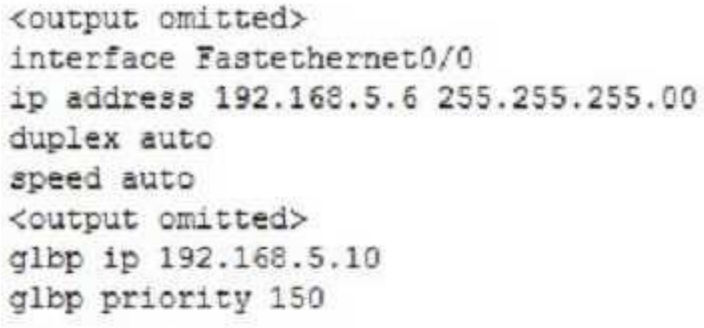
A. Backup gateway
B. Primary gateway
C. Active virtual gateway
D. Active secondary gateway
E. Active virtual forwarder

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Active virtual gateway and active virtual forwarder are the two states defined in the Gateway Load Balancing Protocol (GLBP). The active virtual gateway (AVG) is elected by the members of the GLBP group. The AVG creates the virtual MAC addresses that are assigned to each of the routers in the group. Each router is responsible for handling packets sent to its virtual MAC address. A GLBP router that forwards packets sent to its virtual MAC address is known as the active virtual forwarder (AVF). GLBP members communicate through hello messages sent every 3 seconds to the multicast address 224.0.0.102.

The election of the AVG can be influenced by use of the priority command. By default, all routers configured for GLBP have a priority of 100. A higher value indicates a higher priority. The configured priority of a router can be seen in the show run command as shown below:

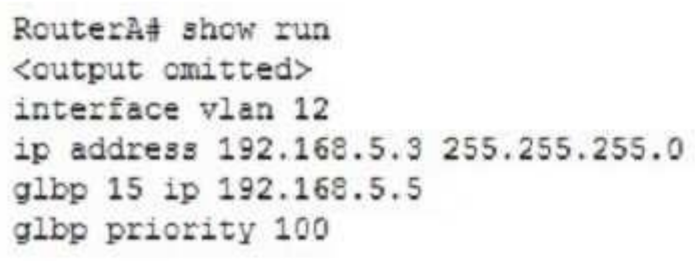


```
<output omitted>
interface Fastethernet0/0
ip address 192.168.5.6 255.255.255.00
duplex auto
speed auto
<output omitted>
glbp ip 192.168.5.10
glbp priority 150
```

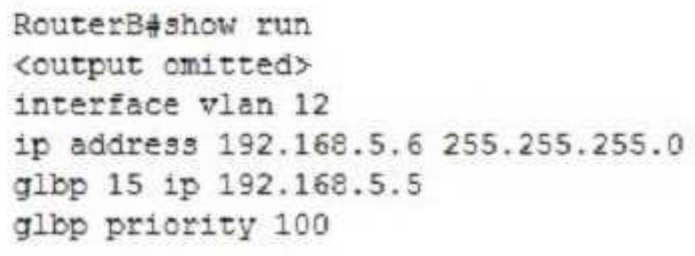
In the above scenario, all other members of the group were left to the default, which can be determined on those routers by the absence of any priority entry in the show run command. In that case, this router would become the AVG. To remove a priority configuration, execute the nostandby priority command. When this command is executed, the router will revert to the default of 100. When all routers are left to the default, the router with the highest configured IP address will become the active router.

GLBP is a Cisco-designed protocol that provides for the dynamic utilization of redundant routers in a broadcast network. It differs from HSRP and VRRP in that it is not necessary to configure multiple groups to fully use redundant paths or routers. GLBP has a configurable load-balancing mechanism that will distribute the use of redundant gateways servicing a broadcast network, such as an Ethernet LAN. Each host will have its gateway set to the address of the AVG. When a host issues an ARP to resolve its gateway's MAC Address, the AVG will respond with the virtual MAC address of a selected AVF. The AVG will perform load balancing by varying which virtual MAC it selects to use in the response. The AVF will own that assigned virtual MAC as long as the gateway is active. If an AVF becomes unable to provide service as gateway, another AVF can assume ownership of the virtual MAC.

Consider the partial output of the show run command for two routers participating in the GLBP group shown below:



```
RouterA# show run
<output omitted>
interface vlan 12
ip address 192.168.5.3 255.255.255.0
glbp 15 ip 192.168.5.5
glbp priority 100
```



```
RouterB#show run
<output omitted>
interface vlan 12
ip address 192.168.5.6 255.255.255.0
glbp 15 ip 192.168.5.5
glbp priority 100
```

In the above scenario, both routers have the same priority, so Router B will become AVG. Hosts will use a gateway address of 192.168.5.5 (the GLBP virtual address in line 4 of both outputs). When hosts send an ARP message for the MAC address of the gateway, Router B will reply with the MAC address of the next AVF.

The AVG can be configured to use one of three load-balancing algorithms:
▪ Round-Robin Load-Balancing: Using round-robin load- balancing the AVG in turn points to each AVF virtual MAC address in its ARP reply (default method). ▪ Weighted Load-Balancing: Using weighted load- balancing, the AVG selects an AVF virtual MAC address to use in the ARP reply proportionally based on the advertised weight value configured in a GLBP gateway.
▪ Host Dependant Load-Balancing: Using host-dependant load- balancing, the AVG selects an AVF virtual MAC address to use in the ARP reply based on which one the host used previously. A host will use the same AVF as long as the GLBP group is unchanged.
▪ GLBP allows better use of network resources by using the standby router through the load-balancing mechanism. The standby router is an available gateway for the network.

GLBP and HSRP are Cisco-developed solutions. VRRP is defined in RFC 2338.

Backup gateway, primary gateway, and active secondary gateway are not terms used when discussing GLBP.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:

Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring GLBP
Cisco > First Hop Redundancy Protocols Configuration Guide, Cisco IOS Release 12.4 > Configuring GLBP > GLBP Active Virtual Gateway

QUESTION 24
You are troubleshooting a problem with two routers configured in a HSRP group. You intended to configure the routers so that Router A and Router B would each track their respective Fa0/1 interfaces and decrement their priorities for several VLAN groups if the tracked interface went down. However, you find that Router A is not taking over as the active device for the HSRP group on VLAN 101 when the Fa0/1 interface on Router B fails.

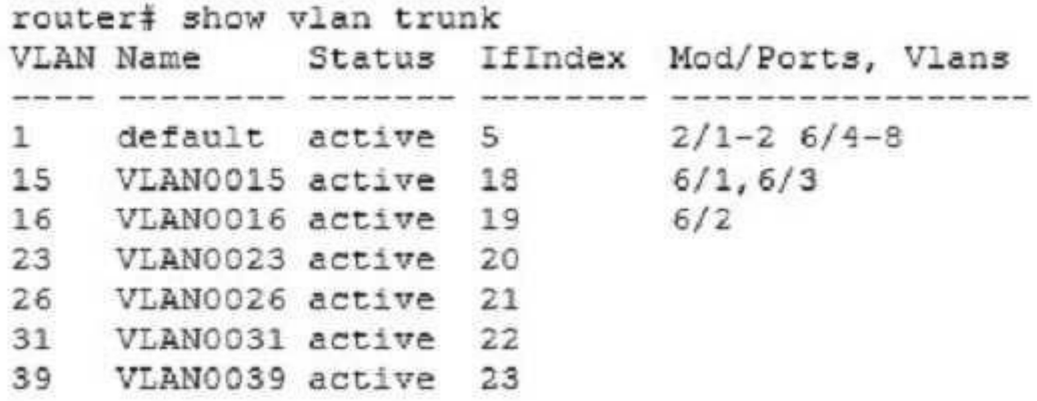
Which command would NOT be useful for discovering the problem?

A. show running-configuration
B. show vlans
C. show standby brief
D. show standby

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The show vlans command would NOT be useful for discovering the problem. When troubleshooting a problem with Hot Standby Router Protocol (HSRP), the show vlans command will yield no useful information. The output of the command is shown below, demonstrating that there is no HSRP information provided.

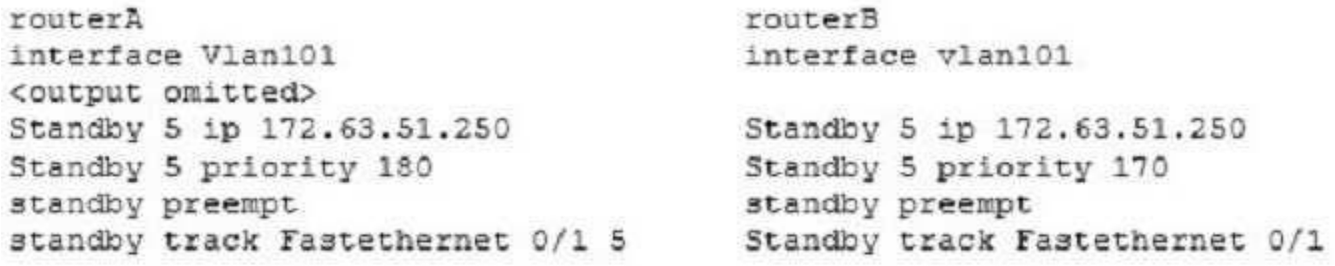


```
router# show vlan trunk
VLAN Name      Status  IfIndex  Mod/Ports, Vlans
---- --------- ------- -------- -----------------
1    default   active  5        2/1-2 6/4-8
15   VLAN0015  active  18       6/1,6/3
16   VLAN0016  active  19       6/2
23   VLAN0023  active  20
26   VLAN0026  active  21
31   VLAN0031  active  22
39   VLAN0039  active  23
```

All three of the remaining commands will be useful in discovering information. Each is shown below with an example of its application to troubleshooting.

Example A:show running-configuration

Router B is not taking over as the active device for VLAN 101's HSRP group when the Fa0/1 interface on Router A fails. Below is a partial output of show run for both routers with the output focused on the section concerning VLAN 101's configuration on each.



```
routerA                                  routerB
interface Vlan101                        interface vlan101
<output omitted>
Standby 5 ip 172.63.51.250               Standby 5 ip 172.63.51.250
Standby 5 priority 180                   Standby 5 priority 170
standby preempt                          standby preempt
standby track Fastethernet 0/1 5         Standby track Fastethernet 0/1
```

The above output displays the source of the problem. Router A has a decrement value of 5 configured for Fa0/1, as shown on the last line of the output after the specification of Fastethernet 0/1. This means that when its Fa0/1 interface goes down, Router A will subtract 5 from its priority for the VLAN 101 group, lowering it to 175. This is still higher than the priority of Router B, which is 170. Therefore, the solution is to change the decrement value for Router A to at least 11. When the interface goes down, Router A's priority will be decremented to 169, allowing Router B to take the role as active for the HSRP group in VLAN 101.

Example B:show standby brief

Router C is not taking over as the active device for VLAN 102's HSRP group when the Fa0/1 interface on Router D fails. Below is a partial output of show standby brief for both routers C and D, with the output focused on the section concerning VLAN 102's configuration on each.

