

Cisco 642-813



Implementing Cisco IP Switched Networks (SWITCH)

Version: 17.0

Topic 1, Implement VLAN based solution, given a network design and a set of requirements

QUESTION NO: 1

Which statement is true about RSTP topology changes?

- A.** Any change in the state of the port generates a TC BPDU.
- B.** Only non-edge ports moving to the forwarding state generate a TC BPDU.
- C.** If either an edge port or a non-edge port moves to a block state, then a TC BPDU is generated.
- D.** Only edge ports moving to the blocking state generate a TC BPDU.
- E.** Any loss of connectivity generates a TC BPDU.

Answer: B

Explanation:

The IEEE 802.1D Spanning Tree Protocol was designed to keep a switched or bridged network loop free, with adjustments made to the network topology dynamically. A topology change typically takes 30 seconds, where a port moves from the Blocking state to the Forwarding state after two intervals of the Forward Delay timer. As technology has improved, 30 seconds has become an unbearable length of time to wait for a production network to failover or "heal" itself during a problem.

Topology Changes and RSTP

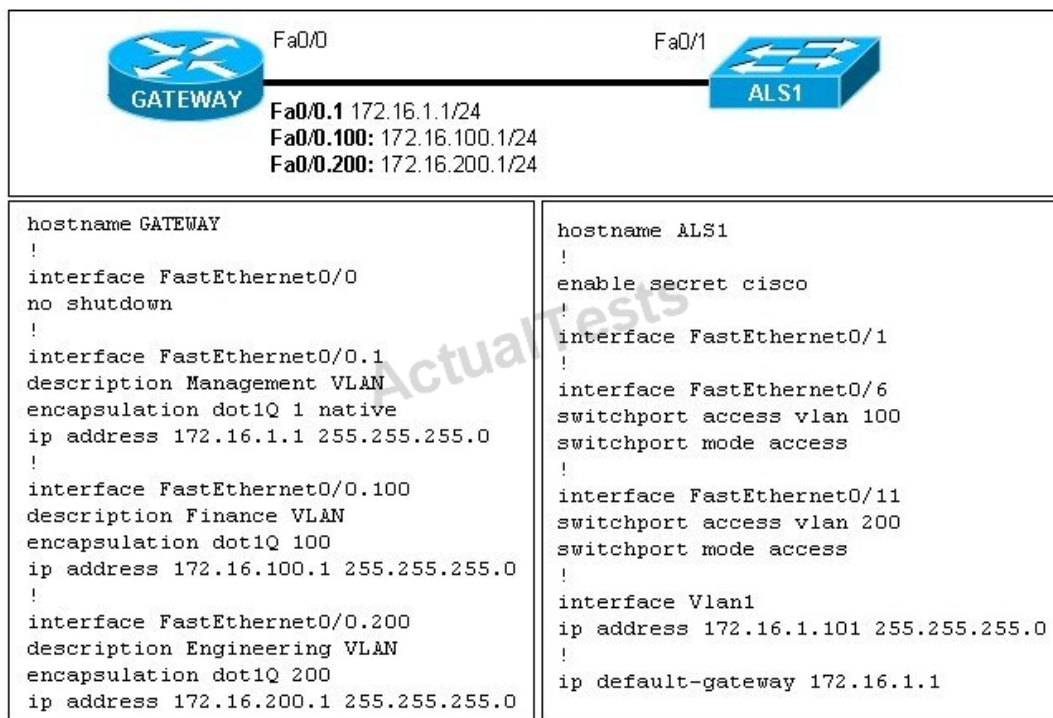
Recall that when an 802.1D switch detects a port state change (either up or down), it signals the Root Bridge by sending topology change notification (TCN) BPDUs. The Root Bridge must then signal a topology change by sending out a TCN message that is relayed to all switches in the STP domain. RSTP detects a topology change only when a non-edge port transitions to the Forwarding state. This might seem odd because a link failure is not used as a trigger. RSTP uses all of its rapid convergence mechanisms to prevent bridging loops from forming. Therefore, topology changes are detected only so that bridging tables can be updated and corrected as hosts appear first on a failed port and then on a different functioning port. When a topology change is detected, a switch must propagate news of the change to other switches in the network so they can correct their bridging tables, too. This process is similar to the convergence and synchronization mechanism-topology change (TC) messages propagate through the network in an ever-expanding wave.

Reference:

CCNP BCMSN Official Exam Certification Guide, Fourth Edition, Chapter 11: Advanced Spanning Tree Protocol, Rapid Spanning Tree Protocol, Topology Changes and RSTP, p. 269

QUESTION NO: 2

Refer to the exhibit.



Why are users from VLAN 100 unable to ping users on VLAN 200?

- A. Encapsulation on the switch is wrong.
- B. Trunking must be enabled on Fa0/1.
- C. The native VLAN is wrong.
- D. VLAN 1 needs the no shutdown command.
- E. IP routing must be enabled on the switch.

Answer: B

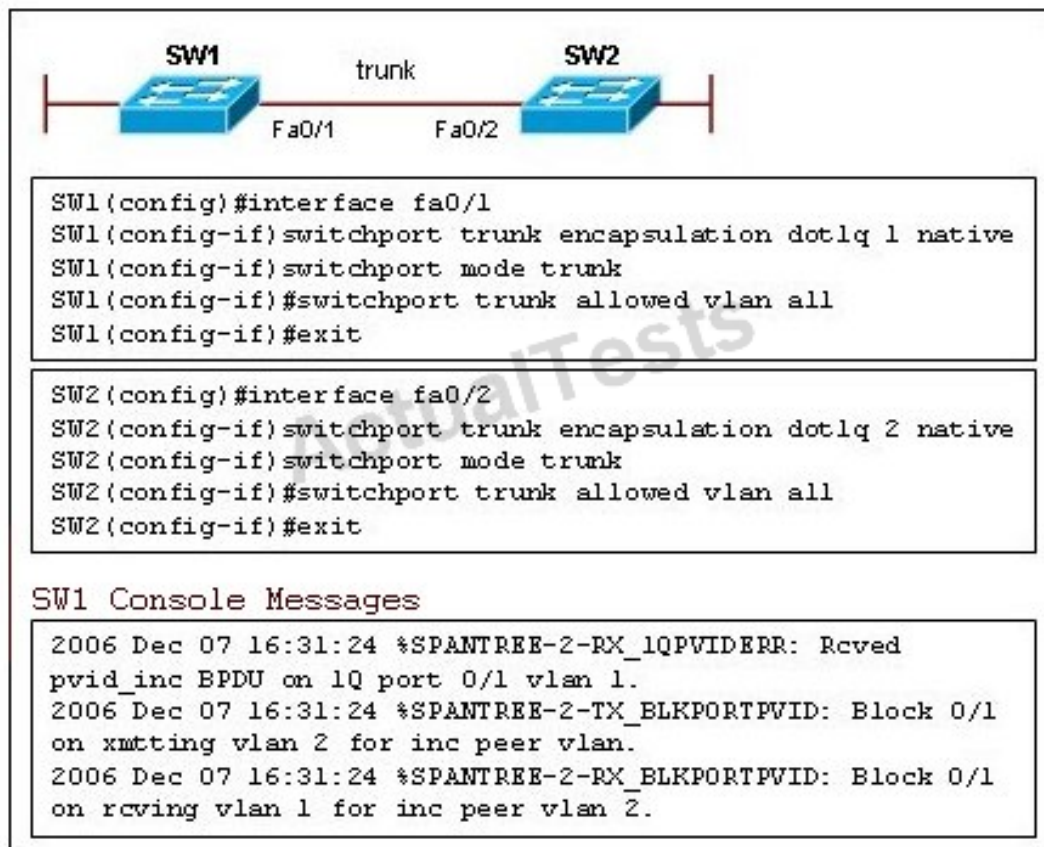
Explanation:

Switch supports multiple VLAN but have no Layer3 capability to route packets between those VLANs, the switch must be connected to router external to the switch. This setup is most efficiently accomplished by providing a single trunk link between the switch and the router that can carry the traffic of multiple VLANs, which can in turn be routed by the router. For that trunk require between Router & Switch. So trunking need to be enable on Fa0/1.

http://www.cisco.com/en/US/tech/tk389/tk815/tk857/tsd_technology_support_sub-protocol_home.html

QUESTION NO: 3

Refer to the exhibit.



The link between switch SW1 and switch SW2 is configured as a trunk, but the trunk failed to establish connectivity between the switches. Based on the configurations and the error messages received on the console of SW1, what is the cause of the problem?

- A. The two ends of the trunk have different duplex settings.
- B. The two ends of the trunk have different EtherChannel configurations.
- C. The two ends of the trunk have different native VLAN configurations.
- D. The two ends of the trunk allow different VLANs on the trunk.

Answer: C

Explanation:

The native VLAN, if not explicitly configured, will default to the default VLAN, (VLAN1). The Native VLAN is configured for an 802.1Q Trunk port. 802.1Q trunks carry traffic from multiple VLANs by tagging the traffic with VLAN identifiers (Tagged Traffic) which identifies which packets are associated with which VLANs, and they can also carry non VLAN traffic from legacy switches or non 802.1Q compliant switches (Untagged Traffic). The switch will place untagged traffic on the

Native VLAN by using a PVID identifier. Native VLAN traffic is not tagged by the switch. It is a best practice to configure the Native VLAN to be different than VLAN1 and to configure it on both ends of the trunk.

QUESTION NO: 4

When you create a network implementation for a VLAN solution, what is one procedure that you should include in your plan?

- A. Perform an incremental implementation of components.
- B. Implement the entire solution and then test end-to-end to make sure that it is performing as designed.
- C. Implement trunking of all VLANs to ensure that traffic is crossing the network as needed before performing any pruning of VLANs.
- D. Test the solution on the production network in off hours.

Answer: A

Explanation:

Cisco recommendations for implementation plan have the following items:

- Some examples of organizational objectives when developing a VLAN implementation plan could include: improving customer support, increasing competitiveness, and reducing costs.
- When creating a VLAN implementation plan, it is critical to have a summary implementation plan that lays out the implementation overview.
- Incremental implementation of components is the recommended approach when defining a VLAN implementation plan.

Reference:

<http://www.ccnpguide.com/design-documentation/>

QUESTION NO: 5

You have just created a new VLAN on your network. What is one step that you should include in your VLAN-based implementation and verification plan?

- A. Verify that different native VLANs exist between two switches for security purposes.
- B. Verify that the VLAN was added on all switches with the use of the show vlan command.
- C. Verify that the switch is configured to allow for trunking on the switch ports.

D. Verify that each switch port has the correct IP address space assigned to it for the new VLAN.

Answer: B

Explanation:

As part of verification plan you have to verify that the VLAN was added on all switches. The command show vlan can be used for this purpose.

Reference:

<http://www.ccnpguide.com/design-documentation/>

QUESTION NO: 6

Which two statements describe a routed switch port on a multilayer switch? (Choose two.)

- A.** Layer 2 switching and Layer 3 routing are mutually supported.
- B.** The port is not associated with any VLAN.
- C.** The routed switch port supports VLAN subinterfaces.
- D.** The routed switch port is used when a switch has only one port per VLAN or subnet.
- E.** The routed switch port ensures that STP remains in the forwarding state.

Answer: B,D

Explanation:

A routed port is a physical port that acts like a port on a router; it does not have to be connected to a router. A routed port is not associated with a particular VLAN, as is an access port. A routed port behaves like a regular router interface, except that it does not support VLAN subinterfaces.

Routed ports can be configured with a Layer 3 routing protocol. A routed port is a Layer 3 interface only and does not support Layer 2 protocols, such as DTP and STP. You can configure routed ports by putting the interface into Layer 3 mode with the no switchport interface configuration command. Then you have to assign an IP address to the port, enable routing, and assign routing protocol characteristics by using the ip routing and router protocol global configuration commands.

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.1_19_ea1/configuration/guide/swint.html#wp1288561

QUESTION NO: 7

On a multilayer Cisco Catalyst switch, which interface command is used to convert a Layer 3 interface to a Layer 2 interface?

- A. switchport
- B. no switchport
- C. switchport mode access
- D. switchport access vlan vlan-id

Answer: A

Explanation:

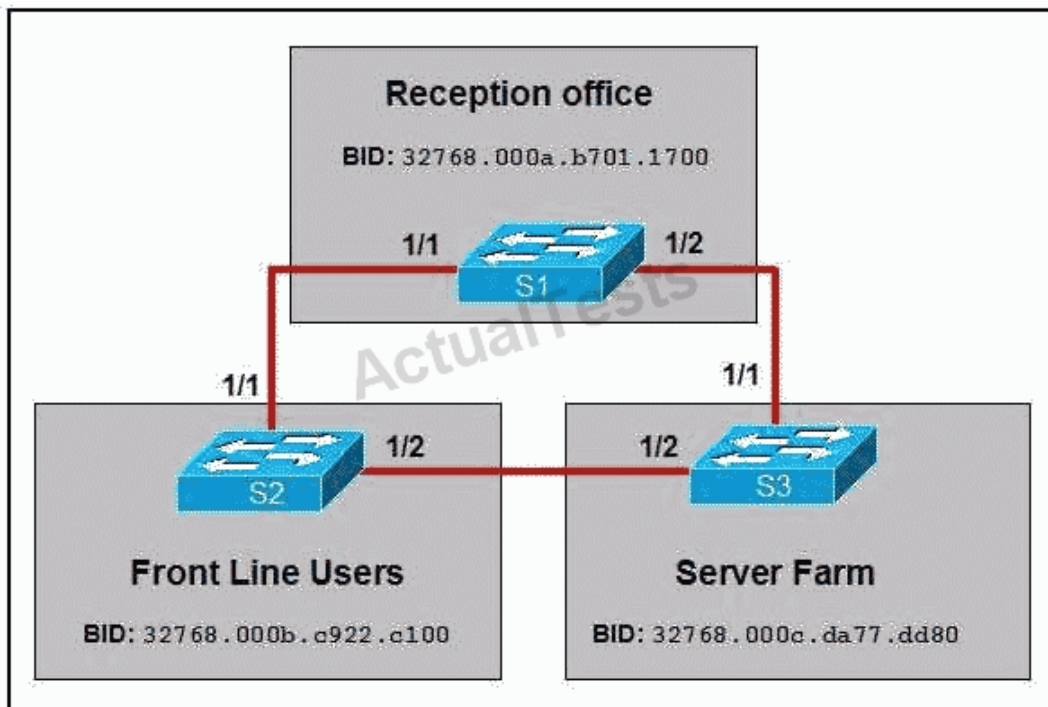
The switchport command puts the port in Layer 2 mode. Then, you can use other switchport command keywords to configure trunking, access VLANs, and so on.

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_25_se/configuration/guide/swint.html#wp1415008

QUESTION NO: 8

Refer to the exhibit.



All network links are FastEthernet. Although there is complete connectivity throughout the network,

Front Line users report that they experience slower network performance when accessing the server farm than the Reception office experiences. Which two statements are true? (Choose two.)

- A. Changing the bridge priority of S1 to 4096 would improve network performance.
- B. Changing the bridge priority of S1 to 36864 would improve network performance.
- C. Changing the bridge priority of S2 to 36864 would improve network performance.
- D. Changing the bridge priority of S3 to 4096 would improve network performance.
- E. Disabling the Spanning Tree Protocol would improve network performance.
- F. Upgrading the link between S2 and S3 to Gigabit Ethernet would improve performance.