Router C

Interface Grp Prio P State Active addr Standby addr Group addr

Fa0/1 102 200 Active local 10.10.10.253 10.10.10.251

Router D

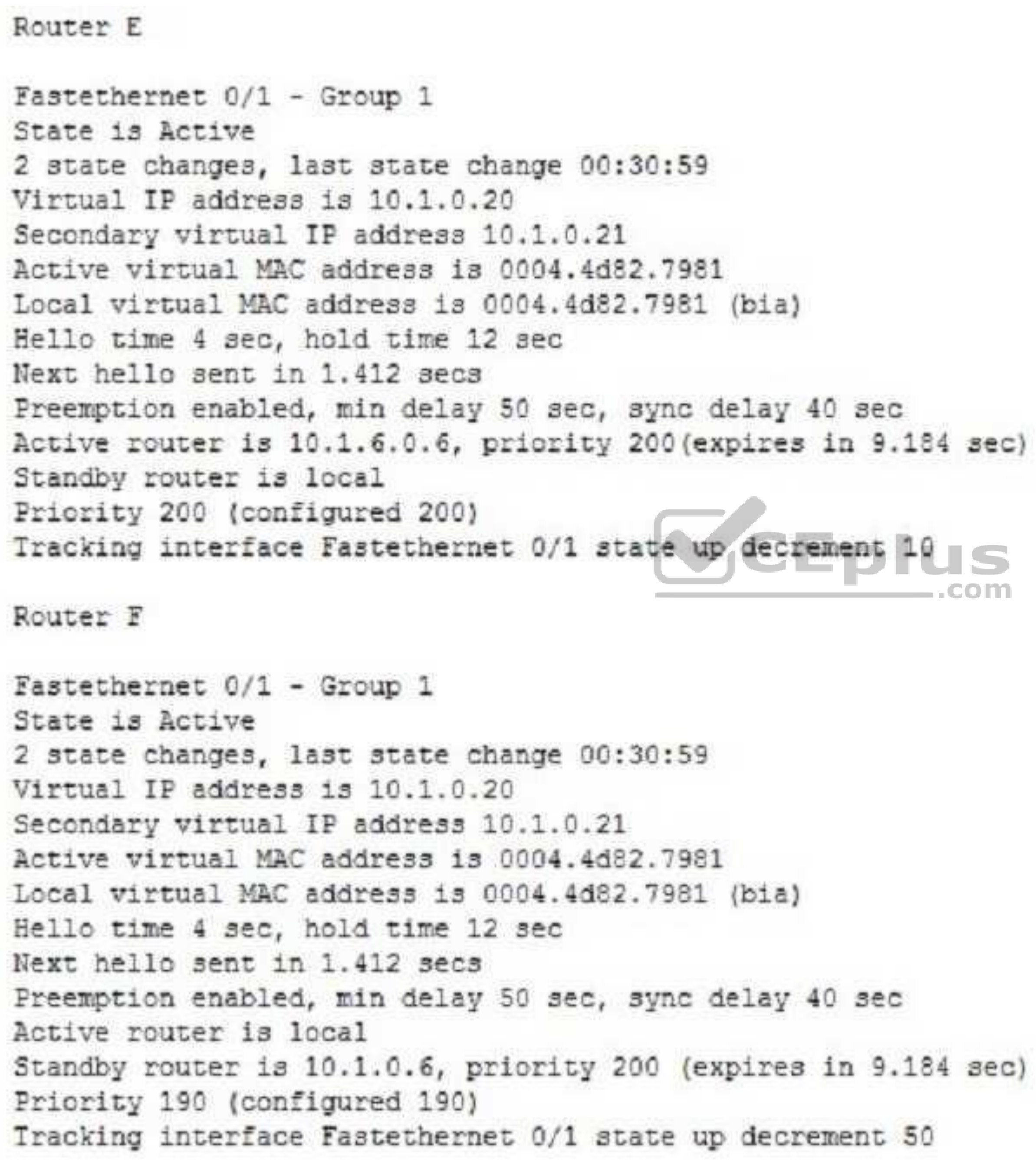
Interface Grp Prio P State Active addr Standby addr Group addr

Fa0/1 102 200 P Active local 10.10.10.253 10.10.10.251

The absence of a P in the P (preempt) column in the output for Router C shows that it is not set to preempt. If not configured to preempt, it will never take over for Router D, regardless of its priority with respect to Router D.

Example C: show standby

Router F is supposed to be the active router for VLAN 103's HSRP group. Occasionally both routers are shut down for maintenance over the weekend. After the routers are rebooted, Router F is not taking over as the active device for VLAN 103's HSRP group. Below is a partial output of the show standby command for both routers, with the output focused on the section concerning VLAN 103's configuration on each



```
Router E

Fastethernet 0/1 - Group 1
State is Active
2 state changes, last state change 00:30:59
Virtual IP address is 10.1.0.20
Secondary virtual IP address 10.1.0.21
Active virtual MAC address is 0004.4d82.7981
Local virtual MAC address is 0004.4d82.7981 (bia)
Hello time 4 sec, hold time 12 sec
Next hello sent in 1.412 secs
Preemption enabled, min delay 50 sec, sync delay 40 sec
Active router is 10.1.6.0.6, priority 200(expires in 9.184 sec)
Standby router is local
Priority 200 (configured 200)
Tracking interface Fastethernet 0/1 state up decrement 10

Router F

Fastethernet 0/1 - Group 1
State is Active
2 state changes, last state change 00:30:59
Virtual IP address is 10.1.0.20
Secondary virtual IP address 10.1.0.21
Active virtual MAC address is 0004.4d82.7981
Local virtual MAC address is 0004.4d82.7981 (bia)
Hello time 4 sec, hold time 12 sec
Next hello sent in 1.412 secs
Preemption enabled, min delay 50 sec, sync delay 40 sec
Active router is local
Standby router is 10.1.0.6, priority 200 (expires in 9.184 sec)
Priority 190 (configured 190)
Tracking interface Fastethernet 0/1 state up decrement 50
```

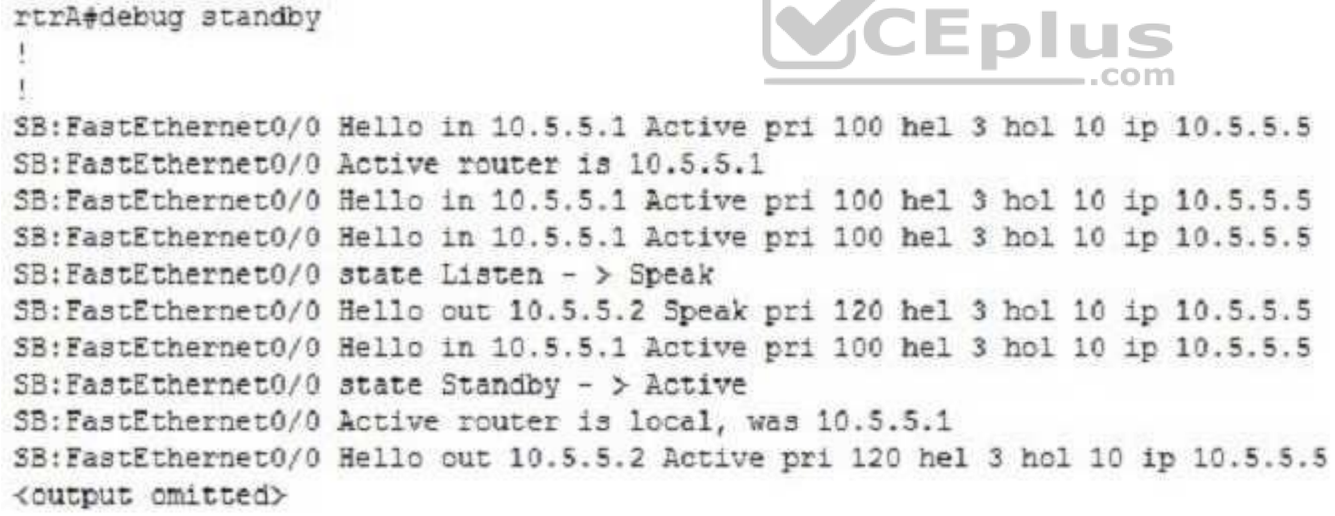
The output shows that Router F is not assuming the active role because of the priority and decrement values configured on the routers. When both routers go down, Router E will decrement its priority (200) by 10, as shown in last two lines of its output, leaving the priority at 190. Router F will decrement its priority (190) by 50 as shown in last two lines of its output, leaving the priority at 140. Therefore, to ensure that Router F maintains its role as active even after the dual shutdowns, the priority of Router F should be increased to at least 241. When both routers decrement their priorities after shutdown, Router F will then have a priority of 191, which will be higher than the priority value of Router E.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Cisco > Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > Understanding and Troubleshooting HSRP Problems in Catalyst Switch Networks
Cisco > Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > How to Use the standby preempt and standby track Commands

QUESTION 25

Refer to the following partial output of the debug standby command on an HSRP-enabled router rtrA:



```
rtrA#debug standby
!
!
SB:FastEthernet0/0 Hello in 10.5.5.1 Active pri 100 hel 3 hol 10 ip 10.5.5.5
SB:FastEthernet0/0 Active router is 10.5.5.1
SB:FastEthernet0/0 Hello in 10.5.5.1 Active pri 100 hel 3 hol 10 ip 10.5.5.5
SB:FastEthernet0/0 Hello in 10.5.5.1 Active pri 100 hel 3 hol 10 ip 10.5.5.5
SB:FastEthernet0/0 state Listen - > Speak
SB:FastEthernet0/0 Hello out 10.5.5.2 Speak pri 120 hel 3 hol 10 ip 10.5.5.5
SB:FastEthernet0/0 Hello in 10.5.5.1 Active pri 100 hel 3 hol 10 ip 10.5.5.5
SB:FastEthernet0/0 state Standby - > Active
SB:FastEthernet0/0 Active router is local, was 10.5.5.1
SB:FastEthernet0/0 Hello out 10.5.5.2 Active pri 120 hel 3 hol 10 ip 10.5.5.5
<output omitted>
```

Which of the following information CANNOT be gathered from the given partial output?

A. IP address of the virtual router
B. IP address of the current active router

C. Priority of the active router
D. The tracked interfaces

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The debug standby command does not provide any information about the tracked HSRP interfaces. This command displays information regarding the changes in the state of the HSRP routers and packet transmissions between the routers. Some of the information that you can view using the debug standby command is as follows:

- IP address of the virtual router
- IP address of the current active router
- Priority of the active router
- Hello timer values
- Hold time values
- State of the router
- Interface used to exchange HSRP packets

HSRP packets contain the IP address of the virtual router. The IP address preceded by the text ip in the debug standby output is the address of the virtual router. In this case, the packets contain 10.5.5.5 after the text ip. This implies that 10.5.5.5 is the IP address of the virtual router.

After HSRP selects the active and standby routers for a group, only the active and standby routers send HSRP packets to the virtual router. If the active router fails, the standby router becomes the active router. The text Hello in and the text Hello out indicate the hello packets received from and sent to the given IP address. Initially the router with IP address 10.5.5.1 is the active router, as indicated by the text Active router is 10.5.5.1.