Answer: B,D

Explanation:

As the switch S1 has the better bridge priority it is selected as root bridge. As the consequence of this the link between S2 and S3 is disabled and traffic from Front Line Users to Server Farm goes through the root bridge S1. To improve network performance you have to make S2 or S3 to become root bridge. You can do it by changing the bridge priority of S1 to 36864 or by changing the bridge priority of S3 to 4096. In any case the traffic from Front Line Users to Server Farm will go through the direct link between S2 and S3.

Reference:

CCNP Self-Study CCNP BCMSN Official Exam Certification Guide, Fourth Edition, Chapter 9: Spanning Tree Configuration, STP Root Bridge, p. 219.

QUESTION NO: 9

Refer to the exhibit.

```
interface FastEthernet 0/13
channel-group 1 mode desirable
```

What does the command channel-group 1 mode desirable do?

- A. enables LACP unconditionally
- B. enables PAgP only if a PAgP device is detected
- C. enables PAgP unconditionally
- D. enables EtherChannel only

E. enables LACP only if an LACP device is detected

Answer: C

Explanation:

The command channel-group 1 mode desirable enables PAgP unconditionally on the interface FastEthernet 0/13:

Switch (config-if)#channel-group 1 mode ?

Active Enable LACP unconditionally

Auto Enable PAgP only if a PAgP device is detected

Desirable Enable PAgP unconditionally

On Enable Etherchannel only

Passive Enable LACP only if a LACP device is detected

Reference:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/5.x/configuration/guide/channel.html>

QUESTION NO: 10

Refer to the exhibit.

3560# show interface gigabitethernet 0/1 switchport

Name: Gi0/1
 Switchport: Enabled
 Administrative Mode: trunk
 Operational Mode: trunk
 Administrative Trunking Encapsulation: dot1q
 Operational Trunking Encapsulation: dot1q
 Negotiation of Trunking: On
 Access Mode VLAN: 1 (default)
 Trunking Native Mode VLAN: 1 (default)
 Voice VLAN: none
 Administrative private-vlan host-association: none
 Administrative private-vlan mapping: none
 Administrative 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-vlan: none
 Trunking VLANs Enabled: ALL
 Pruning VLANs Enabled: 2-1001
 Capture Mode Disabled
 Capture VLANs Allowed: ALL

3560# show vlan

VLAN Name	Status	Ports
1 default	active	Gi0/2, Gi0/3, Gi0/4, Gi0/5
2 VLAN0002	active	Gi0/6, Gi0/7, Gi0/8, Gi0/9 Gi0/10, Gi0/11, Gi0/12
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Which two statements are true? (Choose two.)

- A. Interface gigabitethernet 0/1 has been configured as Layer 3 ports.
- B. Interface gigabitethernet 0/1 does not appear in the show vlan output because switchport is enabled.
- C. Interface gigabitethernet 0/1 does not appear in the show vlan output because it is configured as a trunk interface.
- D. VLAN2 has been configured as the native VLAN for the 802.1q trunk on interface gigabitethernet 0/1.
- E. Traffic on VLAN 1 that is sent out gigabitethernet 0/1 will have an 802.1q header applied.
- F. Traffic on VLAN 2 that is sent out gigabitethernet 0/1 will have an 802.1q header applied.

Answer: C,F

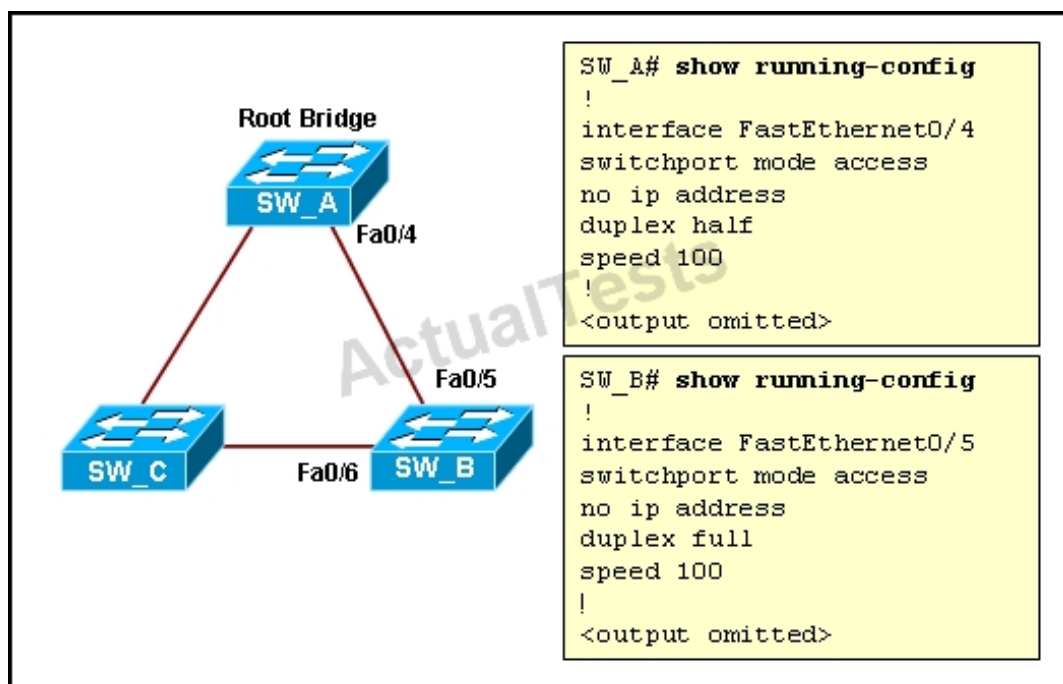
Explanation:

From the output of show interface gigabitethernet 0/1 switchport command we can see this port is currently configured as trunked port (Operational Mode: trunk) and uses 802.1q encapsulation. So surely the "show vlan" command will not list this port -> C is correct.

Also from the first output we learned the native VLAN is VLAN 1 (Trunking Native Mode VLAN:1) so only traffic from this VLAN is sent untagged -> traffic sent from VLAN 2 out this port will have an 802.1q header applied -> F is correct.

QUESTION NO: 11

Refer to the exhibit and the partial configuration of switch SW_A and SW_B.



STP is configured on all switches in the network. SW_B receives this error message on the console port:

00:06:34: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/5 (not half duplex), with SW_A FastEthernet0/4 (half duplex), with TBA05071417 (Cat6K-B) 0/4 (half duplex).

What is the possible outcome of the problem?

- A. The root port on switch SW_A will automatically transition to full-duplex mode.
- B. The root port on switch SW_B will fall back to full-duplex mode.
- C. The interfaces between switches SW_A and SW_B will transition to a blocking state.
- D. Interface Fa 0/6 on switch SW_B will transition to a forwarding state and create a bridging loop.

Answer: D

Explanation:

If switch B misses several BPDUs on the port Fa0/5 due to the duplex mismatch it will assume the path to the root via Fa0/5 is lost and it will put the port Fa0/6 in forwarding state.

Reference:

CCNP Self-Study CCNP BCMSN Official Exam Certification Guide Fourth Edition, Chapter 8: Traditional Spanning Tree Protocol, p. 185.

QUESTION NO: 12

What is the result of entering the command `port-channel load-balance src-dst-ip` on an EtherChannel link?

- A. Packets are distributed across the ports in the channel based on the source and destination MAC addresses.
- B. Packets are distributed across the ports in the channel based on both the source and destination IP addresses.
- C. Packets are balanced across the ports in the channel based first on the source MAC address, then on the destination MAC address, then on the IP address.
- D. Packets are distributed across the access ports in the channel based first on the source IP address and then on the destination IP addresses.

Answer: B

Explanation:

Traffic in an EtherChannel is distributed across the individual bundled links in a deterministic fashion; however, the load is not necessarily balanced equally across all the links. Instead, frames are forwarded on a specific link as a result of a hashing algorithm. The algorithm can use source IP address, destination IP address, or a combination of source and destination IP addresses, source and destination MAC addresses, or TCP/UDP port numbers. The hash algorithm computes a binary pattern that selects a link number in the bundle to carry each frame. The hashing operation can be performed on either MAC or IP addresses and can be based solely on source or destination addresses, or both. Use the following command to configure frame distribution for all

EtherChannel switch links:

Switch(config)# port-channel load-balance method

The default configuration is to use source XOR destination IP addresses, or the src-dst-ip method.

Reference:

CCNP BCMSN Official Exam Certification Guide, Fourth Edition, Chapter 7: Aggregating Switch Links, Distributing Traffic in EtherChannel, p. 165

QUESTION NO: 13

Which statement about the Port Aggregation Protocol is true?

- A.** Configuration changes made on the port-channel interface apply to all physical ports assigned to the port-channel interface.
- B.** Configuration changes made on a physical port that is a member of a port-channel interface apply to the port-channel interface.
- C.** Configuration changes are not permitted with Port Aggregation Protocol. Instead, the standardized Link Aggregation Control Protocol should be used if configuration changes are required.
- D.** The physical port must first be disassociated from the port-channel interface before any configuration changes can be made.

Answer: A

Explanation:

The port-channel interface is a logical interface that encompasses the all physical port members of the EtherChannel. So configuration changes made on the port-channel interface apply to all physical ports assigned to the port-channel interface.

Reference:

http://www.cisco.com/en/US/tech/tk389/tk213/technologies_configuration_example09186a0080094647.shtml

QUESTION NO: 14 DRAG DROP

Syslog information can generate messages up to and including the configured severity level. Organize the levels by dragging each name from the left to the right. Put the highest level at the top and the lowest level at the bottom.

debugging		
notification		
error		
alert		
emergency		
critical		
warning		
informational		

Answer:

Syslog information can generate messages up to and including the configured severity level. Organize the levels by dragging each name from the left to the right. Put the highest level at the top and the lowest level at the bottom.

debugging	emergency
notification	alert
error	critical
alert	error
emergency	warning
critical	notification
warning	informational
informational	debugging

Explanation:

emergency
alert
critical
error
warning
notification
informational
debugging

QUESTION NO: 15 DRAG DROP

Drag the choices on the left to the boxes on the right that should be included when creating a VLAN-based implementation plan. Not all choices will be used.

reference to design documents	
roll back guidelines	
VTP assignments	
detailed implementation plans	
time required to perform the implementation	

Answer:

Drag the choices on the left to the boxes on the right that should be included when creating a VLAN-based implementation plan. Not all choices will be used.

reference to design documents

reference to design documents

roll back guidelines

roll back guidelines

VTP assignments

detailed implementation plans

detailed implementation plans

time required to perform the implementation

time required to perform the implementation

Explanation:

Reference to design documents

Rollback Guidelines

Detailed implementation plan

Time required to perform the implementation

QUESTION NO: 16 DRAG DROP

You have been tasked with planning a VLAN solution that will connect a server in one building to several hosts in another building. The solution should be built using the local VLAN model and Layer 3 switching at the distribution layer. Drag the questions that you would ask the network administrator before you start the planning from the left to the right. Not all questions will be used.

Is there interswitch connectivity?

What version of VTP is being used?

What routing protocol will be used?

What VLANs are available on each switch?

What operating system is used on the server?

What switch ports are available in each building?

What IP addresses are available on each subnet?

What operating system is used on each host?

Questions Related to the VLAN Solution

Answer:

You have been tasked with planning a VLAN solution that will connect a server in one building to several hosts in another building. The solution should be built using the local VLAN model and Layer 3 switching at the distribution layer. Drag the questions that you would ask the network administrator before you start the planning from the left to the right. Not all questions will be used.

Is there interswitch connectivity?
What version of VTP is being used?
What routing protocol will be used?
What VLANs are available on each switch?
What operating system is used on the server?
What switch ports are available in each building?
What IP addresses are available on each subnet?
What operating system is used on each host?

Questions Related to the VLAN Solution

Is there interswitch connectivity?
What routing protocol will be used?
What VLANs are available on each switch?
What switch ports are available in each building?
What IP addresses are available on each subnet?

Explanation:

Questions Related to the VLAN Solution Is there interswitch connectivity? What routing protocol will be used? What VLANs are available on each switch? What switch ports are available in each building? What IP addresses are available on each subnet?
--

QUESTION NO: 17 CORRECT TEXT

Refer to the Exhibit.

The central office for a cement manufacturer is installing a temporary Catalyst 3550 in an IDF to connect 24 additional users. To prevent network corruption, it is important to have the correct configuration prior to connecting to the production network. It will be necessary to ensure that the switch does not participate in VTP but forwards VTP advertisements that are received on trunk ports.

Because of errors that have been experienced on office computers, all nontrunking interfaces should transition immediately to the forwarding state of Spanningtree. Also, configure the user ports (all FastEthernet ports) so that the ports are permanently nontrunking.

The screenshot shows the eSIM Professional software interface. On the left, a 'Scenario 1' window displays the problem statement and instructions. The main area shows a topology diagram with a host icon connected to a switch icon via a curved solid black line labeled 'CONSOLE'. A watermark 'ActualTests' is visible across the diagram.

Scenario 1
Version 1.0

You will have to scroll this window and the problem statement window to view the entire problem.

To configure the switch click on a host icon that is connected to a switch by a serial console cable (shown in the diagram as a curved solid black line).

The [Tab] key

Hide Topology

The information of the question

You will configure FastEthernet ports 0/12 through 0/24 for users who belong to VLAN 20. Also, all VLAN and VTP configurations are to be completed in global configuration mode as VLAN database mode is being deprecated by Cisco. You are required to accomplish the following tasks:

1. Ensure the switch does not participate in VTP but forwards VTP advertisements received on trunk ports.
2. Ensure all non-trunking interfaces (Fa0/1 to Fa0/24) transition immediately to the forwarding state of Spanning-Tree.
3. Ensure all FastEthernet interfaces are in a permanent non-trunking mode.
4. Place FastEthernet interfaces 0/12 through 0/24 in VLAN 20

Answer: switch#conf t

switch(config)#vtp mode transparent

switch(config)#interface range fa0/1 - 24

switch(config-if-range)#switchport mode access

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

switch(config)#interface range fa0/12 - 24

switch(config-if-range)#switchport access vlan 20

switch(config-if-range)#end

switch# copy run start

VTP:

The role of the VLAN Trunking Protocol (VTP) is to maintain VLAN configuration consistency across the entire network. VTP is a messaging protocol that uses Layer 2 trunk frames to manage the addition, deletion, and renaming of VLANs on a network-wide basis from a centralized switch that is in the VTP server mode. VTP is responsible for synchronizing VLAN information within a VTP domain. This reduces the need to configure the same VLAN information on each switch. VTP minimizes the possible configuration inconsistencies that arise when changes are made. These inconsistencies can result in security violations, because VLANs can crossconnect when duplicate names are used. They also could become internally disconnected when they are mapped from one LAN type to another, for example, Ethernet to ATM LANE VLANs or FDDI 802.10 VLANs. VTP provides a mapping scheme that enables seamless trunking within a network employing mixed-media technologies.

VTP provides the following benefits:

VLAN configuration consistency across the network

Mapping scheme that allows a VLAN to be trunked over mixed media

Accurate tracking and monitoring of VLANs

Dynamic reporting of added VLANs across the network

Plug-and-play configuration when adding new VLANs

There are three different VTP modes:

1. Server:

By default, a Catalyst switch is in the VTP server mode and in the “no management domain” state until the switch receives an advertisement for a domain over a trunk link or a VLAN management domain is configured. A switch that has been put in VTP server mode and had a domain name specified can create, modify, and delete VLANs. VTP servers can also specify other configuration parameters such as VTP version and VTP pruning for the entire VTP domain. VTP information is stored in NVRAM.