The priority of the active router is 100, which is indicated by the text pri 100. However, when a hello packet from 10.5.5.2 is received, which has a higher priority (120) than the active router, the 10.5.5.2 router automatically and instantly becomes the active router. This implies that the router with the IP address 10.5.5.2 was the standby router and the standby preempt command was executed.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify first-hop redundancy protocols

References:
Cisco IOS Debug Command Reference > debug sntp adjust Through debug tag-switching xtagatm vc > debug standby

Home > Support > Technology Support > IP > IP Application Services > Configure > Configuration Examples and Technotes > Avoiding HSRP Instability in a

Switching Environment with Various Router Platforms > Troubleshoot > Troubleshooting Commands > Sample Debug Output
Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > Understanding and Troubleshooting HSRP Problems in Catalyst Switch Networks > Understand HSRP

QUESTION 26
Which three methods can be used to manage Cisco APs that are running autonomously? (Choose three.)

A. WLSE
B. WLC
C. WCS
D. CLI
E. Web interface

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The three methods that can be used to manage autonomous APs are WLSE, CLI, and web interfaces. Autonomous access points (APs) maintain their management functionality and can be connected directly and configured. The wireless LAN solution engine (WLSE) allows for centralized coordination of autonomous APs. The WLSE can also work in coordination with another Cisco service, wireless domain services (WDS). The WDS enables the APs to provide fast, secure roaming between APs. The WDS registers all client devices in the subnet, establishes session keys for them, and caches their security credentials. When a client roams to another access point, the WDS device forwards the client's security credentials to the new access point

Wireless LAN controller (WLC) is a physical controller that provides centralized control of a WLAN environment. APs that are being managed by a WLC function in lightweight mode.

Wireless control system (WCS) is a software package that allows for management of a WLAN environment, managing one or multiple WLCs. APs managed by WCS function in lightweight mode.

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

References:
Cisco > Products and Services > Cloud and Systems Management>End-of-sale and End-of-life products>Ciscoworks Wireless Lan Solution E(WLSE>Data sheets and literature>Data sheets>Ciscoworks Wireless Lan Solution engine 2.13

QUESTION 27
When using auxiliary VLANs, how is a phone configured with the appropriate VLAN to join?

A. the administrator configures the phone with CLI
B. the switch connected to the phone provides the VLAN
C. the PC attached to the phone provides the VLAN information
D. a VMPS server provides the VLAN for the switch and phone

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

When using auxiliary VLANs, the switch connected to the phone provides the VLAN to the phone. 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 other is used to connect to the workstation. The PC attached to the switch port via the IP phone is unaware of the presence of the phone

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

References:
Cisco > Home > Products and Services > Cisco Interfaces and Modules > Cisco Network Modules > Product Literature > Data Sheets > Cisco Catalyst 6500 Series Switches
Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport voice vlan

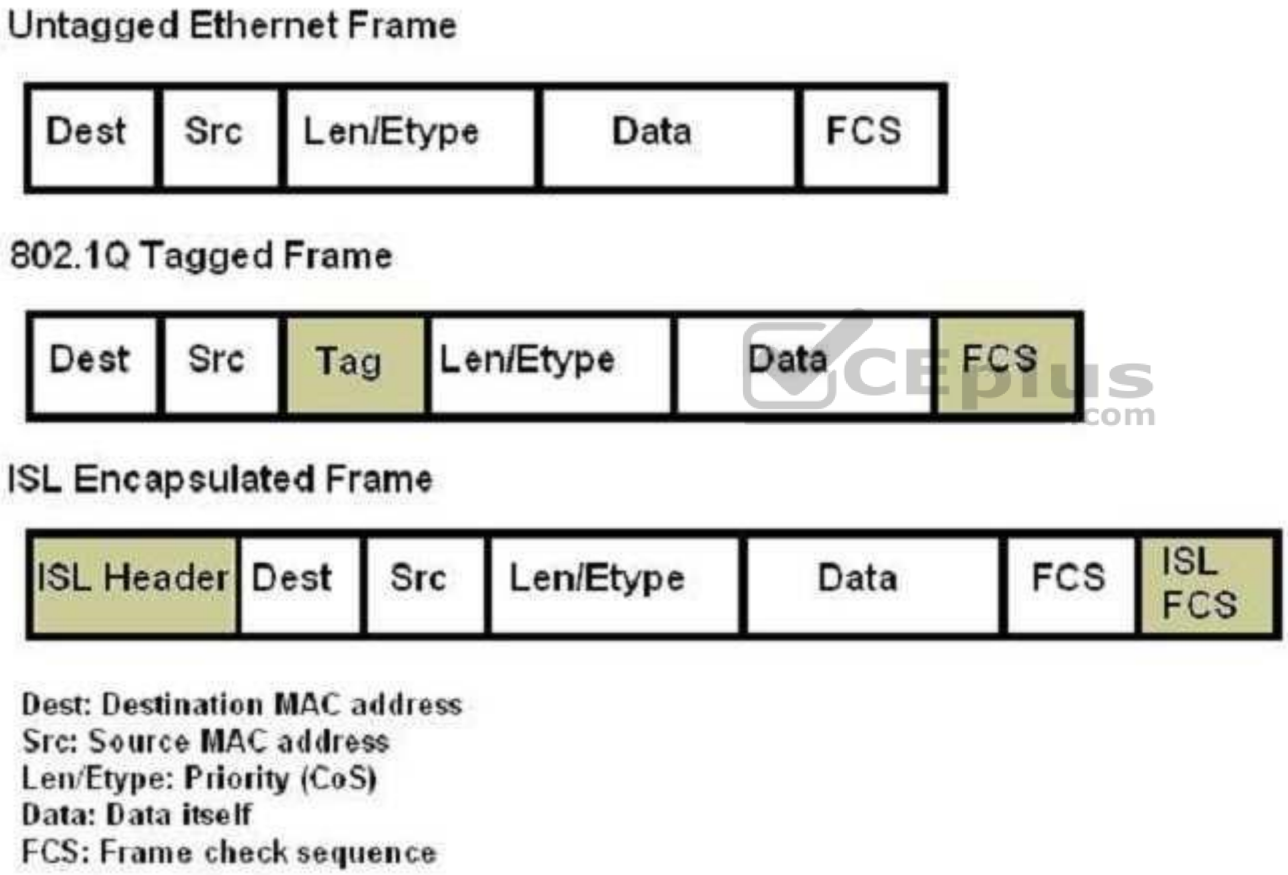
QUESTION 28
Which VLAN trunking protocol adds four bytes to the Ethernet frames?

A. ISL
B. LANE
C. 802.10
D. 802.1Q

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

802.1Q adds 4 bytes to the Ethernet frame. The process is known as 802.1Q tagging, and inserts a four-byte field into the Ethernet frame header between the source address and the Len/Etype fields. This tag identifies the frame as an 802.1Q frame and includes bits used to identify both the priority and the VLAN ID. The VLAN ID field indicates which VLAN the frame belongs to. An 802.1q trunk can support 4096 different VLANs. After the new tag field is inserted into the frame, the frame's previous FCS field is recalculated and replaced. The following graphic shows both the ISL and 802.1Q frame formats as well as the original Ethernet frame:



Dest: Destination MAC address
Src: Source MAC address
Len/Etype: Priority (CoS)
Data: Data itself
FCS: Frame check sequence

Inter switch link (ISL) is a Cisco proprietary trunking protocol that handles the frame in a different manner. It adds a 26- byte frame header and 4-byte trailer to the frame.

LANE (LAN Emulation) is an IEEE standard for identifying VLANs on ATM networks.

802.10 is a Cisco proprietary method of identifying VLANs on FDDI media by writing VLAN information to the Security Association Identifier (SAID) of the 802.10 frame.

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

References:
Cisco > Support > Technology Support > LAN Switching > Virtual LAN/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Inter-Switch Link and IEEE 802.1Q Frame Format

QUESTION 29
Which IOS command configures the switch for the VTP mode that will propagate its VLAN database changes to others in the domain?

A. vtp mode client
B. vtp mode server
C. vtp v1-mode
D. vtp transparent mode

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

```
switch(config)# vtp mode server
```

There are three modes in VTP: server, client, and transparent. The main differentiator among the three modes is whether a switch can create, modify, or delete VLANs. A Catalyst switch can create, modify, and delete VLANs in server or transparent mode, but not in client mode. 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.

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

The 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.

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.

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:

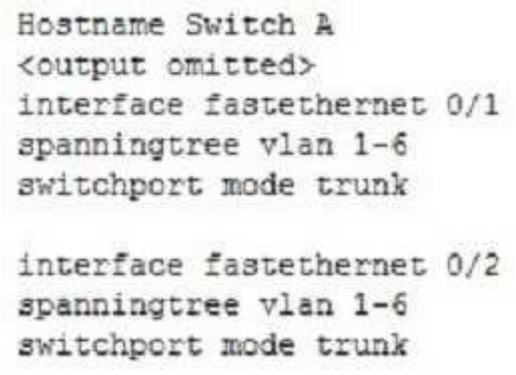
```
switch(config)# vtp domain domain-name
switch(config)# vtp password password
```

The vtp v1-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.

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 30
Examine the following partial output of the show run command. The command was executed from Switch A, which is connected to Switch B through both the Fa0/1 interface and the Fa0/2 interface. Switch A is the root bridge.



```
Hostname Switch A
<output omitted>
interface fastethernet 0/1
spanningtree vlan 1-6
switchport mode trunk

interface fastethernet 0/2
spanningtree vlan 1-6
switchport mode trunk
```

Only one of the links is being used. Your intention was to load share the traffic using both links.

What commands do you need to execute to accomplish this? (Choose two. Each correct answer is part of the solution.)

A. switchA(config)# interface fa0/2switchA(config-if)#spanning-tree vlan 1-3 port-priority 16
B. switchA(config)# interface fa0/1switchA(config-if)#spanning-tree vlan 4-6 port-priority 16
C. switchA(config)# interface fa0/1switchA(config-if)#spanning-tree vlan 1-3 port-priority 128
D. switchA(config)# interface fa0/2switchA(config-if)#spanning-tree vlan 4-6 port-priority 128
E. switchA(config)# interface fa0/1switchA(config-if)#spanning-tree port-priority 20
F. switchA(config)# interface fa0/2switchA(config-if)#spanning-tree port-priority 20

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The correct commands to load share the traffic using both links are:

```
switchA(config)# interface fa0/2
switchA(config-if)# spanning-tree vlan 1-3 port-priority
16 switchA(config)# interface fa0/1 switchA(config-if)#
spanning-tree vlan 4-6 port-priority 16
```

The configuration that was reflected in the exhibit in the show run output indicated that VLANs 1 through 6 were configured under both interfaces. However, the normal operation of STP will block one of the interfaces to prevent a loop. By default, all VLANs are allowed on both trunk links. Load sharing allows you to send some of the VLANs over one of the links and the rest on the other. In this case, the correct option will send VLANs 1-3 over Fa0/1 and VLANs 4-6 over Fa0/2.