VTP servers advertise their VLAN configuration to other switches in the same VTP domain, and synchronize the VLAN configuration with other switches based on advertisements received over trunk links. When a change is made to the VLAN configuration on a VTP server, the change is propagated to all switches in the VTP domain. VTP advertisements are transmitted out all trunk connections, including ISL, IEEE 802.1Q, IEEE 802.10, and ATM LANE trunks.

2. Client:

The VTP client maintains a full list of all VLANs within the VTP domain, but it does not store the information in NVRAM. VTP clients behave the same way as VTP servers, but it is not possible to create, change, or delete VLANs on a VTP client. Any changes made must be received from a VTP server advertisement.

3. Transparent

VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration, and does not synchronize its VLAN configuration based on received advertisements. However, in VTP Version 2, transparent switches do forward VTP advertisements that the switches receive out their trunk ports. VLANs can be configured on a switch in the VTP

transparent mode, but the information is local to the switch (VLAN information is not propagated to other switches) and is stored in NVRAM.

To change the VTP mode:

```
Switch(Config)# vtp mode <Mode>
```

Or

```
Switch#vlan database
```

```
Switch#vtp <mode>
```

PortFast

A prime reason for enabling PortFast is in cases where a PC boots in a period less than the 30 seconds it takes a switch to put a port into forwarding mode from disconnected state. Some NICs do not enable a link until the MAC layer software driver is actually loaded. Most operating systems try to use the network almost immediately after loading the driver, as in the case of DHCP. This can create a problem because the 30 seconds of STP delay from listening to Forwarding states begins right when the IOS begins trying to access the network. In the case of DHCP, the PC will not obtain a valid IP address from the DHCP server. This problem is common with PC Card (PCMCIA) NICs used in laptop computers. Additionally, there is a race between operating systems and CPU manufacturers. CPU manufacturers keep making the chips faster, while at the same time, operating systems keep slowing down, but the chips are speeding up at a greater rate than the operating systems are slowing down. As a result, PCs are booting faster than ever. In fact, modern machines are often finished booting and need to use the network before the STP 30-second delay is over.

Use the spanning-tree portfast global configuration command to globally enable the PortFast feature on all non-trunking ports.

QUESTION NO: 18 CORRECT TEXT

Case 1

The headquarter offices for a footwear distributor are enhancing their wiring closets with Layer3 switches. The new distribution-layer switch has been installed and a new access-layer switch cabled to it. Your task is to configure VTP to share VLAN information from the distribution-layer switch to the access-layer devices. Then, it is necessary to configure interVLAN routing on the distribution-layer switch to route traffic between the different VLANs that are configured on the access-layer switches; however, it is not necessary for you to make the specific VLAN port assignments on the access-layer switches. Also, because VLAN database mode is being deprecated by Cisco, all VLAN and VTP configurations are to be completed in the global configuration mode. Please reference the following table for the VTP and VLAN information to be configured:

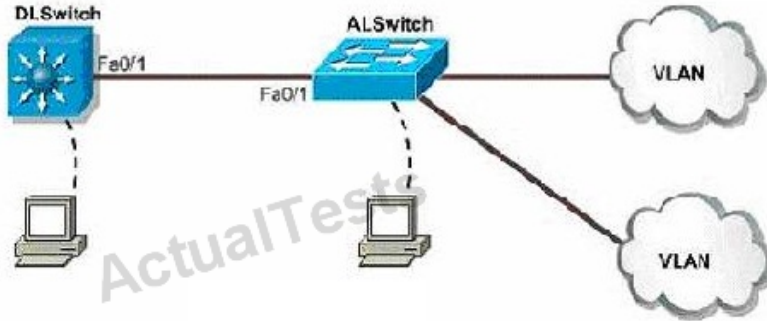
Scenario 1

You will have to scroll this window and the problem statement window to view the entire problem.

To configure the switch click on a host icon that is connected to a switch by a serial console cable (shown in the diagram as a curved dashed black line).

The [Tab] key

Hide Topology



ActualTests

VTP Domain:	CISCO	
VLAN IDs:	20	21
IP Addresses:	172.16.236.1/24	172.16.170.1/24

You must accomplish the following tasks:

- Configure the VTP information with the distribution layer switch as the VTP server.
- Configure the VTP information with the access layer switch as a VTP client.

VLAN IDs:	20	21
IP Addresses:	172.16.236.1/24	172.16.170.1/24

You must accomplish the following tasks:

- Configure the VTP information with the distribution layer switch as the VTP server.
- Configure the VTP information with the access layer switch as a VTP client.
- Configure VLANs on the distribution layer switch.
- Configure inter-VLAN routing on the distribution layer switch.

Answer: Here are the steps.

Explanation:

```
CiscoTerminal

end
DLSwitch#
DLSwitch#
DLSwitch#
DLSwitch#configure terminal
Enter configuration commands, one per line. End with END.
DLSwitch(config)#interface vlan 1
DLSwitch(config-if)#no shutdown
DLSwitch(config-if)#inter
DLSwitch(config-if)#exit
DLSwitch(config)#intr
DLSwitch(config)#interface vlan 20
DLSwitch(config-if)#ip address 172.16.236.1 255.255.255.0
DLSwitch(config-if)#no shutdown
DLSwitch(config-if)#exit
DLSwitch(config)#interface vlan 21
DLSwitch(config-if)#ip address 172.16.170.1 255.255.255.0
DLSwitch(config-if)#no shutdown
DLSwitch(config-if)#exit
DLSwitch(config)#vtp domain CISCO
Changing VTP domain name from NULL to CISCO
DLSwitch(config)#vtp mode server
Setting device to VTP SERVER mode.
DLSwitch(config)#_
```

```
CiscoTerminal

DLSwitch(config-if)#no shutdown
DLSwitch(config-if)#inter
DLSwitch(config-if)#exit
DLSwitch(config)#intr
DLSwitch(config)#interface vlan 20
DLSwitch(config-if)#ip address 172.16.236.1 255.255.255.0
DLSwitch(config-if)#no shutdown
DLSwitch(config-if)#exit
DLSwitch(config)#interface vlan 21
DLSwitch(config-if)#ip address 172.16.170.1 255.255.255.0
DLSwitch(config-if)#no shutdown
DLSwitch(config-if)#exit
DLSwitch(config)#vtp domain CISCO
Changing VTP domain name from NULL to CISCO
DLSwitch(config)#vtp mode server
Setting device to VTP SERVER mode.
DLSwitch(config)#exit
00:00:04:44: %SYS-5-CONFIG_I: Configured from console by console
DLSwitch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

[OK]
DLSwitch#_
```

```
CiscoTerminal

!
ip http server
!
!
!
!
line con 0
line aux 0

line vty 5 15
login
!
end
DLSwitch#conf t
Enter configuration commands, one per line. End with END.
DLSwitch(config)#ip routing
DLSwitch(config)#end
00:00:06:36: %SYS-5-CONFIG_I: Configured from console by console
DLSwitch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

[OK]
DLSwitch#
```

```
CiscoTerminal

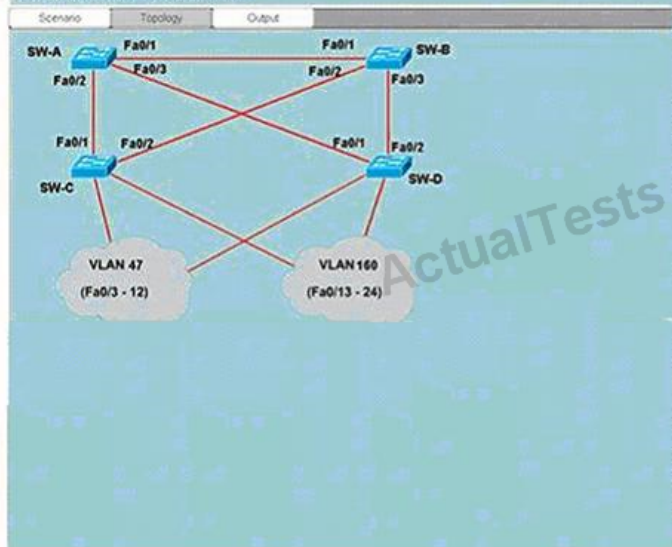
ALSwitch#
ALSwitch#
ALSwitch#
ALSwitch#
ALSwitch#
ALSwitch#configure terminal
Enter configuration commands, one per line. End with END.
ALSwitch(config)#interface f
ALSwitch(config)#interface fastEthernet 0/1
ALSwitch(config-if)#switchport mode trunk
ALSwitch(config-if)#exit
ALSwitch(config)#vtp mode CLIENT
Setting device to VTP CLIENT mode
ALSwitch(config)#vtp domain CISCO
Domain name already set to CISCO.
ALSwitch(config)#
ALSwitch(config)#exit
00:00:08:43: %SYS-5-CONFIG_I: Configured from console by console
ALSwitch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

[OK]
ALSwitch#_
```

QUESTION NO: 19 HOTSPOT

This is a "Testlet" - it contains 5 question(s) that relate to the scenario below.

Online Incorporated is an internet game provider. The game service network had recently added an additional switch block with multiple VLANs configured. Unfortunately, system administrators neglected to document the spanning-tree topology during configuration. For baseline purposes, you will be required to identify the spanning-tree topology for the switch block. Using the output of the show spanning-tree command on switch SW-C and the provided physical topology, answer the following questions:



SW-C# show spanning-tree

```

VLAN0001
Spanning tree enabled protocol rstp
Root ID: Priority 32769
Address: 000d.65db.01dd
Cost: 19
Port: 1 (FastEthernet0/1)
Hello Time: 2 sec Max Age: 20 sec Forward Delay: 15 sec

Bridge ID: Priority 32769 (priority 32768 sys-id-ext 1)
Address: 000d.65db.029b
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 Desig FWD 19 128.2 P2p Peer (STP)
VLAN0047

Spanning tree enabled protocol rstp
Root ID: Priority 24623
Address: 000f.34f5.039b
Cost: 19
Port: 2 (FastEthernet0/2)
Hello Time: 2 sec Max Age: 20 sec Forward Delay: 15 sec
Bridge ID: Priority 32815 (priority 32768 sys-id-ext 47)
Address: 000d.b0d3.029b
Hello Time: 2 sec Max Age: 20 sec Forward Delay: 15 sec
Aging Time: 300

Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/1 Altn BLK 19 128.1 P2p
Fa0/2 Root FWD 19 128.2 P2p Peer (STP)
VLAN0160

Spanning tree enabled protocol rstp
Root ID: Priority 24736
Address: 000d.65db.01dd
Cost: 19
Port: 1 (FastEthernet0/1)
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 Desig FWD 19 128.2 P2p Peer (STP)
  
```

Which port state is interface Fa0/2 of switch SW-B in for VLANs 1 and 175?

- Question 1 of 5
- ☐ blocking
 - ☐ disabled
 - ☐ discarding
 - ☐ forwarding
 - ☐ learning
 - ☐ listening

1
2
3
4
5

Which Spanning Tree Protocol has been implemented on switch SW-B?

- Question 2 of 5
- ☐ PVST+
 - ☐ PVRST
 - ☐ MSTP/IEEE 802.1s
 - ☐ STP/IEEE 802.1D

1
2
3
4
5

Which bridge ID belongs to switch SW-A?

- Question 3 of 5
- ☐ 24620.000f34f5.013d
 - ☐ 32768.000e b403.0249
 - ☐ 32768.000e 65cb.01a1
 - ☐ 32769.000e 65cb.01a1
 - ☐ 32943.000e b403.0249
 - ☐ 32943.000e b403.0249

1
2
3
4
5

Which port role has interface Fa0/2 of switch SW-A adopted for VLAN 44?

- Question 4 of 5
- ☐ alternate port
 - ☐ backup port
 - ☐ designated port
 - ☐ root port
 - ☐ nondesignated port

1
2
3
4
5

Answer:

Which port state is interface Fa0/2 of switch SW-B in for VLANs 1 and 175?

- Question 1 of 5
- ☒ blocking
 - ☐ disabled
 - ☐ discarding
 - ☐ forwarding
 - ☐ learning
 - ☐ listening

1
2
3
4
5

Which Spanning Tree Protocol has been implemented on switch SW-B?

- Question 2 of 5
- ☒ PVST+
 - ☐ PVRST
 - ☐ MSTP/IEEE 802.1s
 - ☐ STP/IEEE 802.1D

1
2
3
4
5

Which bridge ID belongs to switch SW-A?

- Question 3 of 5
- ☐ 24820.000f34f5.013d
 - ☐ 32768.000c.bdc3.0249
 - ☐ 32768.000c.65cb.01a1
 - ☒ 32769.000c.65cb.01a1
 - ☐ 32943.000c.bdc3.0249
 - ☐ 32943.000c.bdc3.0249

1
2
3
4
5

Which port role has interface Fa0/2 of switch SW-A adopted for VLAN 44?

- Question 4 of 5
- ☐ alternate port
 - ☐ backup port
 - ☒ designated port
 - ☐ root port
 - ☐ nondesignated port

1
2
3
4
5

Explanation:

Which port state is interface Fa0/2 of switch SW-B in for VLANs 1 and 175?

- Question 1 of 5
- ☒ blocking
 - ☐ disabled
 - ☐ discarding
 - ☐ forwarding
 - ☐ learning
 - ☐ listening

1
2
3
4
5

Which Spanning Tree Protocol has been implemented on switch SW-B?

- Question 2 of 5
- ☒ PVST+
 - ☐ PVRST
 - ☐ MSTP/IEEE 802.1s
 - ☐ STP/IEEE 802.1D

1
2
3
4
5

Which bridge ID belongs to switch SW-A?

- Question 3 of 5
- ☐ 24820.000f34f5.013d
 - ☐ 32768.000c.bdc3.0249
 - ☐ 32768.000c.65db.01a1
 - ☒ 32769.000c.65db.01a1
 - ☐ 32843.000c.bdc3.0249
 - ☐ 32812.000c.bdc3.0249

1
2
3
4
5

Which port role has interface Fa0/2 of switch SW-A adopted for VLAN 44?

- Question 4 of 5
- ☐ alternate port
 - ☐ backup port
 - ☒ designated port
 - ☐ root port
 - ☐ nondesignated port

1
2
3
4
5

Which bridge ID belongs to switch SW-B?

- Question 5 of 5
- ☒ 24820.000f34f5.013d
 - ☐ 32768.000c.bdc3.0249
 - ☐ 32768.000c.65db.01a1
 - ☐ 32769.000c.65db.01a1
 - ☐ 32843.000c.bdc3.0249
 - ☐ 32812.000c.bdc3.0249

1
2
3
4
5

QUESTION NO: 20 CORRECT TEXT

Acme is small export company that has an existing enterprise network comprised of 5 switches; CORE,DSW1,

DSW2,ASW1 and ASW2. The topology diagram indicates their desired pre-VLAN spanning tree mapping.

Previous configuration attempts have resulted in the following issues:

- CORE should be the root bridge for VLAN 20; however, DSW1 is currently the root bridge for VLAN 20.