By altering the port priority of the VLAN 1-3 on one interface and VLANs 4-6 on the other on the root bridge (Switch A) with the port-priority keyword, the behavior of STP is altered on the other switch. The port priority value must be set in increments of 16. Now Switch A will send VLANs 1-3 over one interface without blocking and 4-6 over the other interface without blocking. The additional benefit to this configuration is that if either link goes down, all VLANs can be sent over the remaining link and until the redundant link comes back up.

The commands below will have no effect because the default port priority is already 128, so the situation will remain the same:

```
switchA(config)# interface fa0/1
switchA(config-if)# spanning-tree vlan 1-3 port-priority
128 switchA(config)# interface fa0/2 switchA(config-if)#
spanning-tree vlan 4-6 port-priority 128
```

The commands below will have no effect because they omit the vlan 1-3 and vlan 4-6 parameters, and therefore change the port priority for all VLANs. Since the port priority is changed equally on both interfaces, there will be no load sharing as a result. More over the priority value is not entered in an increment of 16, which will generate an error message indicating that it must be set in increments of 16.

```
switchA(config)# interface fa0/1
switchA(config-if)# spanning-tree port-priority 20
switchA(config)# interface fa0/2 switchA(config-
if)# spanning-tree port-priority 20
```

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

References:
Cisco > Home > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Design > Design Technotes > VLAN Load Balancing Between Trunks Using the Spanning-Tree Protocol Port Priority
Cisco > Cisco IOS LAN Switching Command Reference > show vlan through ssl-proxy module allowed-vlan > spanning-tree port-priority

QUESTION 31
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.

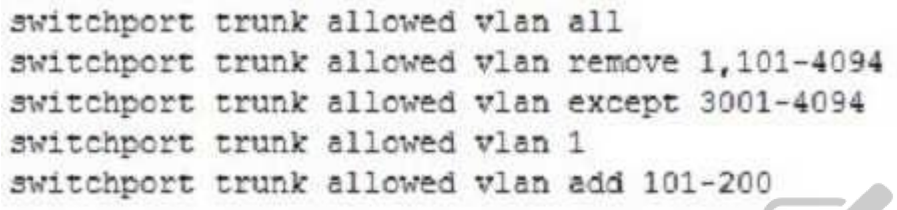
To map one or more VLANs to an MST instance, issue the instance instance-ID vlans vlan-range command, where ID is the number of the MST instance and vlanrange is the VLAN or VLANs that should be mapped to the instance. For example, the command instance 1 vlans 14-16,99 maps VLANs 14 through 16 and VLAN 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 32
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 33
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 forwarddelay 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 34
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 35
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 36
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 37
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 38

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 39
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:

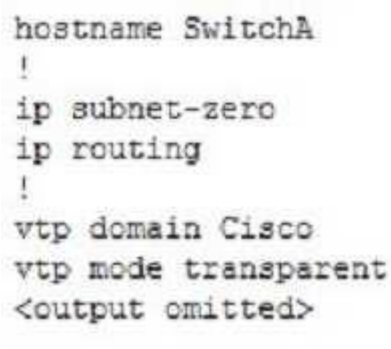
Routing between different VLANs can be accomplished using VLAN-capable multilayer switches or routers.

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 40
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 41
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.

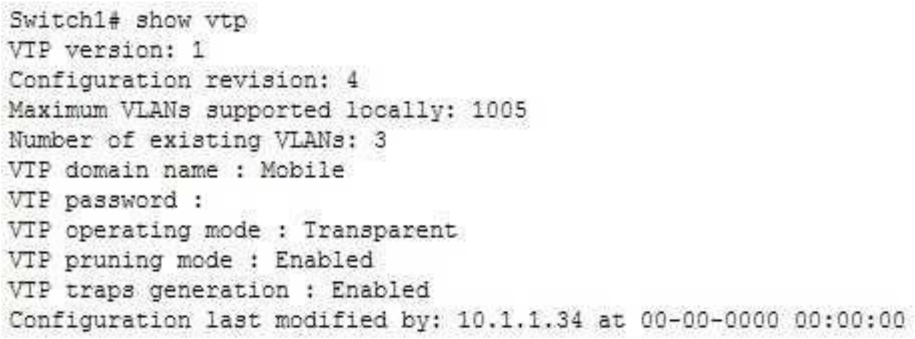
switch(config-if)# switchport

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 42
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 43
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 44
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 45
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.

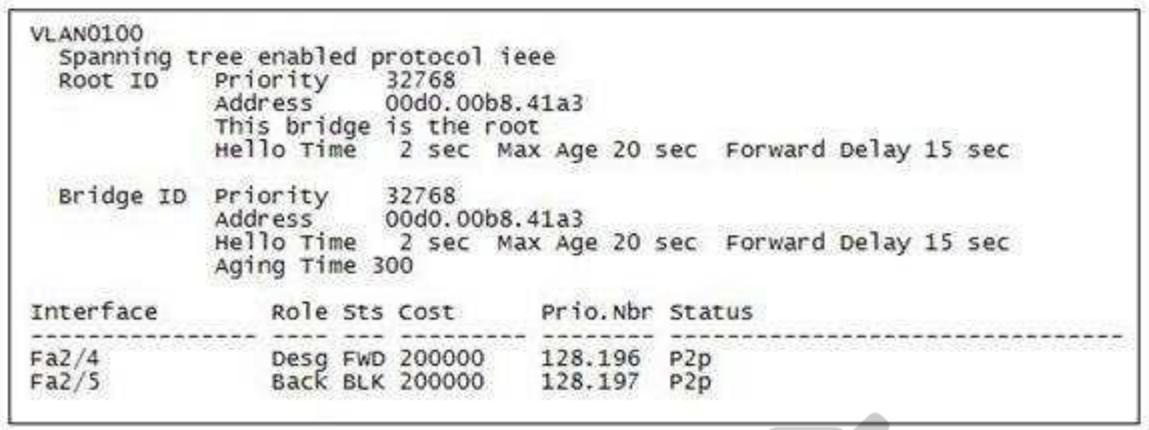
Objective:
Layer 2 Technologies Sub-
Objective:
Configure and verify other LAN switching technologies

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 46

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.

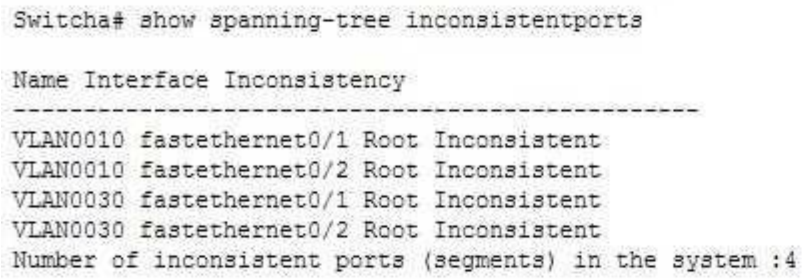
The command show vlan 100 will provide basic information about VLAN 100, such as what ports are assigned to it, but will not display the STP information about the VLAN as the exhibit shows.

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 47

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

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

Correct Answer:
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 48
How is a VLAN best described?

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

D

Correct Answer:
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 49
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

AFG

Correct Answer:
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 50
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)

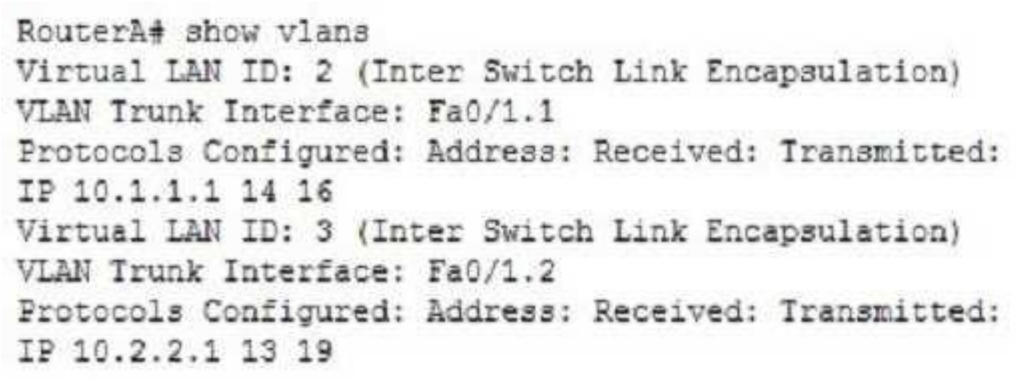
QUESTION 51
What commands can be used to verify the trunking configuration of a router performing inter-VLAN routing? (Choose all that apply. Each correct answer is a complete solution.)

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

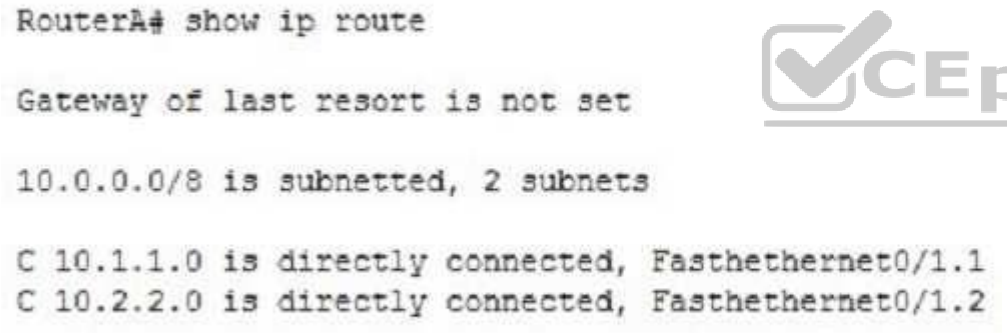
Explanation/Reference:
Explanation:

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 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
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.

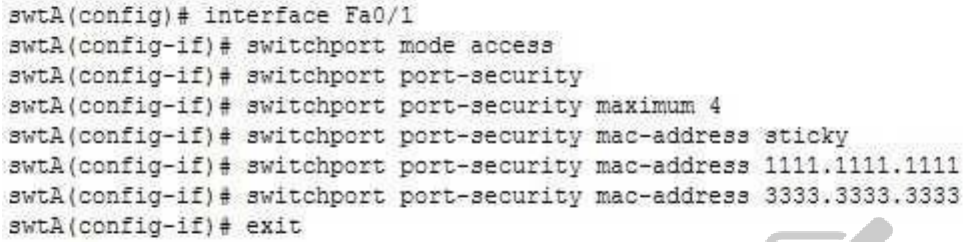
VTP user mode and private mode do not exist.

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)

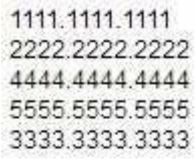
QUESTION 55

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:

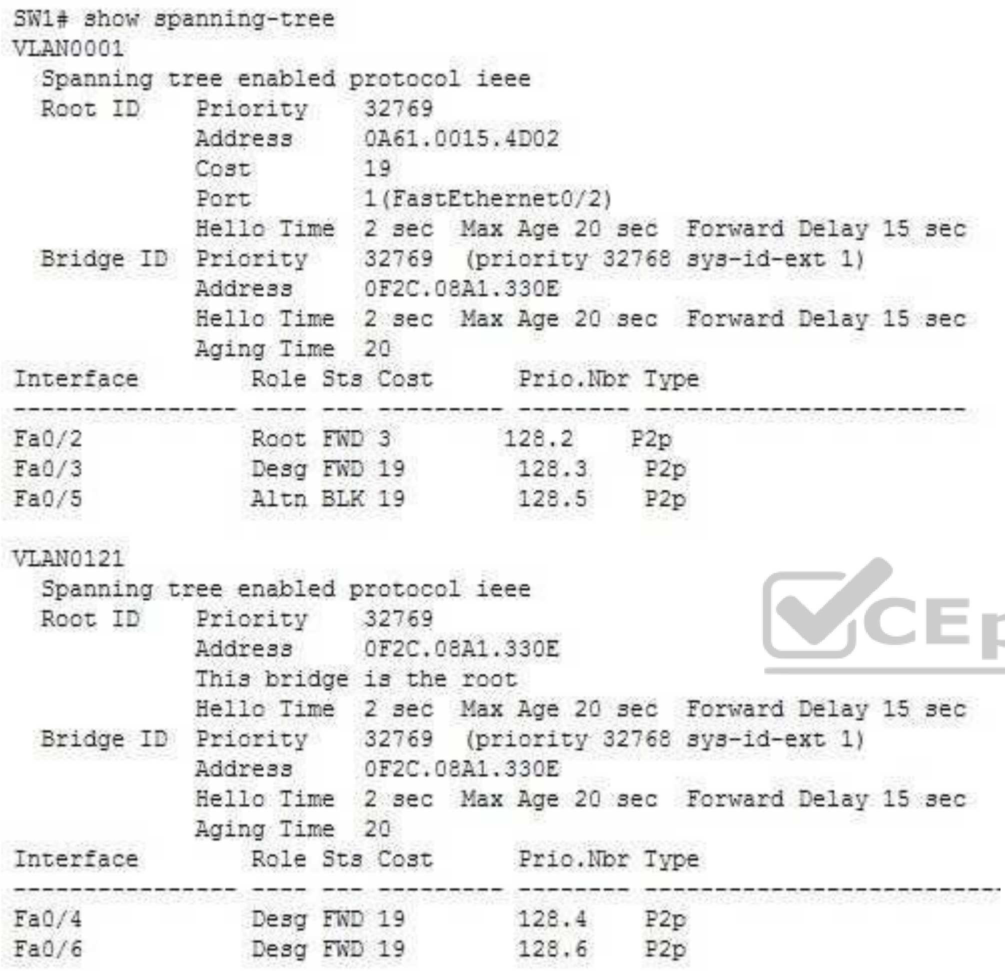
The MAC address 5555.5555.5555 caused the Fa0/1 port to shut down because it violates the port security enabled on the port. The switchport port-security maximum 4 command allows at most four MAC addresses or hosts to be connected to the Fa0/1 switch port. Two secure MAC addresses, 1111.1111.1111 and 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 56
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

QUESTION 57
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 58
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 59
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 60

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.

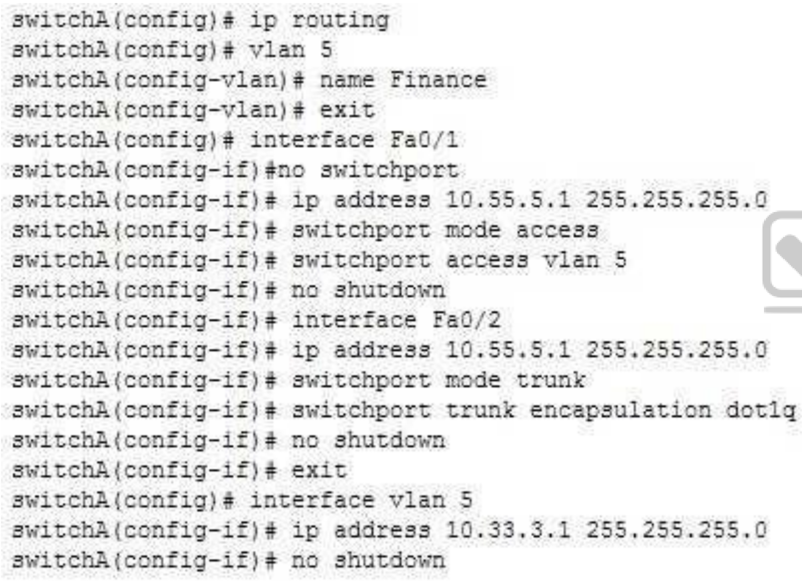
Untagged frames are not tagged with the tag of the native VLAN. They are simply forwarded to that VLAN. No packets in the native VLAN have tags.

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 61
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 62
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 63
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 64
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 65
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 66
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

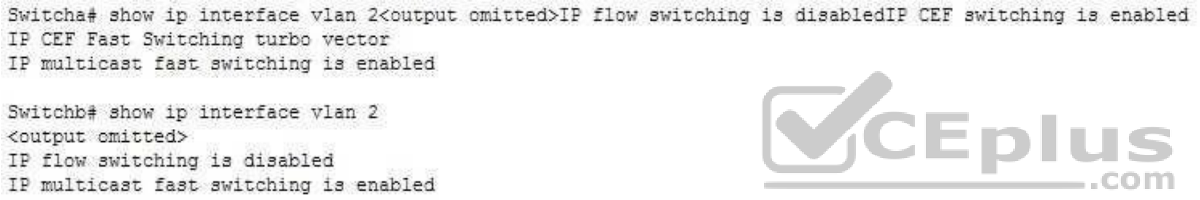
Section: (none)
Explanation

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 enabled
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 67
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.

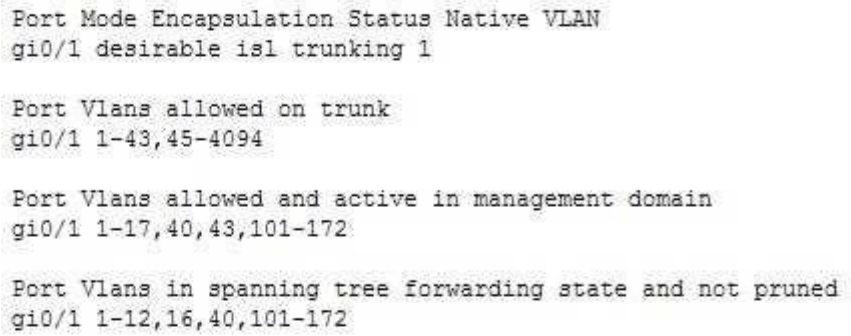
Marking is the process of setting the CoS, IP precedence, or DSCP of a packet to a specific value that will provide appropriate QoS throughout the network.

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 68
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 69
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 70

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 71

During which STP state can ports add information to their address tables, but not send any data?

A. Learning B.

Listening

C. Blocked

D. Forwarding

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

In the learning state, a switch port can add learned information into its address table, but cannot forward data.

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

- Blocking: In the blocking state, a port does not forward frames, learn information, or send out information. A forwarding port is placed in the blocked state when the port senses an absence of BPDUs, which are sent out in the interval defined by the hello time (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 root ports on the nonroot bridges, and the designated ports on each segment. Ports that remain as 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.

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 72
Which IOS command enables the VTP feature that eliminates unnecessary trunk traffic being flooded to switches that do not have memberships in particular VLANs?

A. vtp mode client
B. no vtp mode
C. vtp v1-mode
D. vtp pruning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

To enable pruning on a switch operating in VLAN Trunk Protocol (VTP) server mode, enter the vtp pruning command at the global configuration prompt.

```
switch(config)# vtp pruning
```

VTP pruning enhances network bandwidth usage by restricting unnecessary flooded traffic on trunk links. If a trunk link does not have devices in the VLAN attached, flooded traffic on that VLAN is blocked. VTP pruning can reduce broadcasts, multicasts, unknown traffic, and flooded unicast packets.

Enabling VTP pruning on a switch in VTP server mode enables pruning for the entire domain.

Multicast and unicast traffic are not blocked for the VLANs that are not being pruned.

There are three modes in VTP: server, client, and transparent. The main differentiator among the three modes is whether a switch can create, modify, or delete VLANs. A Catalyst switch can create, modify, and delete VLANs in server or transparent mode, but not in client mode. 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.

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

The 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. They only affect the local switch.

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.

The command vtp mode client sets the switch to client mode. It does not eliminate unnecessary trunk traffic.

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.

The vtp v1-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.

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 73
During a CEF packet rewrite, which of the following changes are NOT made to the packet?

A. The source MAC address is changed to the MAC address of the outbound Layer 3 switch interface.
B. The destination MAC address is changed to the MAC address of the next-hop router's MAC address.
C. Layer 3 TTL is decremented by one.
D. Layer 2 TTL is decremented by one.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

There is no Layer 2 TTL in the packet, so the Layer 2 time to live (TTL) cannot be decremented by one. All other options are correct. The following changes will be made when the Cisco Express Forwarding (CEF) packet rewrite process occurs:

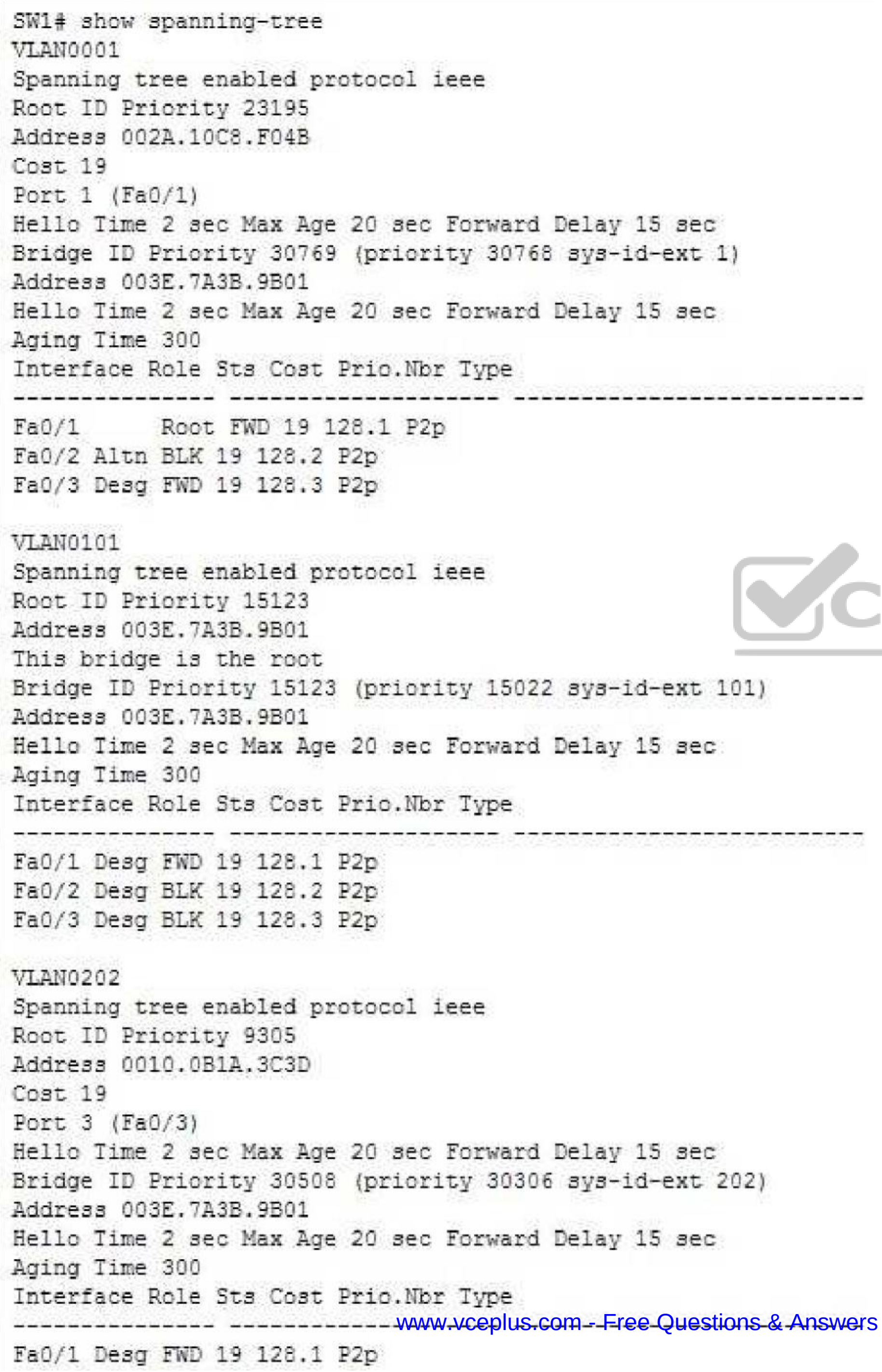
- The source MAC address is changed to the MAC address of the outbound Layer 3 switch interface.