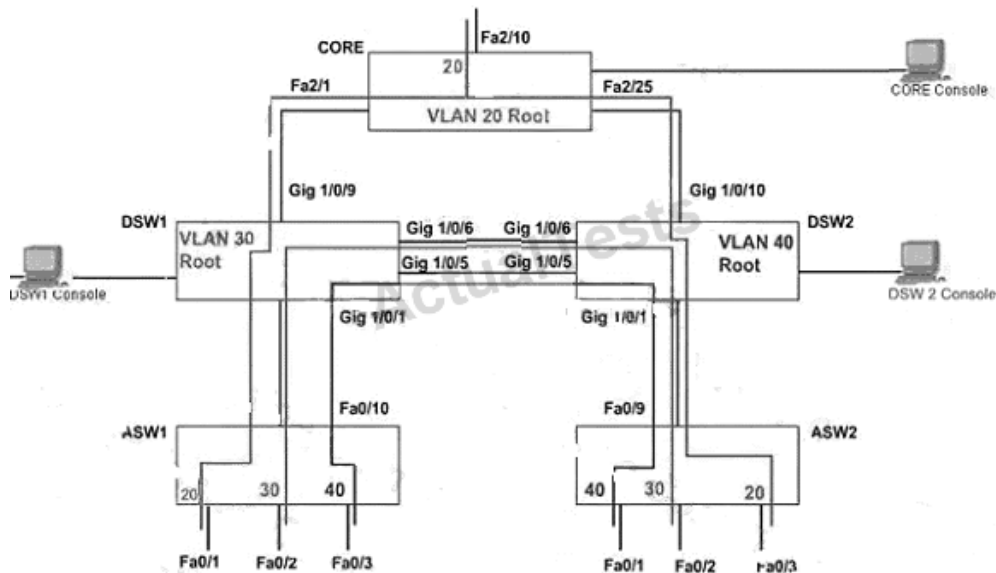
- Traffic for VLAN 30 should be forwarding over the gig 1/0/6 trunk port between DSW1 and DSW2.

However VLAN 30 is currently using gig 1/0/5.

- Traffic for VLAN 40 should be forwarding over the gig 1/0/5 trunk port between DSW1 and DSW2.

However VLAN 40 is currently using gig 1/0/6.

You have been tasked with isolating the cause the these issuer and implementing the appropriate solutions. You task is complicated by the fact that you only have full access to DSW1, with isolating the cause of these issues and implementing the appropriate solutions, Your task is complicated by the fact that you only have full access to DSW1, with the enable secret password cisco. Only limited show command access is provided on CORE, and DSW2 using the enable 2 level with a password of acme. No configuration changes will be possible on these routers. No access is provided to ASW1 or ASW2.



```
hostname DSW1
```

```
!
```

```
enable secret 5 $1$wN16$j5RnayatKfxaKxhX30TVo0
```

```
!
```

```
no aaa new-model
```

```
switch 1 provision ws-c3750g-24t
```

```
ip subnet-zero
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
no file verify auto
```

```
!
```

```
spanning-tree mode pvst
```

```
spanning-tree extend system-id
```

```
spanning-tree "vlan 20 priority 28672
spanning-tree vlan 30 priority 24576
!
vlan internal allocation policy ascending
!
!
interface GigabitEthernet1/0/1
description trunk line to ASW1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
speed 100
duplex full
!
interface GigabitEthernet1/0/2
shutdown
!
interface GigabitEthernet1/0/3
shutdown
!
interface GigabitEthernet1/0/4
shutdown
!
interface GigabitEthernet1/0/5
description trunk line to DSW 2
switchport trunk encapsulation dot1q
switchport mode trunk
```

switchport nonegotiate

speed 100

duplex full

!

interface GigabitEthernet1/0/6

description trunk line to DSW 2

switchport trunk encapsulation dot1q

switchport mode trunk

switchport nonegotiate

speed 100

duplex full

!

interface GigabitEthernet1/0/7

shutdown

!

interface GigabitEthernet1/0/8

shutdown

!

Interface GigabitEthernet1/0/9

description trunk line to CORE

switchport trunk encapsulation dot1q

switchport mode trunk

!

end

DSW1# Show sp

DSW1# Show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0016. 4658. f300

Cost 19

Port 9 (GigabitEthernet/0/9)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0016. 46fa. 9b00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface	Role	Sts	Cost	Prio...Nbr	Type
-----	-----	-----	-----	-----	-----
Gil/0/1	Desg	FWD	19	128.1	P2p
Gil/0/5	Altn	BLK	19	128.5	P2p
Gil/0/6	Altn	BLK	19	128.6	P2p
Gil/0/9	Root	FWD	19	128.9	P2p

VLAN0020

Spanning three enabled protocol ieee

Root ID Priority 28692

Address 0016. 46fa. 9b00

This bridge is the root

Bridge ID Priority 28692 (priority 28672 sys-id-ext 20)

Address 0016. 46fa. 9b00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface	Role	Sts	Cost	Prio..Nbr	Type
-----	-----	-----	-----	-----	-----
Gil/0/5	Altn	BLK	19	128.5	P2p
Gil/0/6	Altn	BLK	19	128.6	P2p
Gil/0/9	Root	FWD	19	128.9	P2p

VLAN0020

Spanning three enabled protocol ieee

Root ID Priority 28692

Address 0016. 46fa. 9b00

This bridge is the root

Bridge ID Priority 28692 (priority 28672 sys-id-ext 20)

Address 0016. 46fa. 9b00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface	Role	Sts	Cost	Prio..Nbr	Type
-----	-----	-----	-----	-----	-----
Gil/0/1	Desg	FWD	19	128.1	P2p
Gil/0/5	Desg	BLK	19	128.5	P2p
Gil/0/6	Desg	BLK	19	128.6	P2p
Gil/0/9	Desg	FWD	19	128.9	P2p

VLAN0030

Spanning three enabled protocol ieee

Root ID Priority 24606

This bridge is the root

Bridge ID Priority 28692 (priority 28672 sys-id-ext 20)

Address 0016. 46fa. 9b00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface	Role	Sts	Cost	Prio..Nbr	Type
-----	-----	-----	-----	-----	-----
Gil/0/1	Desg	FWD	19	128.1	P2p
Gil/0/5	Desg	BLK	19	128.5	P2p
Gil/0/6	Desg	BLK	19	128.6	P2p
Gil/0/9	Desg	FWD	19	128.9	P2p

VLAN0040

Spanning three enabled protocol ieee

Root ID Priority 24616

Address 0016. 46fa. 6a00

Cost 19

Port 9 (GigabitEthernet/0/9)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32808 (priority 32768 sys-id-ext 40)

Address 0016. 46fa. 9b00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface	Role	Sts	Cost	Prio..Nbr	Type
-----	-----	-----	-----	-----	-----
Gil/0/1	Desg	FWD	19	128.1	P2p
Gil/0/5	Altn	BLK	19	128.5	P2p
Gil/0/6	Root	FWD	19	128.6	P2p
Gil/0/9	Altn	BLK	19	128.9	P2p

DSW1#

Answer: DSW1#conf t

DSW1(config)#spanning-tree vlan 20 priority 61440

DSW1(config)#int g1/0/5

DSW1(config-if)#spanning-tree vlan 40 cost 1

DSW1(config-if)#no shut

DSW1(config-if)#exit

DSW1(config)#int g1/0/6

DSW1(config-if)#spanning-tree vlan 30 port-priority 64

DSW1(config-if)#no shut

DSW1(config-if)#end

DSW1#copy run start

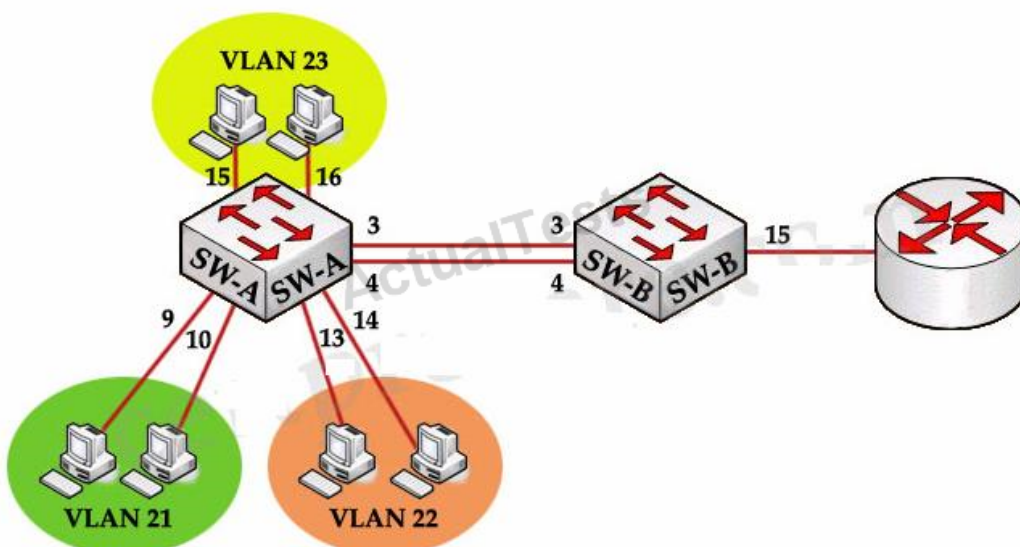
Verification:

DSW1# show spanning-tree vlan 20

DSW1# show spanning-tree vlan 40

DSW2# show spanning-tree vlan 30

QUESTION NO: 21 CORRECT TEXT



Each of these vlans has one host each on its ports

SVI on vlan 1 - ip 192.168.1.11

Switch B -

Ports 3, 4 connected to ports 3 and 4 on Switch A

Port 15 connected to Port on Router.

Tasks to do:

1. Use non proprietary mode of aggregation with Switch B being the initiator
-- Use LACP with B being in Active mode
2. Use non proprietary trunking and no negotiation
-- Use switchport mode trunk and switchport trunk encapsulation dot1q
3. Restrict only to the VLANs needed
-- Use either VTP pruning or allowed VLAN list. The preferred method is using allowed VLAN list
4. SVI on VLAN 1 with some ip and subnet given
5. Configure switch A so that nodes other side of Router C are accessible
-- on switch A the default gateway has to be configured.
6. Make switch B the root

Answer: on Switch A

verify with show run if you need to create vlans 21-23

int range fa0/9 - 10

switchport mode access

switchport access vlan 21

spanning-tree portfast

no shut

int range fa0/13 - 14

switchport mode access

switchport access vlan 22

```
spanning-tree portfast
no shut
int range fa0/16 - 16
switchport mode access
switchport access vlan 23
spanning-tree portfast
no shut
int range fa0/3 - 4
channel-protocol lacp
channel group 1 mode passive
no shut
int port-channel 1
switchport mode trunk
switchport trunk encapsulation dot1q
spanning-tree allowed vlans 1,21-23
no shut
int vlan 1
ip address 192.168.1.11 255.255.255.0
no shut
SW B
conf t
interface range fastethernet 0/9-10
switchport mode access
switchport access vlan 21
spanning-tree portfast
no shut
interface rang fastethernet 0/13-14
switchport mode access
switchport access vlan 22
spanning-tree portfast
no shut
interface rang fastethernet 0/15-16
switchport mode access
switchport access vlan 23
spanning-tree portfast
no shut
interface range fastethernet 0/3-4
switchport trunk encapsulation dot1q
switchport trunk native vlan 99
switchport trunk allowed vlan 1,21-23,99
switchport mode trunk
```

```
channel-protocol lacp
channel-group 1 mode passsive
no shut
// port-channel 1 automatically created and nothing needs to be configured under it
ip default-gateway 10.10.10.1
// VLAN 1 already configured nothing more to be done on it
SWA
vlan 21
vlan 22
vlan 23
interface range fastethernet 0/3-4
switchport trunk native vlan 99
switchport trunk allowed vlan 1,21-23,99
switchport mode trunk
channel-protocol lacp
channel-group 1 mode active
no shut
spanning-tree vlan 1,21-23,99 root primary
```

QUESTION NO: 22 CORRECT TEXT

Scenario:

You work for SWITCH.com. They have just added a new switch (SwitchB) to the existing network as shown in the topology diagram.

RouterA is currently configured correctly and is providing the routing function for devices on SwitchA and SwitchB. SwitchA is currently configured correctly, but will need to be modified to support the addition of SwitchB. SwitchB has a minimal configuration. You have been tasked with competing the needed configuring of SwitchA and SwitchB. SwitchA and SwitchB use Cisco as the enable password.

Configuration Requirements for SwitchA

The VTP and STP configuration modes on SwitchA should not be modified.

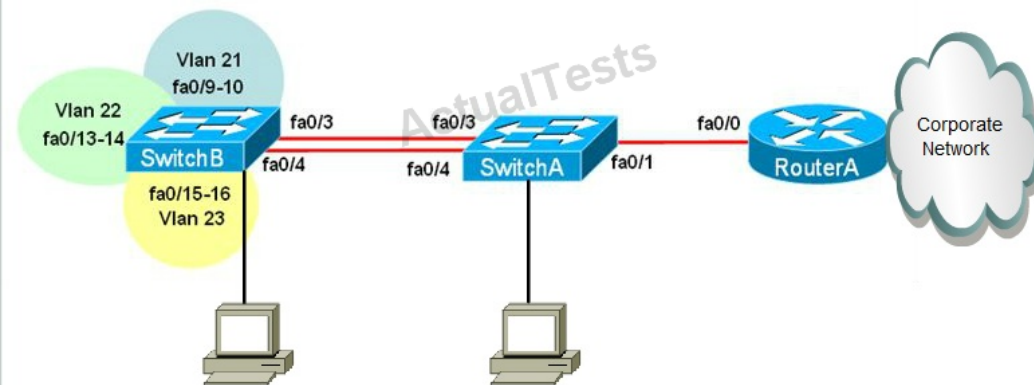
- SwitchA needs to be the root switch for vlans 11, 12, 13, 21, 22 and 23. All other vlans should be left are their default values.

Configuration Requirements for SwitchB

- Vlan 21
 - o Name: Marketing
 - o will support two servers attached to fa0/9 and fa0/10
- Vlan 22
 - o Name: Sales
 - o will support two servers attached to fa0/13 and fa0/14
- Vlan 23
 - o Name: Engineering
 - o will support two servers attached to fa0/15 and fa0/16
- Access ports that connect to server should transition immediately to forwarding state upon detecting the connection of a device.
- SwitchB VTP mode needs to be the same as SwitchA.
- SwitchB must operate in the same spanning tree mode as SwitchA
- No routing is to be configured on SwitchB
- Only the SVI vlan 1 is to be configured and it is to use address 192.168.1.11/24

Inter-switch Connectivity Configuration Requirements

- For operational and security reasons trunking should be unconditional and Vlans 1, 21, 22 and 23 should tagged when traversing the trunk link.
- The two trunks between SwitchA and SwitchB need to be configured in a mode that allows for the maximum use of their bandwidth for all vlans. This mode should be done with a non-proprietary protocol, with SwitchA controlling activation.
- Propagation of unnecessary broadcasts should be limited using manual pruning on this trunk link.



Answer: Here are steps:

```
hostname SWITCH_B
```

```
!
```

```
!
```

```
vlan 21
```

```
name Marketing
```

```
vlan 22
```

```
name Sales
```

```
vlan 23
```

```
name Engineering
```

```
!
```

```
!
```

```
interface FastEthernet0/3
```

```
switchport trunk allowed vlan 1,21-23
```

```
channel-protocol lacp
```

```
channel-group 1 mode passive
```

```
switchport mode trunk
```

```
!
```

```
interface FastEthernet0/4
```

```
switchport trunk allowed vlan 1,21-23
```

```
channel-protocol lacp
```

```
channel-group 1 mode passive
```

```
switchport mode trunk
```

```
!
```

```
interface FastEthernet0/9
```

```
switchport access vlan 21
```

```
switchport mode access
```

```
spanning-tree portfast
```

```
!  
interface FastEthernet0/10  
switchport access vlan 21  
switchport mode access  
spanning-tree portfast  
!  
interface FastEthernet0/13  
switchport access vlan 22  
switchport mode access  
spanning-tree portfast  
!  
!  
interface FastEthernet0/14  
switchport access vlan 22  
switchport mode access  
spanning-tree portfast  
!  
interface FastEthernet0/15  
switchport access vlan 23  
switchport mode access  
spanning-tree portfast  
!  
interface FastEthernet0/16  
switchport access vlan 23  
switchport mode access  
spanning-tree portfast  
!  
!  
interface GigabitEthernet1/1  
!  
interface GigabitEthernet1/2  
!  
interface Port-channel 1  
switchport mode trunk  
switchport trunk encapsulation dot1q  
spanning-tree allowed vlans 1,21-23  
!  
interface Vlan1  
ip address 192.168.1.11 255.255.255.0  
!  
end
```

```
SWITCH_B(config)#
hostname SWITCH_A
!
spanning-tree vlan 11 root primary
spanning-tree vlan 12 root primary
spanning-tree vlan 13 root primary
spanning-tree vlan 21 root primary
spanning-tree vlan 22 root primary
spanning-tree vlan 23 root primary
!
interface FastEthernet0/3
switchport trunk allowed vlan 1,21-23
channel-protocol lacp
channel-group 1 mode active
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk allowed vlan 1,21-23
channel-protocol lacp
channel-group 1 mode active
switchport mode trunk
!
interface FastEthernet0/21
switchport access vlan 21
switchport mode access
!
interface FastEthernet0/22
switchport access vlan 22
switchport mode access
!
interface FastEthernet0/23
switchport access vlan 23
switchport mode access
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Port-channel 1
!
interface Vlan1
```

```
no ip address
shutdown
!
ip default-gateway 192.168.1.1
!
!
End
```

QUESTION NO: 23 CORRECT TEXT

You have been tasked with configuring multilayer SwitchC, which has a partial configuration and has been attached to RouterC as shown in the topology diagram.

You need to configure SwitchC so that Hosts H1 and H2 can successfully ping the server S1. Also SwitchC needs to be able to ping server S1.

Due to administrative restrictions and requirements you should not add/delete VLANs or create trunk links. Company policies forbid the use of static or default routing. All routes must be learned via EIGRP 65010 routing protocol.

You do not have access to RouterC, RouterC is correctly configured. No trunking has been configured on RouterC.

Routed interfaces should use the lowest host on a subnet when possible. The following subnets are available to implement this solution:

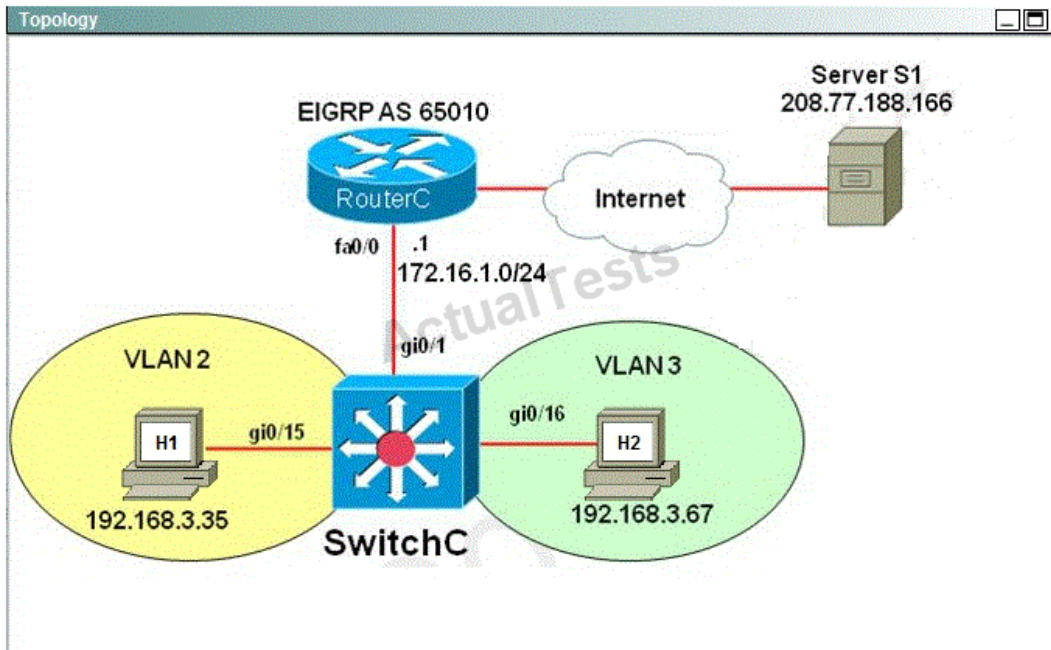
- 172.16.1.0/24
- 192.168.3.32/27
- 192.168.3.64/27

Hosts H1 and H2 are configured with the correct IP address and default gateway.

SwitchC uses Cisco as the enable password.

Routing must only be enabled for the specific subnets shown in the diagram.

Note: Due to administrative restrictions and requirements you should not add or delete VLANs, changes VLAN port assignments or create trunks. Company policies forbid the use of static or default routing. All routes must be learning via the EIGRP routing protocol.



HOST 1

```
Press RETURN to get started!  
C:\>  
C:\>  
C:\>  
C:\>ipconfig  
  
IP Configuration  
  
Ethernet adapter Generic Network Adapter:  
  
    Connection-specific DNS Suffix  . :  
    Ip Address. . . . . : 192.168.3.35  
    Subnet Mask . . . . . : 255.255.255.224  
    Default Gateway . . . . . : 192.168.3.33  
  
C:\>
```

HOST 2

```
Press RETURN to get started!
C:\>
C:\>
C:\>ipconfig

IP Configuration

Ethernet adapter Generic Network Adapter:

    Connection-specific DNS Suffix  . : 
    Ip Address. . . . . : 192.168.3.67
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : 192.168.3.65

C:\>
```

Answer: Here are Step by Step Configuration:

Explanation:

On switch C:

ip routing

router eigrp 65010

network 172.16.1.0 0.0.0.255

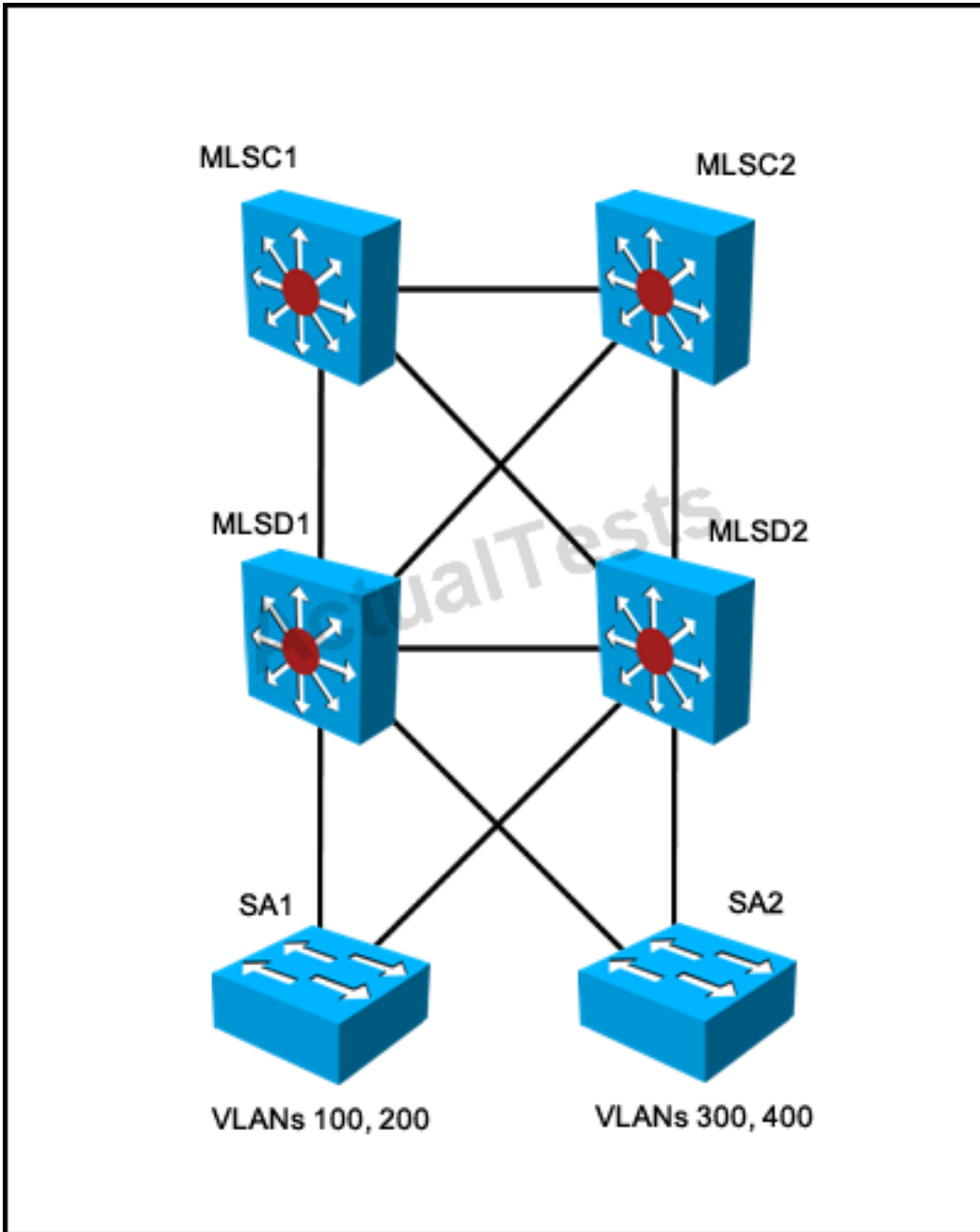
network 192.168.3.32 0.0.0.31

network 192.168.3.64 0.0.0.31

no auto-sum

QUESTION NO: 24

Refer to the exhibit.



For the configuration shown, which is the recommended method of providing interVLAN routing?

- A. determine which switch is the root bridge then connect a router on a stick to it
- B. configure SVIs on the core switches
- C. configure SVIs on the distribution switches
- D. configure SVIs on the access layer switches

Answer: C

Explanation:

Inter-VLAN routing on distribution layer switches is made possible with switch virtual interfaces (SVIs). Multilayer switches, such as Cisco Catalyst 3560 switches, are capable of wire-speed IP

routing in addition to traditional Layer 2 switching. In this case, distribution layer bound IP subnets with hosts pointing to the SVIs as default gateways for the respective IP subnets. Full IP communications, previously available only with dedicated routers, are made available with these multilayer switches.

QUESTION NO: 25

Under what circumstances should an administrator prefer local VLANs over end-to-end VLANs?

- A. Eighty percent of traffic on the network is destined for Internet sites.
- B. There are common sets of traffic filtering requirements for workgroups located in multiple buildings.
- C. Eighty percent of a workgroup's traffic is to the workgroup's own local server.
- D. Users are grouped into VLANs independent of physical location.
- E. None of the other alternatives apply

Answer: A

Explanation:

This geographic location can be as large as an entire building or as small as a single switch inside a wiring closet. In a geographic VLAN structure, it is typical to find 80 percent of the traffic remote to the user (server farms and so on) and 20 percent of the traffic local to the user (local server, printers, and so on).

Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 93

QUESTION NO: 26

What are some virtues of implementing end-to-end VLANs? (Choose two)

- A. End-to-end VLANs are easy to manage.
- B. Users are grouped into VLANs independent of a physical location.
- C. Each VLAN has a common set of security and resource requirements for all members.
- D. Resources are restricted to a single location.

Answer: B,C

Explanation:

In an end-to-end VLAN, users are grouped into VLANs independent of physical location and dependent on group or job function.

Each VLAN has a common set of security requirements for all members.

QUESTION NO: 27

Which of the following statements is true about the 80/20 rule (Select all that apply)?

- A. 20 percent of the traffic on a network segment should be local
- B. no more than 20 percent of the network traffic should be able to move across a backbone.
- C. no more than 80 percent of the network traffic should be able to move across a backbone.
- D. 80 percent of the traffic on a network segment should be local

Answer: B,D

Explanation:

The 80/20 rule in network design originated from the idea that most of the traffic should remain local to the LAN, since bandwidth is plentiful compared to WAN links, and a great deal of broadcast traffic that is evident at the LAN is not passed over the backbone.

Note: With the availability of inexpensive bandwidth and centralized data centers, this rule appears to have become obsolete. In fact, most networks have taken on the 20/80 rules, as opposed to the legacy 80/20 rule.

QUESTION NO: 28

What are three results of issuing the switchport host command? (Choose three.) Select 3 response(s).

- A. enables PortFast
- B. disables trunking
- C. disables Cisco Discovery Protocol
- D. enables port security
- E. enables loopguard
- F. disables EtherChannel

Answer: A,B,F

Explanation:

Catalyst 6500 switches running Cisco IOS software support the macro command switchport host. The switchport host macro command was designed to facilitate the configuration of switch ports that connect to end stations. Entering this command sets the switch port mode to access, enables

spanning tree PortFast, and disables channel grouping, all at the same time. The switchport host macro command can be used as an alternative to the switchport mode access command.

Reference:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/sec_chap7.html

QUESTION NO: 29 DRAG DROP

Drag the attributes on the left to the types of VLAN designs that they describe on the right.

Created with physical boundaries in mind rather than the departments or organizations of the users on the end devices.	End-to-End VLANs
VLANs on one switch are not advertised to all other switches in the network, nor do they need to be created in the VLAN database of any other switch.	
As a user moves through a campus, the VLAN membership of the user remains the same, regardless of the physical switch this user attaches to.	
Users are grouped into each VLAN regardless of physical location.	Local VLANs

Answer:

Drag the attributes on the left to the types of VLAN designs that they describe on the right.

Created with physical boundaries in mind rather than the departments or organizations of the users on the end devices.	End-to-End VLANs
VLANs on one switch are not advertised to all other switches in the network, nor do they need to be created in the VLAN database of any other switch.	As a user moves through a campus, the VLAN membership of the user remains the same, regardless of the physical switch this user attaches to.
As a user moves through a campus, the VLAN membership of the user remains the same, regardless of the physical switch this user attaches to.	Users are grouped into each VLAN regardless of physical location.
Users are grouped into each VLAN regardless of physical location.	Local VLANs
	Created with physical boundaries in mind rather than the departments or organizations of the users on the end devices.
	VLANs on one switch are not advertised to all other switches in the network, nor do they need to be created in the VLAN database of any other switch.