- The destination MAC address is changed to the MAC address of the next hop routers MAC address
- The Layer 3 IP TTL is decremented by one
- The Layer 3 IP checksum is recalculated
- The Layer 2 frame checksum is recalculated

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

References:
Cisco > Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.1E > Configuring IP Unicast Layer 3 Switching on Supervisor Engine 2 > Understanding How IP Multicast Layer 3 Switching Works

QUESTION 74
Consider the following output of the show spanning-tree command for the SW1 switch:



```
SW1# show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 23195
Address 002A.10C8.F04B
Cost 19
Port 1 (Fa0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 30769 (priority 30768 sys-id-ext 1)
Address 003E.7A3B.9B01
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
Interface Role Sts Cost Prio.Nbr Type
--------------- -------------------- --------------------------
Fa0/1      Root FWD 19 128.1 P2p
Fa0/2 Altn BLK 19 128.2 P2p
Fa0/3 Desg FWD 19 128.3 P2p

VLAN0101
Spanning tree enabled protocol ieee
Root ID Priority 15123
Address 003E.7A3B.9B01
This bridge is the root
Bridge ID Priority 15123 (priority 15022 sys-id-ext 101)
Address 003E.7A3B.9B01
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
Interface Role Sts Cost Prio.Nbr Type
--------------- -------------------- --------------------------
Fa0/1 Desg FWD 19 128.1 P2p
Fa0/2 Desg BLK 19 128.2 P2p
Fa0/3 Desg BLK 19 128.3 P2p

VLAN0202
Spanning tree enabled protocol ieee
Root ID Priority 9305
Address 0010.0B1A.3C3D
Cost 19
Port 3 (Fa0/3)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 30508 (priority 30306 sys-id-ext 202)
Address 003E.7A3B.9B01
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
Interface Role Sts Cost Prio.Nbr Type
--------------- -------------------- --------------------------
Fa0/1 Desg FWD 19 128.1 P2p
```

You need to change the spanning-tree configuration such that the following is true:

- SW1 is the root bridge for VLAN0001
- SW1 is not the root bridge for VLAN0101
- Fa0/2 port of SW1 should be in the forwarding state for VLAN0202 traffic

Which of the following commands should be executed on SW1 to achieve the desired results? (Choose all that apply.)

A. spanning-tree vlan 1 priority 23189 in global configuration mode
B. spanning-tree vlan 1 priority 32768 in global configuration mode
C. spanning-tree vlan 101 priority 32768 in global configuration mode
D. spanning-tree vlan 202 cost 2 in interface configuration mode of Fa0/2
E. spanning-tree vlan 202 cost 252 in interface configuration mode of Fa0/2

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following commands should be executed to achieve the desired results:

spanning-tree vlan 1 priority 23189 in global configuration mode spanning-tree vlan 101 priority 32768 in global configuration mode spanning-tree vlan 202 cost 2 in interface configuration mode on Fa0/2

The spanning-tree vlan 1 priority 23189 command changes the bridge priority of SW1 to 23189 for the native VLAN (VLAN0001). According to the show spanningtree output in the scenario, the root bridge for VLAN0001 has a priority of 23195. Therefore, if SW1 has to become the root bridge for VLAN0001, then SW1 should have the least bridge priority for that VLAN. Setting the bridge priority of SW1 to 23189, which is less than 23195, serves the purpose.

The spanning-tree vlan 101 priority 32768 command changes the bridge priority of SW1 to 32768 for VLAN0101. The maximum priority that can be assigned to a switch is 32768, which implies that the switch cannot be a root bridge for the VLAN provided its MAC address is higher than the other switches. This will ensure that
SW1 will NOT be the root bridge for VLAN 101

The spanning-tree vlan 202 cost 2 command sets the port cost to 2 for VLAN0202. The port cost is used by STP to determine a loop-free path. The port with the least cost is selected and placed in Forwarding state. Therefore, as a result of this command, the Fa0/2 port will be in the Forwarding state to pass the VLAN0202 traffic, rather than Fa0/1.

Executing the spanning-tree vlan 1 priority 32768 command in the global configuration mode does not achieve the desired results. This command sets the bridge priority of SW1 to the highest possible value for VLAN0001. As 32768 is greater than 23190, the new bridge priority of SW1 does not affect the root bridge for VLAN0001 and SW1 remains a non-root bridge.

The spanning-tree vlan 202 cost 252 command in the interface configuration mode of Fa0/2 does not achieve the desired results. This command changes the port cost of Fa0/2 for VLAN0202 to 252, which is the maximum cost value. STP selects the port with the least cost as the best loop-free path. Therefore, setting the cost to 252 for Fa0/2 will not put Fa0/2 in the Forwarding state.

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

References:
Cisco > Cisco IOS Bridging Command Reference > rif through spanning-tree portfast (interface mode)
Cisco > Technology Support > Lan Switching > Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches

QUESTION 75
What is the easiest way to force a specific switch to become the spanning-tree root bridge for a VLAN?

A. Raise the spanning-tree priority value on the switch.
B. Lower the spanning-tree priority value on the switch.
C. Raise the port-cost value of an interface on the switch.
D. Lower the port-cost value of an interface on the switch.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

The spanning-tree root bridge is the bridge with the lowest bridge ID. The bridge ID is a value calculated from the bridge priority and the bridge MAC address. Therefore, lowering the bridge-priority value lowers the bridge ID, which can force the switch to become the root bridge.

The easiest way to force a specific switch to become the spanning-tree root bridge for a VLAN is to lower its priority using the spanning-tree vlan vlan_id priority priority command. For example, the following command will configure the switch as the root bridge for VLAN 10:

```
switch(config)# spanning-tree vlan 10 priority 4096
```

The priority value of 4096 is used by convention. It could be set to any value as long as it is lower than any other switch in the VLAN. The priority value 4096 is typically used when forcing the placement of the root bridge, and 8192 is used to force placement of the secondary root bridge. These values work because the default priority value for switches is 32768.

Lowering the port cost of an interface is an effective way to force spanning tree to put the interface into a forwarding state. However, it does not affect the placement of the root bridge.

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 76
Which protocol is used to maintain the contents of the Cisco Express Forwarding (CEF) adjacency table?

A. ARP
B. RARP
C. PING
D. INARP

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

The CEF adjacency table is maintained as each adjacent node is discovered. Link header entries are created and stored in the adjacency table as the information is learned through the ARP protocol.

Cisco Express Forwarding (CEF) is a Layer 3 switching technology based on information contained in the Forwarding Information Base (FIB) and the adjacency table.

The FIB is conceptually equivalent to a routing table in that it contains information used in the packet forwarding decision. The adjacency table contains information about the adjacent route processors. The adjacency table contains the MAC information for the next-hop addresses for all FIB entries. A device is considered adjacent if it is reachable over a single Layer 2 connection. It is stored in DRAM.

The Layer 3 processor engine builds the FIB and adjacency tables in software. That information is distributed from the control-plane hardware to the data-plane hardware Application Specific Integrated Circuits (ASICs) at the port or line card. This enhances the Layer 3 forwarding operation by moving it from the softwarebased engine to the ASICs. Of course, there are exception packets that are still software-processed, such as non-conforming protocols and datalink encapsulations.

Reverse ARP (RARP) is used an obsolete networking protocol used by a host computer to obtain its Internet Protocol (IPv4) address when it has available its linklayer address, such as an Ethernet address. It has been replaced with DHCP. It is not used maintain the contents of the Cisco Express Forwarding (CEF) adjacency table

INverse ARP (INARP) is used by Frame relay connection to dynamically learn the DLCI associated with a connection. It is not used maintain the contents of the Cisco Express Forwarding (CEF) adjacency table

PING is a diagnostic tool used to test connectivity. It is not used maintain the contents of the Cisco Express Forwarding (CEF) adjacency table.

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

References:
Cisco >IP Switching Cisco Express Forwarding Configuration Guide, Cisco IOS Release 15 > CEF Overview > CEF Adjacency Tables Overview

QUESTION 77
Which IOS interface configuration command is required to configure a switch port to be a promiscuous PVLAN access port?

A. switchport mode promiscuous
B. switchport mode promiscuous-vlan
C. switchport mode private-vlan host
D. switchport mode private-vlan promiscuous

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A promiscuous port type can send frames to all other ports in the same private VLAN (PVLAN). The switchport mode private-vlan promiscuous command configures a port to be a promiscuous port. The syntax is as follows:

switch(config-if)# switchport mode private-vlan promiscuous

There are three types of ports in a private VLAN (PVLAN): promiscuous, isolated, and community. A promiscuous port can send and receive frames with other promiscuous, isolated, or community ports assigned to the same private VLAN. Isolated ports are able to send frames to promiscuous ports, but not to each other. A community port can communicate with other community ports of the same private VLAN or with promiscuous ports.

Private VLANs are supported on switches that allow the configuration of primary and secondary VLANs. A primary VLAN carries the traffic between the promiscuous port and the isolated and community ports assigned to the same primary VLAN. There are two types of secondaryVLANs, isolated and community. Isolated VLANs carry traffic from isolated ports to promiscuous ports. Community VLANs carry traffic between community ports and to the promiscuous

port. Therefore, on a promiscuous port, you would use the following command syntax to configure its primary and secondary VLANs: switch(config-if)#

private-vlan mapping primary_vlan_id secondary_vlan_id PVLANs are created using the following special VLAN configuration commands:

switch(config)# vlan vlan_id switch(config-vlan)# private-vlan
[primary | isolated | community] switch(config-vlan)# private-vlan
association secondary_vlan_list

Host ports are defined using the following special PVLAN configuration command:

switch(config-if)# switchport mode private-vlan host

The command used for isolated and community ports is as follows:

switch(config-if)# switchport mode private-vlan host-association primary_vlan_id secondary_vlan_id

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 Interface and Hardware Component Command Reference > switchport mode

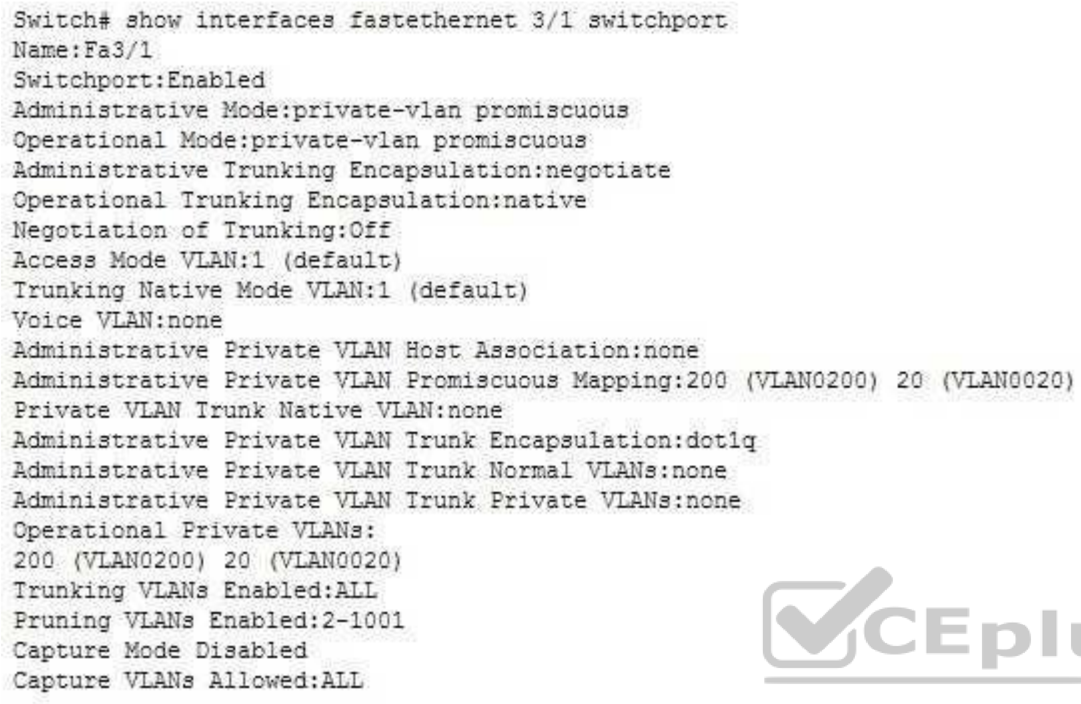
QUESTION 78
What command should be used to view the private VLANs configured on ports and the private VLAN mappings?

A. show vlan brief
B. show pvlan
C. show interfaces switchport
D. show mac-address-table

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command show interfaces switchport is used to verify private VLANs configured on ports and the private VLAN mappings. The following is a sample of the output:



```
Switch# show interfaces fastethernet 3/1 switchport
Name:Fa3/1
Switchport:Enabled
Administrative Mode:private-vlan promiscuous
Operational Mode:private-vlan promiscuous
Administrative Trunking Encapsulation:negotiate
Operational Trunking Encapsulation:native
Negotiation of Trunking:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Voice VLAN:none
Administrative Private VLAN Host Association:none
Administrative Private VLAN Promiscuous Mapping:200 (VLAN0200) 20 (VLAN0020)
Private VLAN Trunk Native VLAN:none
Administrative Private VLAN Trunk Encapsulation:dot1q
Administrative Private VLAN Trunk Normal VLANs:none
Administrative Private VLAN Trunk Private VLANs:none
Operational Private VLANs:
200 (VLAN0200) 20 (VLAN0020)
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001
Capture Mode Disabled
Capture VLANs Allowed:ALL
```

This output reveals that Fa3/1 is a promiscuous port in private VLAN (PVLAN) 20. PVLAN 20 is a member of the primary VLAN 200. Since this is a promiscuous port, it is able to exchange information with all other PVLANs associated with VLAN 200.

The show vlan brief command is only used to view the VLANs that exist and the ports that are members of them. No information about PVLANs and member association is included.

The show mac-address-table command is used to view the MAC addresses stored in the switches memory and the port and VLAN they are members of. No information about PVLANs is included in this output.

The command show pvlan is incorrect due to invalid syntax.

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

References:

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

QUESTION 79
What is accomplished by the command switchport port-security violation protect?

A. The switch will generate a log message but will not block any packets
B. The switch will drop packets that are in violation and generate a log message
C. The switch will drop packets that are in violation, but not generate a log message
D. The switch will shut down the interface when packets in violation are detected

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command switchport port-security port violation protect will cause the switch to drop packets that are in violation, but does not generate a log message.

The complete syntax of the command is: switch(config-if)# switchport port-security violation protect

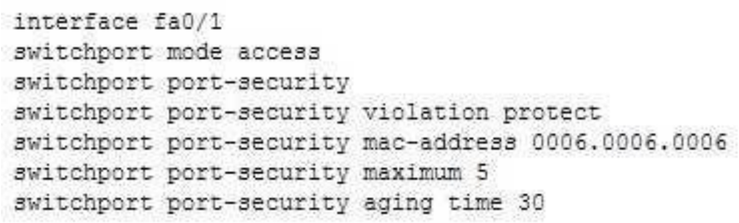
The port-security command is used to lock a port to a specific MAC addresses. Port security can be used to limit access to a port by MACaddress. It can be applied to:
▪ access ports ▪ VoIP ports ▪ ports where multiple MAC addresses are expected, such as a port connecting to a hub

It cannot be applied to trunk ports or to ports that are part of an Etherchannel.

Three keywords can be used with this command: protect, restrict and shutdown. The restrict keyword tells the port to drop packets and generate a log message for packets that are in violation. The protect keyword tells the port to drop packets without generating a log message for packets that are in violation. The shutdown keyword causes the port to be place into the errdisable state if a violation is detected.

The following configuration, generated from a partial output of the show run command, would apply port security to the Fa0/1 interface. It would allow five addresses to access the interface at time. This count includes addresses that have been seen by the port but are currently inactive. Therefore, if five addresses have been seen and three are inactive, then a sixth address would not be allowed. If the port security maximum command has not been issued, the default behavior will only allow one address on the port.

The aging command can be used to force inactive addresses to be dropped from the list of addresses seen, thereby allowing active addresses access to the port.



```
interface fa0/1
switchport mode access
switchport port-security
switchport port-security violation protect
switchport port-security mac-address 0006.0006.0006
switchport port-security maximum 5
switchport port-security aging time 30
```

The above configuration also includes a static entry for the MAC address 0006.0006.0006. This means that this address is always in the list, and so in effect, this configuration leaves only four other dynamic MAC addresses that can connect at a time.

There is no option to generate a log message but not block any packets.

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

References:
Cisco > Catalyst 6500 Release 15.0SY Software Configuration Guide > Security > Port Security > How to Configure Port Security

QUESTION 80
Which PVLAN port types can send frames through a switch to community and promiscuous ports? (Choose two.)

A. public
B. private
C. isolated
D. community
E. promiscuous

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Community ports and promiscuous ports can send frames to other community ports and promiscuous ports in the same private VLAN.

There are three types of ports in a private VLAN (PVLAN): promiscuous, isolated, and community. A PVLAN community port (a port in the same VLAN) and promiscuous ports (a port that can forward to all interfaces, including the isolated and community ports within a PVLAN) can send traffic to other community or promiscuous ports.

Isolated ports are able to send frames to promiscuous ports, but not to other isolated ports.

A community port can communicate with other community ports in the same privateVLAN or with promiscuous ports.

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

QUESTION 81
What attack technique uses double VLAN tagging to access network devices that might not otherwise be accessible?

A. VLAN hopping
B. DHCP spoofing
C. Rogue devices
D. MAC flooding

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Double VLAN tagging is used by a VLAN hopping attack. An attacker can create a packet with two VLAN headers on it 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. This becomes a security concern because this hopping can be accomplished without passing through a router and its security access lists. For this reason, private VLANs and VACLs should be used to secure access between VLANs.

DHCP spoofing is an attack that can be used to force user traffic through an attacking device. This is accomplished by an attacker responding to DHCP queries from users. Eliminating the response from the correct DHCP server would make this more effective, but if the attacker's response gets to the client first, the client will accept it. The DHCP response from the attacker will include a different gateway or DNS server address. If they define a different gateway, the user traffic will be forced to travel through a device controlled by the attacker. This will allow the attacker to capture traffic and gain company information. If the attacker changes the DNS server in the response, they can use their own DNS server to force traffic to selected hosts to go to a device they control. Again, this would allow the attacker to capture traffic and gain information.

MAC flooding is an attack technique that attempts to fill a switch's MAC address table so the attacker can capture flooded traffic sent from the switch. The concept of this attack is to use the CAM table limit to the attacker's advantage. The attacker would send packets addressed from a large number of MAC addresses to the switch. The switch adds the source MAC address to the MAC address table. 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.

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

References:
Cisco > Products and Services > Switches > Cisco Catalyst 6500 Series Switches > Product Literature > White Papers > Cisco Catalyst 6500 Series Switches > VLAN Security White Paper > Double-Encapsulated 802.1Q/Nested VLAN Attack

QUESTION 82
What Cisco switch features are designed to work together to mitigate ARP spoofing attacks? (Choose two.)

A. DHCP snooping
B. port security
C. 802.1x
D. DAI

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Dynamic ARP inspection (DAI) and DHCP snooping are Cisco features designed to work together to mitigate ARP spoofing attacks. DAI validates ARP packets in a network. DAI determines the validity of an ARP packet based on the valid MAC address-to-IP-address bindings stored in the DHCP snooping database. This capability protects the network from some man-in-the-middle attacks. The following global configuration command instructs the switch to intercept, log, and discard packets with invalid IP-to-MAC address bindings for the specified VLANs.

```
switch(config)# ip arp inspection vlan 10-12,15
```

When configuring DAI, ports are configured as either trusted or untrusted. DAI forwards all packets received on a trusted interface without checks but intercepts all packets on an untrusted port.

DHCP snooping creates an IP address to MAC address database that DAI uses to validate ARP packets. It compares the MAC address and IP address in ARP packets and only permits the traffic if the addresses match. This eliminates attackers spoofing MAC addresses. The following command enables DHCP MAC address verification:

```
router(config)# ip dhcp snooping verify mac-address
```

DHCP Authorized ARP can also be used to mitigate ARP spoofing. When implemented, the server assigns an IP address to a client and then creates a static mapping. The DHCP server then sends periodic ARPs to clients to make sure that the clients are still active. Clients respond with an ARP reply. Unauthorized clients cannot respond to these periodic ARPs. The unauthorized ARP responses are blocked at the DHCP server.