Explanation:

End-to-End VLANs

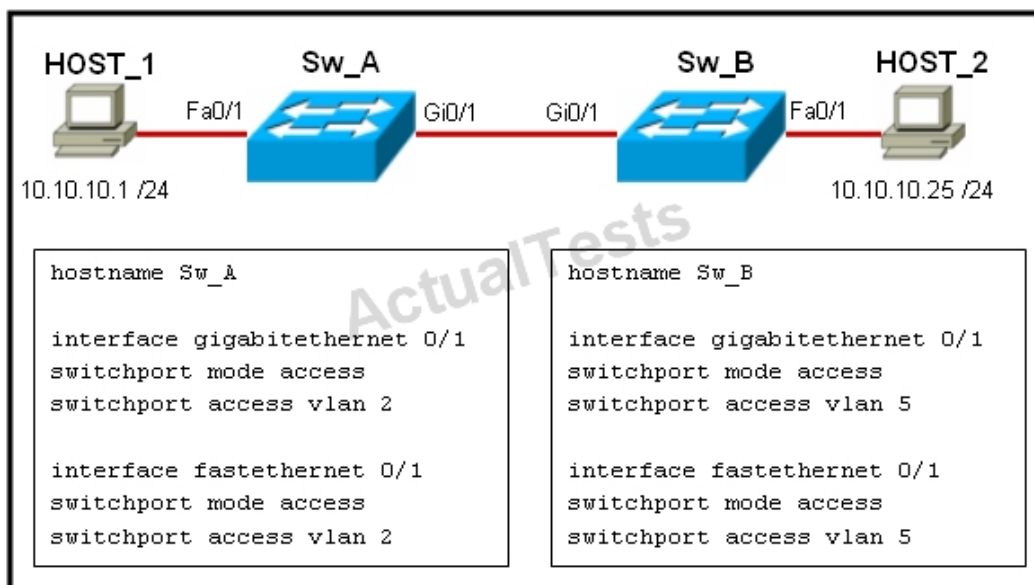
As a user moves through a campus, the VLAN membership of the user remains the same, regardless of the physical switch this user attaches to.

Users are grouped into each VLAN regardless of physical location.

Local VLANs

Created with physical boundaries in mind rather than the departments or organizations of the users on the end devices.

VLANs on one switch are not advertised to all other switches in the network, nor do they need to be created in the VLAN database of any other switch.

QUESTION NO: 30

Given the configurations on SwitchA and SwitchB, which statement is true?

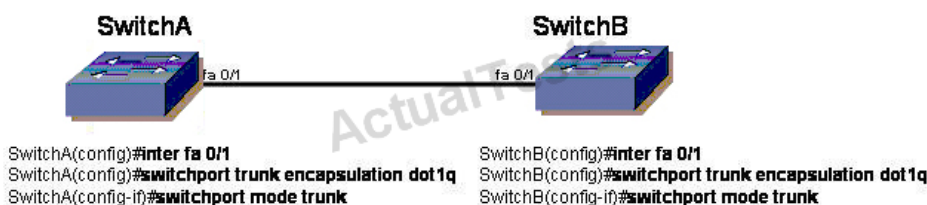
- A.** The link is set to auto-negotiate trunking, and it will automatically become a trunk link unless configured otherwise.
- B.** The link is a trunking link and by default all VLANs will be transmitted across this trunk.
- C.** The link is prevented from generating DTP frames, turning the Negotiation of Trunking off.
- D.** The link is not a trunk link so both interfaces must be on the same VLAN and only that single VLAN is transmitted across the link.

Answer: D

Explanation:

In order for this link to become a trunk, the “switchport trunk encapsulation dot1q” command should be put under the interface fa 0/1 as well as the “switchport mode trunk” command. These ports are configured for VLANS, so as it stands now HOST_1 will not be able to communicate with HOST_2.

QUESTION NO: 31



Given the configurations on SwitchA and SwitchB, which two statements are true? (Choose two.)

- A.** The trunk is currently using the ISL trunking protocol.
- B.** The trunk is currently using the 802.1q trunking protocol.
- C.** By default, the trunk can only support one VLAN, and only that single VLAN is transmitted across the trunk.
- D.** By default, all VLANs will be transmitted across this trunk.
- E.** By default, SwitchA and SwitchB's Fast Ethernet 0/1 port will not generate DTP messages.

Answer: B,D

Explanation:

The "switchport mode trunk" command sets the interface to be a trunk, while the "switchport trunk encapsulation dot1q" command specifies that 802.1q should be used, not ISL. By default, all VLANs are allowed to traverse a trunk link. To limit specific VLANs to cross the trunk, VLAN pruning would need to be configured.

QUESTION NO: 32

A network administrator enters the following switch commands:

```
Switch(config)#interface range fa0/0-5
```

```
Switch(config-if-range)#switchport access vlan 2
```

What is the result of these commands?

- A. Two new vlans are created on six switch ports
- B. One new vlan is created on five switch ports
- C. Six new vlans are created on six switch ports
- D. One new vlan is created with the vlan number 2

Answer: D

Explanation:

The interface range command is used to configure the same values across multiple ports. In this case, each interface in the range (fa0/0 to fa0/5) will be assigned to be in VLAN 2.

QUESTION NO: 33

When a VLAN port configured as a trunk receives an untagged frame, what will happen?

- A. The frame will be dropped.
- B. The frame will cause an error message to be sent.
- C. The frame will be processed as a native VLAN frame
- D. The frame will first be tagged, then processed as a native VLAN frame.

Answer: C

Explanation:

If a switch receives untagged frames on a trunk port, they are assumed to be part of the VLAN that are designated on the switchport as the native VLAN.

QUESTION NO: 34

By default, which statement is correct when an IEEE 802.1Q trunk port receives an untagged frame?

- A.** The frame is considered in the native VLAN and forwarded to the ports associated with that VLAN.
- B.** The frame is encapsulated and tagged as in the native VLAN.
- C.** The frame is broadcast on all ports regardless of VLAN association.
- D.** The frame is dropped.

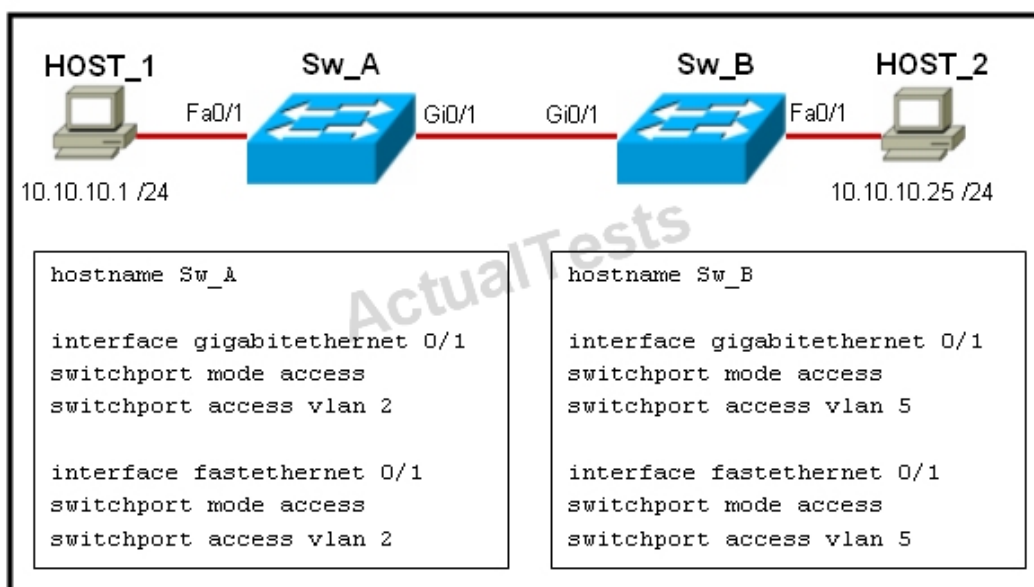
Answer: A

Explanation:

If a switch receives untagged frames on a trunk port, they are assumed to be part of the VLAN that are designated on the switchport as the native VLAN.

QUESTION NO: 35

Refer to the exhibit.



Both host stations are part of the same subnet but are in different VLANs. On the basis of the information presented in the exhibit, which statement is true about an attempt to ping from host to host?

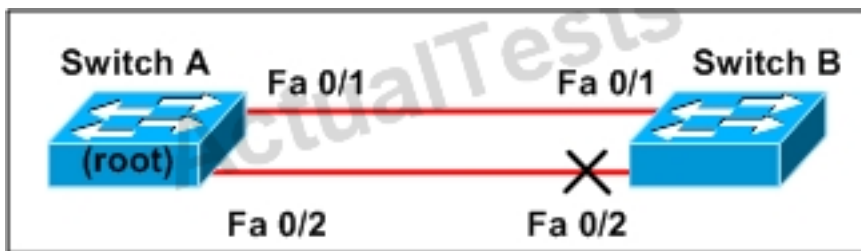
- A. A trunk port will need to be configured on the link between Sw_A and Sw_B for the ping command to be successful.
- B. The two different hosts will need to be in the same VLAN in order for the ping command to be successful.
- C. A Layer 3 device is needed for the ping command to be successful.
- D. The ping command will be successful without any further configuration changes.

Answer: A

Explanation:

In order for hosts in different VLANs to communicate, they must be connected via a trunk link. If the Sw_A and Sw_B link was a trunk, traffic from both VLAN 2 and VLAN 5 would be sent across.

QUESTION NO: 36



Refer to the exhibit. VLAN 1 and VLAN 2 are configured on the trunked links between Switch A and Switch B. Port Fa 0/2 on Switch B is currently in a blocking state for both VLANs. What should be done to load balance VLAN traffic between Switch A and Switch B?

- A. Lower the port priority for VLAN 1 on port 0/1 for Switch A.
- B. Lower the port priority for VLAN 1 on port 0/2 for Switch A.
- C. Make the bridge ID of Switch B lower than the ID of Switch A.
- D. Enable HSRP on the access ports.

Answer: B

Explanation:

Lowering the port priority for VLAN 1 on Switch A will lower the Root Bridge ID for port Fa0/2 on Switch A so then traffic for VLAN 1 will go via the Fa0/2 link.

QUESTION NO: 37

Refer to the exhibit.

```
Switch#show spanning-tree inconsistentports
Name                Interface                Inconsistency
-----
VLAN0001            FastEthernet3/1          Port Type Inconsistent
VLAN0001            FastEthernet3/2          Port Type Inconsistent
VLAN1002            FastEthernet3/1          Port Type Inconsistent
VLAN1002            FastEthernet3/2          Port Type Inconsistent
VLAN1003            FastEthernet3/1          Port Type Inconsistent
VLAN1003            FastEthernet3/2          Port Type Inconsistent
VLAN1004            FastEthernet3/1          Port Type Inconsistent
VLAN1004            FastEthernet3/2          Port Type Inconsistent
VLAN1005            FastEthernet3/1          Port Type Inconsistent
VLAN1005            FastEthernet3/2          Port Type Inconsistent
Number of inconsistent ports (segments) in the system :10
```

What information can be derived from the output?

- A.** Interfaces FastEthernet3/1 and FastEthernet3/2 are connected to devices that are sending BPDUs with a superior root bridge parameter and no traffic is forwarded across the ports. After the sending of BPDUs has stopped, the interfaces must be shut down administratively, and brought back up, to resume normal operation.
- B.** Devices connected to interfaces FastEthernet3/1 and FastEthernet3/2 are sending BPDUs with a superior root bridge parameter, but traffic is still forwarded across the ports.
- C.** Devices connected to interfaces FastEthernet3/1 and FastEthernet3/2 are sending BPDUs with a superior root bridge parameter and no traffic is forwarded across the ports. After the inaccurate BPDUs have been stopped, the interfaces automatically recover and resume normal operation.
- D.** Interfaces FastEthernet3/1 and FastEthernet3/2 are candidates for becoming the STP root port, but neither can realize that role until BPDUs with a superior root bridge parameter are no longer received on at least one of the interfaces.

Answer: C

Explanation: Root guard is configured on a per-port basis. If a superior BPDU is received on the port, root guard does not take the BPDU into account and so puts the port into a root-inconsistent state. When devices connected on FastEthernet3/1 and FastEthernet3/2 stops sending superior BPDUs, the port will be unblocked again and will transition through STP states like any other port.

Reference:

http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00800ae96b.shtml

QUESTION NO: 38

What are three results of issuing the switchport host command? (Choose three.)

- A. disables EtherChannel
- B. enables port security
- C. disables Cisco Discovery Protocol
- D. enables PortFast
- E. disables trunking
- F. enables loopguard

Answer: A,D,E

Explanation:

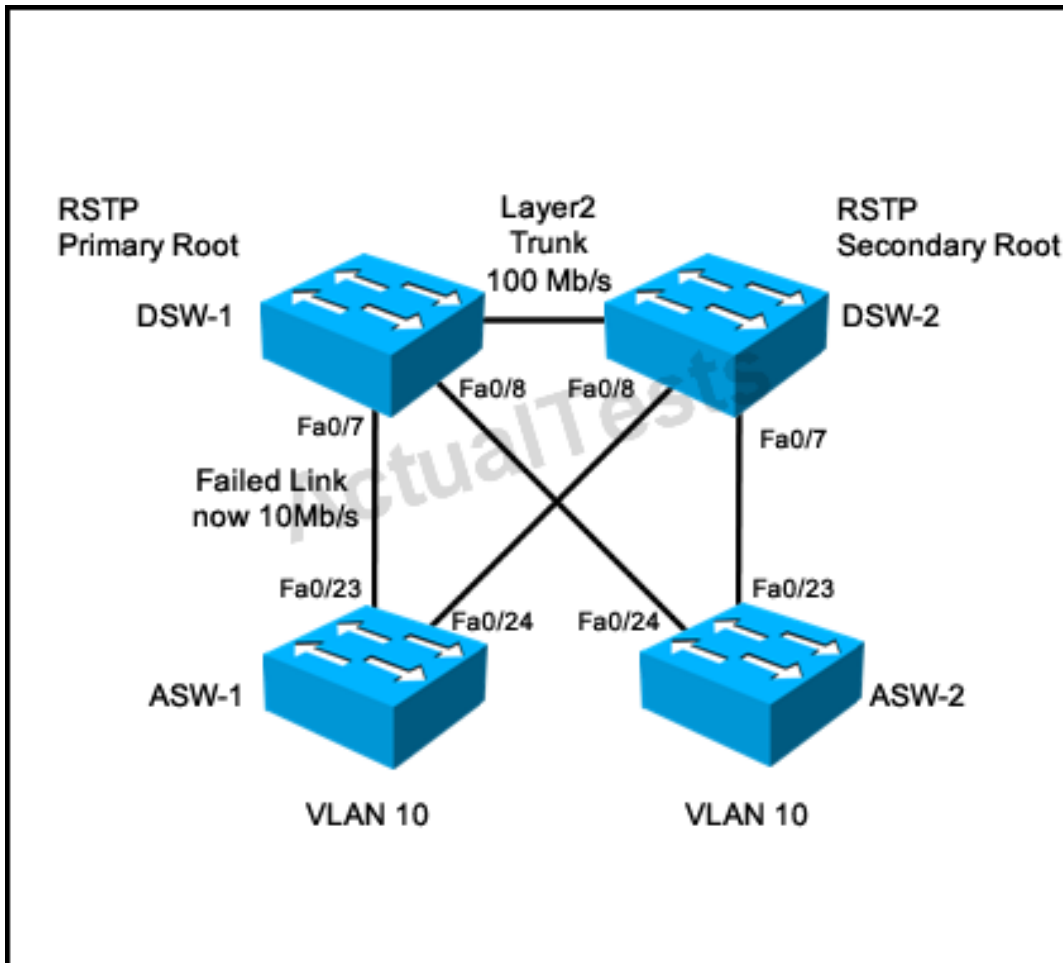
The switchport host command disables channeling, enables spanning-tree portfast and enables the switchport nonegotiate command to turn off DTP negotiation packets.

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a008015bfd6.shtml#hostfix

QUESTION NO: 39

Refer to the exhibit.