DHCP snooping also is used to define ports as trusted for DHCP server connections. The purpose of DHCP snooping is to mitigate DHCP spoofing attacks. DHCP snooping can be used to determine what ports are able to send DHCP server packets such as DHCPOFFER, DHCPACK, and DHCPNAK. DHCP snooping can also cache the MAC address to IP address mapping for clients receiving DHCP addresses from a valid DHCP server.

Port security is a method of only permitting specified MAC addresses access to a switch port. This can be used to define what computer or device can be connected to a port, but not eliminate ARP spoofing.

802.1x is a method of determining authentication before permitting access to a switch port. This is useful in restricting who can connect to the switch; it does not inspect ARP packets.

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

References:
Catalyst 6500 Release 12.2SXF and Rebuilds Software Configuration Guide > Configuring Dynamic ARP Inspection (DAI)
Cisco > Cisco IOS IP Addressing Services Command Reference > ARP Commands > ip arp inspection vlan

QUESTION 83
What command would be used to verify trusted DHCP ports?

A. show mls qos
B. show ip dhcp snooping
C. show ip trust

D. show ip arp trust

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command show ip dhcp snooping is used to verify trusted DHCP ports. This command is used to verify which ports are intended to have DHCP servers connected to them. DHCP snooping creates an IP address to MAC address database that Dynamic ARP Inspection (DAI) uses to validate ARP packets. It compares the MAC address and IP address in ARP packets and only permits the traffic if the addresses match. This eliminates attackers that are spoofing MAC addresses.

DHCP snooping is used to define ports as trusted for DHCP server connections. The purpose of DHCP snooping is to mitigate DHCP spoofing attacks. DHCP snooping can be used to determine what ports are able to send DHCP server packets, such as DHCPOFFER, DHCPACK, and DHCPNAK. DHCP snooping can also cache the MAC address to IP address mapping for clients receiving DHCP addresses from a valid DHCP server.

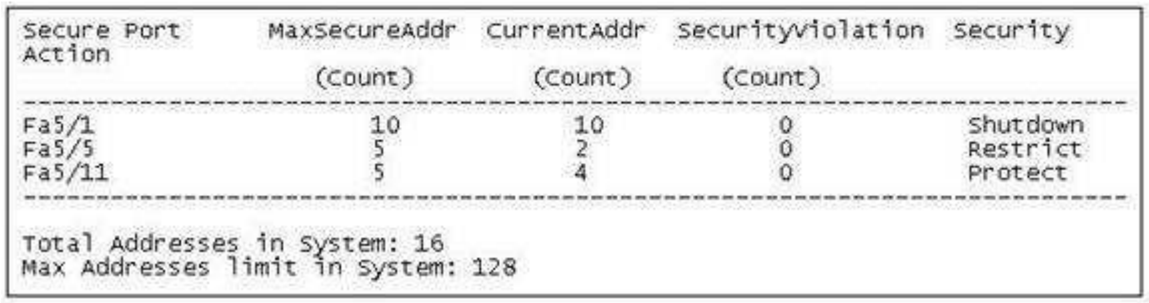
MLS QOS has no bearing on DHCP services, so show mls qos is not correct.

The other commands are incorrect because of invalid syntax.

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

References:
Cisco > Cisco IOS IP Addressing Services Command Reference > DHCP Commands > show ip dhcp snooping

QUESTION 84
What command produces the output in the exhibit?



```
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
                    (Count)        (Count)        (Count)
---------------------------------------------------------------------------
Fa5/1                 10             10             0              Shutdown
Fa5/5                  5              2             0              Restrict
Fa5/11                 5              4             0              Protect
---------------------------------------------------------------------------

Total Addresses in System: 16
Max Addresses limit in System: 128
```

A. show port-security interface
B. show vlan private-vlan type
C. show port-security
D. show ip dhcp snooping

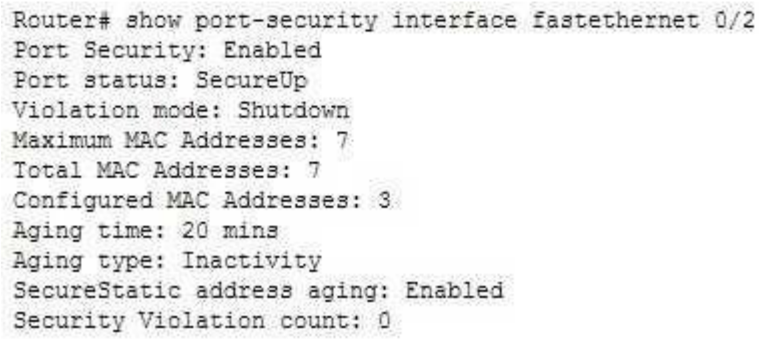
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The exhibit displays the output of the show port-security command. This command is useful in verifying the reaction set for packets in violation. In the exhibit, Fa5/1 is configured to shut down if a violating packet is received. Port Fa5/5 is configured to drop violating packets and port Fa5/11 is configured to drop packets and generate a log message.

The output also indicates the number of secure MAC addresses permitted on each interface, the number of secure MAC addresses currently in use on the port, and how many security violations there have been.

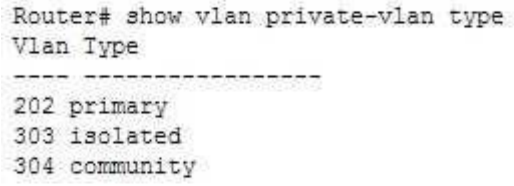
The show port-security interface command shows the port security configuration on the specified interface. Below is an example of the command and its output:



```
Router# show port-security interface fastethernet 0/2
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 7
Total MAC Addresses: 7
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

In the example, seven MAC addresses are allowed on this interface. It can be seen that seven are now connected. Therefore, if one more user connects to the hub or switch connected to this port, the port will be placed into the err-disabled state and an SMTP trap message will be sent.

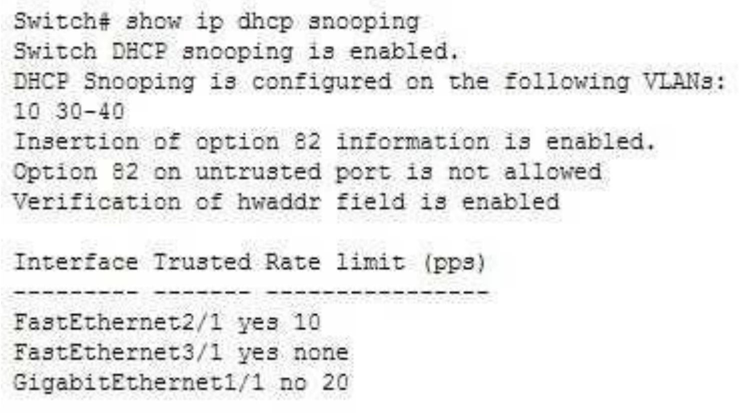
The show vlan private-vlan type command displays the private VLANs on the switch and indicates whether they are primary, isolated, or community VLANs. An example of the output is below:



```
Router# show vlan private-vlan type
Vlan Type
---- -----------------
202 primary
303 isolated
304 community
```

In the output, VLAN 202 carries traffic from promiscuous ports to isolated, community, and other promiscuous ports in the same VLAN. VLAN 303 carries traffic from isolated ports to a promiscuous port.

The show ip dhcp snooping command displays whether DHCP snooping is enabled, what VLANs it is configured for, and what ports are trusted DHCP ports. An example of the output is below:



```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled.
DHCP Snooping is configured on the following VLANs:
10 30-40
Insertion of option 82 information is enabled.
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled

Interface Trusted Rate limit (pps)
--------- ------- ----------------
FastEthernet2/1 yes 10
FastEthernet3/1 yes none
GigabitEthernet1/1 no 20
```

The output indicates that:
▪ The switch is defending against a DHCP spoofing attack (indicated by lines 2 and 3) ▪
Two ports are trusted and one is not (shown in bottom table)
▪ Option 82 (relay agent information) is only allowed on trusted ports (indicated by lines 4 and 5) ▪
ARP spoofing is being monitored (indicated by line 6)

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

References:
Cisco > Support > show multicast protocols status through show rif > show port-security

QUESTION 85
What Cisco Catalyst switch feature is designed to inspect ARP packets and mitigate ARP spoofing attacks?

A. DHCP snooping
B. port security
C. 802.1x
D. DAI

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

ARP spoofing attacks are attempts to redirect traffic to an attacking host by sending an ARP message with a forged identity to a transmitting host. Dynamic ARP inspection (DAI) is a Cisco feature designed to inspect ARP packets and mitigate spoofing attacks. It works in combination with DHCP snooping. DHCP snooping creates an IP address to MAC address database that DAI uses to validate ARP packets. It compares the MAC address and IP address in ARP packets and only permits the traffic if the addresses match. This eliminates attackers from spoofing MAC addresses. Characteristics of DAI include:

- DAI can only be performed on ingress ports
- DAI is supported on access ports, trunk ports, Etherchannel ports, and private VLAN ports
- DAI should be configured on all access switch ports as untrusted, and on all switch ports connected to other switches as trusted

An interface can be configured as trusted by using the ip arp inspection trust command. Consider the configuration shown below. If an ARP spoof attack arrives on interface Fa0/2, it will not be inspected because the port is set as trusted, and the spoof packets will be allowed.

```
<output omitted> ip arp
inspection vlan 5
interface fastethernet
0/2 switchport mode
trunk
swtchport trunk encapsulation dot1q
ip arp inspection trust
```

DHCP snooping is used to define ports as trusted for DHCP server connections. The purpose of DHCP snooping is to mitigate DHCP spoofing attacks. DHCP snooping can be used to determine what ports are able to send DHCP server packets, such as DHCPOFFER, DHCPACK, and DHCPNAK. DHCP snooping can also cache the MAC address to IP address mapping for clients receiving DHCP addresses from a valid DHCP server.

Port security is a method of only permitting specified MAC addresses access to a switch port. This can be used to define what computer or device can be connected to a port, but not eliminate ARP spoofing.

802.1x is a method of determining authentication before permitting access to a switch port. This is useful in restricting who can connect to the switch; it does not inspect ARP packets.

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

References:
Catalyst 6500 Release 12.2SXF and Rebuilds Software Configuration Guide > Configuring Dynamic ARP Inspection (DAI)

QUESTION 86
What is accomplished by the command switchport port-security violation restrict?

A. The switch will generate a log message but will not block any packets.
B. The switch will drop packets that are in violation and generate a log message.
C. The switch will drop packets that are in violation, but not generate a log message.
D. The switch will shut down the interface when packets in violation are detected.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command switchport port-security violation restrict drops packets that are in violation and generates a log message. The complete syntax of the command is:

```
switch(config-if)# switchport port-security violation restrict
```

The port security command is used to lock a port down to specific MAC addresses. The three keywords that can be used with this command are protect, restrict, and shutdown. The protect keyword tells the port to drop packets without generating a log message for packets that are in violation. The restrict keyword tells the port to drop packets and generates a log message for packets that are in violation. The shutdown keyword causes the port to be disabled if a violation is detected.

There is no option to generate a log message but not block any packets.

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

References:
Cisco > Catalyst 6500 Release 15.0SY Software Configuration Guide > Security > Port Security > How to Configure Port Security