All links in this network are layer 2, fast Ethernet 100 Mb/s and operating as trunks. After a failure, the link between ASW-1 and DSW-1 has incorrectly come back up at 10Mb/s although it is connected.

Which one of the following will occur as a result of this failure?

- A. There will be no change to the forwarding path of traffic from ASW-1
- B. ASW1 will block Fa0/24 in order to maintain the shortest path to the root bridge DSW-1
- C. ASW-1 will block Fa0/23 in order to maintain the shortest path to the root bridge DSW-1
- D. ASW-1 will elect DSW-2 as the root primary since it is closer than DSW-1

Answer: C

Explanation:

ASW1 will block Fa0/24 to maintain shortest path to the root bridge DSW1

QUESTION NO: 40

What is the result of entering the command spanning-tree loopguard default?

- A. The command enables loop guard and root guard.
- B. The command changes the status of loop guard from the default of disabled to enabled.
- C. The command activates loop guard on point-to-multipoint links in the switched network.
- D. The command disables EtherChannel guard.

Answer: B

Explanation:

By default, loop guard is disabled on all switch ports. You can enable loop guard as a global default, affecting all switch ports, with the following global configuration command:

```
Switch(config)# spanning-tree loopguard default
```

You also can enable or disable loop guard on a specific switch port by using the following interface-configuration command:

```
Switch(config-if)# [no] spanning-tree guard loop
```

Although loop guard is configured on a switch port, its corrective blocking action is taken on a per-VLAN basis. In other words, loop guard doesn't block the entire port; only the offending VLANs are blocked. You can enable loop guard on all switch ports, regardless of their functions. The switch figures out which ports are nondesignated and monitors the BPDU activity to keep them nondesignated. Nondesignated ports are generally the root port, alternate root ports, and ports that normally are blocking.

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/stp_enha.html#wp1033825

QUESTION NO: 41

What is the effect of applying the switchport trunk encapsulation dot1q command to a port on a Cisco Catalyst switch?

- A. By default, native VLAN packets going out this port are tagged.
- B. Without an encapsulation command, 802.1Q is the default encapsulation if DTP fails to

negotiate a trunking protocol.

C. The interface supports the reception of tagged and untagged traffic.

D. If the device connected to this port is not 802.1Q-enabled, it is unable to handle 802.1Q packets.

Answer: C

Explanation:

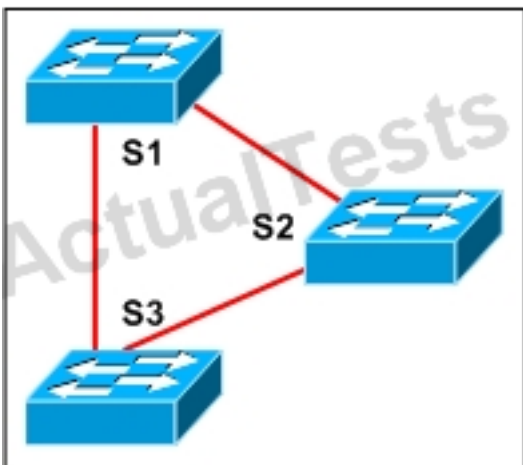
Catalyst trunk port can use two types of encapsulation: 802.1q and ISL. The command `switchport trunk encapsulation dot1q` selects the first type. Reference:

http://www.cisco.com/en/US/tech/tk389/tk689/technologies_configuration_example09186a008009441a.shtml

http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094665.shtml

QUESTION NO: 42

Refer to the exhibit.



Switch S1 has been configured with the command `spanning-tree mode rapid-pvst`. Switch S3 has been configured with the command `spanning-tree mode mst`. Switch S2 is running the IEEE 802.1D instance of Spanning Tree. What is the result?

- A.** IEEE 802.1w and IEEE 802.1s are compatible. IEEE 802.1d is incompatible. Switches S1 and S3 can pass traffic between themselves. Neither can pass traffic to switch S2.
- B.** Switches S1, S2, and S3 can pass traffic between themselves.
- C.** Switches S1, S2, and S3 can pass traffic between themselves. However, if the topology is changed, switch S2 does not receive notification of the change.
- D.** IEEE 802.1d, IEEE 802.1w, and IEEE 802.1s are incompatible. All three switches must use the

same standard or no traffic can pass between any of the switches.

Answer: B

Explanation:

A switch running both MSTP and RSTP supports a built-in protocol migration mechanism that enables it to interoperate with legacy 802.1D switches. If this switch receives a legacy 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only 802.1D BPDUs on that port. An MST switch can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (version 3) associated with a different region, or an RST BPDU (version 2).

However, the switch does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs because it cannot determine whether the legacy switch has been removed from the link unless the legacy switch is the designated switch

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swmstp.htm

QUESTION NO: 43

Which statement about 802.1Q trunking is true?

- A. Both switches must be in the same VTP domain.
- B. The encapsulation type on both ends of the trunk does not have to match.
- C. The native VLAN on both ends of the trunk must be VLAN 1.
- D. In 802.1Q trunking, all VLAN packets are tagged on the trunk link, except the native VLAN.

Answer: D

Explanation:

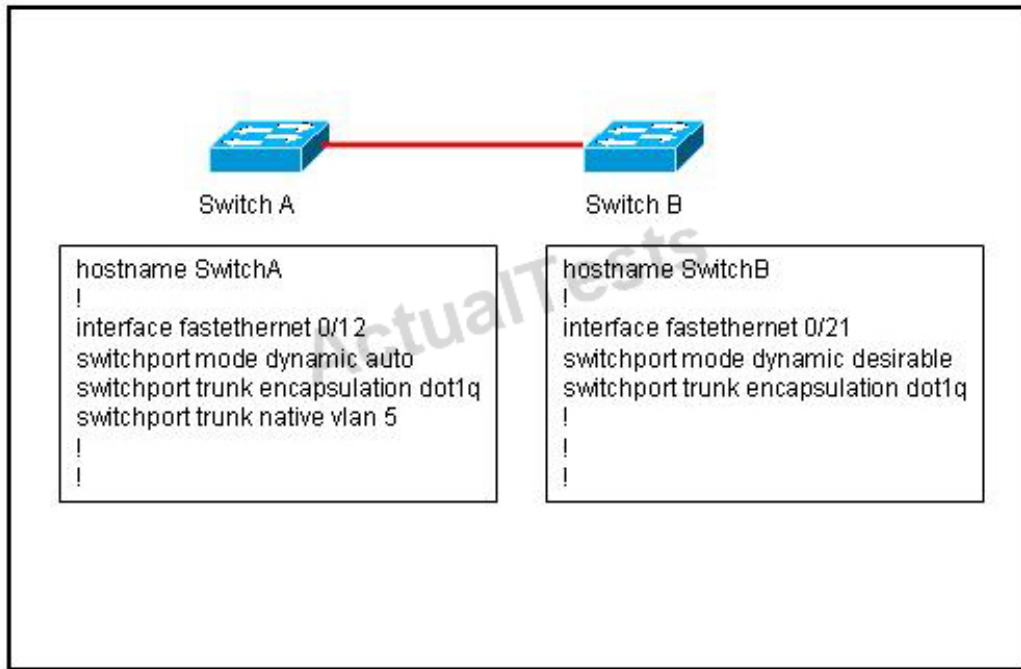
E is correct because, "frames from the native VLAN of an 802.1Q trunk are not tagged with the VLAN number."

Reference:

<http://www.cisco.com/warp/public/473/27.html>

QUESTION NO: 44

Refer to the exhibit.



Which three statements are true? (Choose three.)

- A. A trunk link will be formed.
- B. Only VLANs 1-1001 will travel across the trunk link.
- C. The native VLAN for switch B is VLAN 1.
- D. DTP is not running on switch A.
- E. DTP packets are sent from switch B.

Answer: A,C,E

Explanation:

You can manually configure trunk links on Catalyst switches for either ISL or 802.1Q mode. In addition, Cisco has implemented a proprietary, point-to-point protocol called Dynamic Trunking Protocol (DTP) that negotiates a common trunking mode between two switches. The negotiation covers the encapsulation (ISL or 802.1Q) as well as whether the link becomes a trunk at all. You can configure the trunk encapsulation with the `switchport trunk encapsulation` command, as one of the following:

- `isl`—VLANs are tagged by encapsulating each frame using the Cisco ISL protocol.
- `dot1q`—VLANs are tagged in each frame using the IEEE 802.1Q standard protocol. The only exception is the native VLAN, which is sent normally and not tagged at all.
- `negotiate` (the default)—The encapsulation is negotiated to select either ISL or IEEE 802.1Q, whichever is supported by both ends of the trunk. If both ends support both types, ISL is favored. (The Catalyst 2950 switch does not support ISL encapsulation.)

In the `switchport mode` command, you can set the trunking mode to any of the following:

- `trunk`—This setting places the port in permanent trunking mode. The corresponding switch port at the other end of the trunk should be similarly configured because negotiation is not allowed. You should also manually configure the encapsulation mode.

- dynamic desirable (the default)—The port actively attempts to convert the link into trunking mode. If the far-end switch port is configured to trunk, dynamic desirable, or dynamic auto mode, trunking is successfully negotiated.
- dynamic auto—The port converts the link into trunking mode. If the far-end switch port is configured to trunk or dynamic desirable, trunking is negotiated. Because of the passive negotiation behavior, the link never becomes a trunk if both ends of the link are left to the dynamic auto default.

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_25_se/configuration/guide/swvlan.html#wp1100014

QUESTION NO: 45

The Company LAN is becoming saturated with broadcasts and multicast traffic. What could you do to help a network with many multicasts and broadcasts?

- A. Creating smaller broadcast domains by implementing VLANs.
- B. Separate nodes into different hubs.
- C. Creating larger broadcast domains by implementing VLANs.
- D. Separate nodes into different switches.
- E. All of the above.

Answer: A

Explanation:

Controlling broadcast propagation throughout the network is important to reduce the amount of overhead associated with these frames. Routers, which operate at Layer 3 of the OSI model, provide broadcast domain segmentation for each interface. Switches can also provide broadcast domain segmentation using virtual LANs (VLANs). A VLAN is a group of switch ports, within a single or multiple switches, that is defined by the switch hardware and/or software as a single broadcast domain. A VLANs goal is to group devices connected to a switch into logical broadcast domains to control the effect that broadcasts have on other connected devices. A VLAN can be characterized as a logical network.

Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 8

QUESTION NO: 46

You are the network administrator tasked with designing a switching solution for the Company

network. Which of the following statements describing trunk links are INCORRECT? (Select all that apply)

- A. The trunk link belongs to a specific VLAN.
- B. Multiple trunk links are used to connect multiple end user devices.
- C. A trunk link only supports native VLAN.
- D. Trunk links use 802.1Q to identify a VLAN.
- E. The native VLAN of the trunk link is the VLAN that the trunk uses for untagged packets.

Answer: A,B,C,D

Explanation:

A trunk is a point-to-point link that transmits and receives traffic between switches or between switches and routers. Trunks carry the traffic of multiple VLANs and can extend VLANs across an entire network. 100BaseT and Gigabit Ethernet trunks use Cisco ISL (the default protocol) or industry-standard IEEE 802.1Q to carry traffic for multiple VLANs over a single link. Frames received from users in the administratively-defined VLANs are identified or tagged for transmission to other devices. Based on rules you define, a unique identifier (the tag) is inserted in each frame header before it is forwarded. The tag is examined and understood by each device before any broadcasts or transmission to other switches, routers, or end stations. When the frame reaches the last switch or router, the tag is removed before the frame is transmitted to the target end station.

QUESTION NO: 47

Which of the following specifications is a companion to the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) algorithm, and warrants the use multiple spanning-trees?

- A. IEEE 802.1s (MST)
- B. IEEE 802.1Q (CST)
- C. Cisco PVST+
- D. IEEE 802.1d (STP)
- E. None of the other alternatives apply

Answer: A

Explanation:

MST uses the modified RSTP version called the Multiple Spanning Tree Protocol (MSTP). MST extends the IEEE 802.1w rapid spanning tree (RST) algorithm to multiple spanning trees. This extension provides both rapid convergence and load balancing in a VLAN environment. MST converges faster than PVST+. MST is backward compatible with 802.1D STP, 802.1w (rapid spanning tree protocol [RSTP]), and the Cisco PVST+ architecture.

MST allows you to build multiple spanning trees over trunks. You can group and associate VLANs

to spanning tree instances. Each instance can have a topology independent of other spanning tree instances. This new architecture provides multiple forwarding paths for data traffic and enables load balancing. Network fault tolerance is improved because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).

In large networks, you can more easily administer the network and use redundant paths by locating different VLAN and spanning tree instance assignments in different parts of the network. A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments. You must configure a set of bridges with the same MST configuration information, which allows them to participate in a specific set of spanning tree instances. Interconnected bridges that have the same MST configuration are referred to as an *MST region*.

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007e71a.html#wp1082480

QUESTION NO: 48

Which of the following specification will allow you to: associate VLAN groups to STP instances so you can provide multiple forwarding paths for data traffic and enable load balancing?

- A. IEEE 802.1d (STP)
- B. IEEE 802.1s (MST)
- C. IEEE 802.1Q (CST)
- D. IEEE 802.1w (RSTP)

Answer: B

Explanation:

IEEE 802.1s MST Overview

MST extends the IEEE 802.1w rapid spanning tree (RST) algorithm to multiple spanning trees. This extension provides both rapid convergence and load balancing in a VLAN environment. MST converges faster than PVST+. MST is backward compatible with 802.1D STP, 802.1w (rapid spanning tree protocol [RSTP]), and the Cisco PVST+ architecture.

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007e71a.html#1050594

QUESTION NO: 49

Which two statements correctly describe VTP? (Choose two.)

- A. Transparent mode always has a configuration revision number of 0.
- B. Transparent mode cannot modify a VLAN database.
- C. Client mode cannot forward received VTP advertisements.
- D. Client mode synchronizes its VLAN database from VTP advertisements.
- E. Server mode can synchronize across VTP domains.

Answer: A,D

Explanation:

VTP enabled switch resets revision number to 0 when VTP mode is set to transparent. The switch in the both client and server mode synchronizes its VLAN database from VTP advertisements.

Reference:

http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080890613.shtml

QUESTION NO: 50

Which two DTP modes permit trunking between directly connected switches? (Choose two.)

- A. dynamic desirable (VTP domain A) to dynamic desirable (VTP domain A)
- B. dynamic desirable (VTP domain A) to dynamic desirable (VTP domain B)
- C. dynamic auto (VTP domain A) to dynamic auto (VTP domain A)
- D. dynamic auto (VTP domain A) to dynamic auto (VTP domain B)
- E. dynamic auto (VTP domain A) to nonegotiate (VTP domain A)
- F. nonegotiate (VTP domain A) to nonegotiate (VTP domain B)

Answer: A,F

Explanation: There are three DTP modes of operation:

- Trunk
- Dynamic desirable
- Dynamic auto

For dynamic trunking to be successful VTP domain names at the both sides of the trunk must matches. Also DTP could be switched off by the command switchport nonegotiate. In the later case the matching of VTP domain names is not required. From the three DTP modes the one (the dynamic auto) is passive. The trunk will not be created if at the both sides passive mode is used.

Reference:

QUESTION NO: 51

Which two RSTP port roles include the port as part of the active topology? (Choose two.)

- A. root
- B. designated
- C. alternate
- D. backup
- E. forwarding
- F. learning

Answer: A,B

Explanation:

RSTP defines four port roles:

- Root port
- Designated port
- Alternate port
- Backup port and three port states:
 - Discarding
 - Learning
 - Forwarding

Only the root ports and designated ports belong to the active STP topology.

Reference:

http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfa.shtml

QUESTION NO: 52

Which two statements correctly describe characteristics of the PortFast feature? (Choose two.)

- A. STP is disabled on the port.
- B. PortFast can also be configured on trunk ports.
- C. PortFast is needed to enable port-based BPDU guard.
- D. PortFast is used for STP and RSTP host ports.

E. PortFast is used for STP-only host ports.

Answer: B,D

Explanation:

Catalyst switches offer the PortFast feature, which shortens the Listening and Learning states to a negligible amount of time. When a workstation link comes up, the switch immediately moves the PortFast port into the Forwarding state. Spanning-tree loop detection is still in operation, however, and the port moves into the Blocking state if a loop is ever detected on the port. You can use PortFast to connect a single end station or a switch port to a switch port. If you enable PortFast on a port that is connected to another Layer 2 device, such as a switch, you might create network loops. When PortFast is enabled between two switches, the system will verify that there are no loops in the network before bringing the blocking trunk to a forwarding state.

Reference:

http://www.cisco.com/en/US/docs/routers/7600/ios/12.1E/configuration/guide/stp_enha.html#wp1042489

QUESTION NO: 53

Which statement correctly describes the Cisco implementation of RSTP?

- A. PortFast, UplinkFast, and BackboneFast specific configurations are ignored in Rapid PVST mode.
- B. RSTP is enabled globally and uses existing STP configuration.
- C. Root and alternative ports transition immediately to the forwarding state.
- D. Convergence is improved by using subsecond timers for the blocking, listening, learning, and forwarding port states.

Answer: B

Explanation: By default, a switch operates in Per-VLAN Spanning Tree Plus (PVST+) mode using traditional 802.1D STP. Therefore, RSTP cannot be used until a different spanning-tree mode (MST or RPVST+) is enabled. Remember that RSTP is just the underlying mechanism that a spanning-tree mode can use to detect topology changes and converge a network into a loop-free topology.

Reference:

http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfa.shtml

QUESTION NO: 54

You are the administrator of a switch and currently all host-connected ports are configured with the portfast command. You have received a new directive from your manager that states that, in the future, any host-connected port that receives a BPDU should automatically disable PortFast and begin transmitting BPDUs. Which command will support this new requirement?

- A. Switch(config)#spanning-tree portfast bpduguard default
- B. Switch(config-if)#spanning-tree bpduguard enable
- C. Switch(config-if)#spanning-tree bpdufilter enable
- D. Switch(config)#spanning-tree portfast bpdufilter default

Answer: D

Explanation:

When spanning-tree bpdufilter enable either on interface configuration or on global configuration mode prevents from sending or receiving Bridge Protocol Data Units on portfast enabled interface.

To enable bpdufilter global configuration mode:

Device1(Config)#spanning-tree portfast bpdufilter default

Be careful when enabling BPDU filtering. Functionality is different when enabling on a per-port basis or globally. When enabled globally, BPDU filtering is applied only on ports that are in an operational PortFast state. Ports still send a few BPDUs at linkup before they effectively filter outbound BPDUs. If a BPDU is received on an edge port, it immediately loses its operational PortFast status and BPDU filtering is disabled.

Reference:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.1E/native/command/reference/S1.html#wp1180453>

QUESTION NO: 55

A port in a redundant topology is currently in the blocking state and is not receiving BPDUs. To ensure that this port does not erroneously transition to the forwarding state, which command should be configured?

- A. Switch(config)#spanning-tree loopguard default
- B. Switch(config-if)#spanning-tree bdpufilter

- C. Switch(config)#udld aggressive
- D. Switch(config-if)#spanning-tree bpduguard

Answer: A

Explanation: The STP loop guard feature provides additional protection against Layer 2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the STP blocking port) no longer receives STP BPDUs. In its operation, STP relies on continuous reception or transmission of BPDUs based on the port role. The designated port transmits BPDUs, and the non-designated port receives BPDUs. When one of the ports in a physically redundant topology no longer receives BPDUs, the STP conceives that the topology is loop free. Eventually, the blocking port from the alternate or backup port becomes designated and moves to a forwarding state. This situation creates a loop. The loop guard feature makes additional checks. If BPDUs are not received on a non-designated port, and loop guard is enabled, that port is moved into the STP loop-inconsistent blocking state, instead of the listening / learning / forwarding state. Without the loop guard feature, the port assumes the designated port role. The port moves to the STP forwarding state and creates a loop.

Reference:

http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a0080094640.shtml#loop_guard

QUESTION NO: 56

Which command can be issued without interfering with the operation of loop guard?

- A. Switch(config-if)#spanning-tree guard root
- B. Switch(config-if)#spanning-tree portfast
- C. Switch(config-if)#switchport mode trunk
- D. Switch(config-if)#switchport mode access

Answer: C

Explanation:

The spanning-tree guard root cannot be enabled together with loop guard. The loop guard feature is supposed to be used on the port receiving BPDU and guard root will shutdown the port as soon as the first BPDU comes to that port.

Configuring portfast on the port connected to the other switch can create temporal loop.

Configuring access mode on the port can filter BPDU from other VLANs from coming to the port and force loop guard feature to put this port into error-disabled state.

So the only command that can be issued without interfering with the operation of loop guard is "switchport mode trunk".

Reference:

http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a0080094640.shtml

QUESTION NO: 57

Which statement is a characteristic of multi-VLAN access ports?

- A. The port has to support STP PortFast.
- B. The auxiliary VLAN is for data service and is identified by the PVID.
- C. The port hardware is set as an 802.1Q trunk.
- D. The voice service and data service use the same trust boundary.

Answer: C

Explanation:

The integration of 802.1x and IP phones is based on the switch configuration of multi-VLAN access ports. Multi-VLAN ports belong to two VLANs: native VLAN (PVID) and auxiliary VLAN (VVID). This allows the separation of voice and data traffic and enables 802.1x authentication only on the PVID.

Reference:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/20ew/configuration/guide/voice.html>

QUESTION NO: 58

Which two statements are true about recommended practices that are to be used in a local VLAN solution design where layer 2 traffic is to be kept to a minimum? (Choose two.)

- A. Routing should occur at the access layer if voice VLANs are utilized. Otherwise, routing should occur at the distribution layer.
- B. Routing may be performed at all layers but is most commonly done at the core and distribution layers.
- C. Routing should not be performed between VLANs located on separate switches.

- D. VLANs should be local to a switch.
- E. VLANs should be localized to a single switch unless voice VLANs are being utilized.

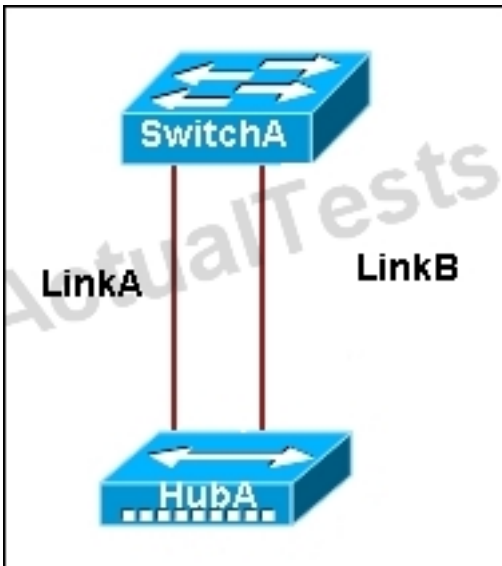
Answer: B,D

Explanation:

Routing is performed at all layers but it is most commonly done at the core and distribution layers. Secondly, the VLANs should be local to a switch.

QUESTION NO: 59

Refer to the exhibit.



BPDUGuard is enabled on both ports of SwitchA. Initially, LinkA is connected and forwarding traffic. A new LinkB is then attached between SwitchA and HubA. Which two statements about the possible result of attaching the second link are true? (Choose two.)

- A. The switch port attached to LinkB does not transition to up.
- B. One or both of the two switch ports attached to the hub goes into the err-disabled state when a BPDU is received.
- C. Both switch ports attached to the hub transitions to the blocking state.
- D. A heavy traffic load could cause BPDU transmissions to be blocked and leave a switching loop.
- E. The switch port attached to LinkA immediately transitions to the blocking state.

Answer: B,D

Explanation:

we know that there will have only one Designated port for each segment (notice that the two ports of SwitchA are on the same segment as they are connected to a hub). The other port will be in Blocking state. But how does SwitchA select its Designated and Blocking port? The decision process involves the following parameters inside the BPDU:

- * Lowest path cost to the Root
- * Lowest Sender Bridge ID (BID)
- * Lowest Port ID

In this case, both interfaces of SwitchA have the same "path cost to the root" and "sender bridge ID" so the third parameter "lowest port ID" will be used. Suppose two interfaces of SwitchA are fa0/1 & fa0/2 then SwitchA will select fa0/1 as its Designated port (because fa0/1 is inferior to fa0/2) -> B is correct.

Suppose the port on LinkA (named portA) is in forwarding state and the port on LinkB (named portB) is in blocking state. In blocking state, port B still listens to the BPDUs. If the traffic passing through LinkA is too heavy and the BPDUs can not reach portB, portB will move to listening state (after 20 seconds for STP) then learning state (after 15 seconds) and forwarding state (after 15 seconds). At this time, both portA & portB are in forwarding state so a switching loop will occur -> D is correct.

QUESTION NO: 60

What action should a network administrator take to enable VTP pruning on an entire management domain?

- A. Enable VTP pruning on any client switch in the domain.
- B. Enable VTP pruning on every switch in the domain.
- C. Enable VTP pruning on any switch in the management domain.
- D. Enable VTP pruning on a VTP server in the management domain.

Answer: D

Explanation:

Enabling VTP pruning on a VTP server allows pruning for the entire management domain. Enabling this on the VTP server will mean that the VTP pruning configuration will be propagated to all VTP client switches within the domain. VTP pruning takes effect several seconds after you enable it. By default, VLANs 2 through 1000 are pruning-eligible.

Reference:

Building Cisco Multilayer Switched Networks (Cisco Press) page 117

http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml#vtp_pruning

QUESTION NO: 61

How does VTP pruning enhance network bandwidth?

- A. by restricting unicast traffic across VTP domains
- B. by reducing unnecessary flooding of traffic to inactive VLANs
- C. by limiting the spreading of VLAN information
- D. by disabling periodic VTP updates

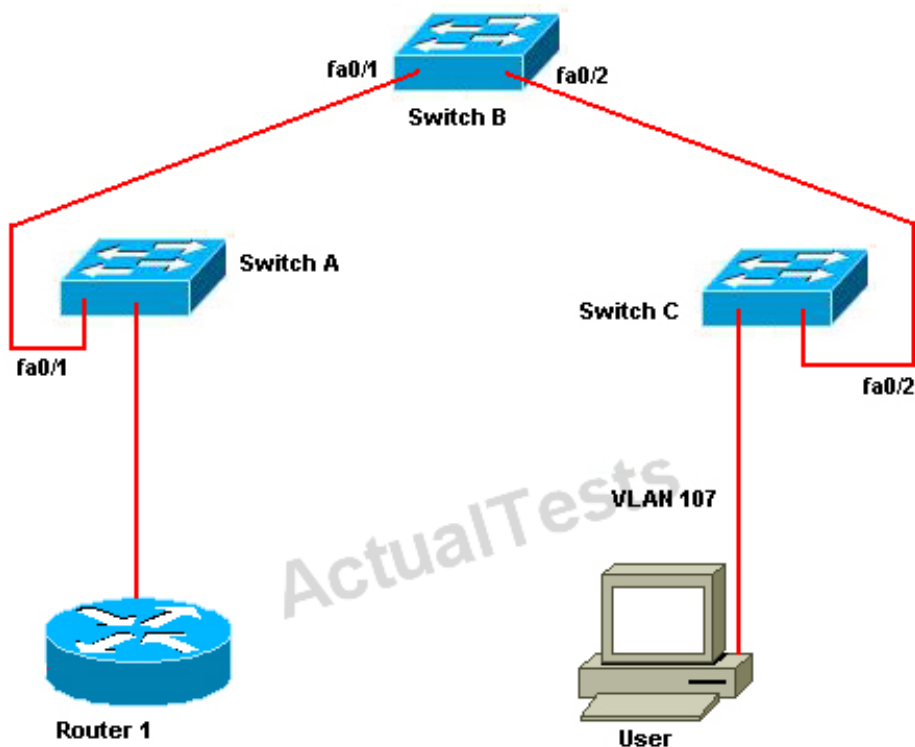
Answer: B

Explanation:

VTP Pruning makes more efficient use of trunk bandwidth by forwarding broadcast and unknown unicast frames on a VLAN only if the switch on the receiving end of the trunk has ports in that VLAN.

QUESTION NO: 62

Refer to the exhibit.



Use the following information from switch A:

Port	Mode	Encapsulation	Status	Native VLAN
fa0/1	desirable	n-802.1q	trunking	5
Port fa0/1	VLANs allowed on trunk 1-100, 102-1005			
Port fa0/1	VLANs allowed and active in management domain 1-6, 8-100, 102-105, 107-999, 1002-1005			
Port fa0/1	VLANs in spanning tree forwarding state and not pruned 1-6, 8-100, 102-105, 108-999, 1002-1005			

The network operations center has received a call stating that users in VLAN 107 are unable to access resources through router 1. What is the cause of this problem?

- A. VLAN 107 does not exist on switch A.
- B. VTP is pruning VLAN 107.
- C. VLAN 107 is not configured on the trunk.
- D. Spanning tree is not enabled on VLAN 107.

Answer: B

Explanation:

In this example, VLAN 7, 101, 106, and 107 are being pruned. VLAN 107 is being pruned incorrectly in this case. By disabling VTP pruning, VLAN 107 should be able to once again gain access to the network resources.

Reference:

http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml#vtp_pruning

QUESTION NO: 63

What two things occur when an RSTP edge port receives a BPDU? (Choose two.)

- A. The port immediately transitions to the forwarding state.
- B. The switch generates a Topology Change Notification BPDU.
- C. The port immediately transitions to the err-disable state.
- D. The port becomes a normal STP switch port.

Answer: B,D

Explanation:

Edge ports are used to connect Workstations to a switch. There are not supposed to receive STP BPDU. When BPDU comes to edge port the port becomes a normal STP switch port and generate TCN BPDU.

Reference:

CCNP Self-Study CCNP BCMSN Official Exam Certification Guide, Fourth Edition, Chapter 10: Protecting the Spanning Tree Protocol Topology, p. 248.

QUESTION NO: 64

What is the effect of configuring the following command on a switch?

Switch(config) # spanning-tree portfast bpduguard default

- A. If BPDUs are received by a port configured for PortFast, then PortFast is disabled and the BPDUs are processed normally.
- B. If BPDUs are received by a port configured for PortFast, they are ignored and none are sent.
- C. If BPDUs are received by a port configured for PortFast, the port transitions to the forwarding state.

D. The command enables BPDU filtering on all ports regardless of whether they are configured for BPDU filtering at the interface level.

Answer: A

Explanation:

Ordinarily, STP operates on all switch ports in an effort to eliminate bridging loops before they can form. BPDUs are sent on all switch ports—even ports where PortFast has been enabled. BPDUs also can be received and processed if any are sent by neighboring switches. You always should allow STP to run on a switch to prevent loops. However, in special cases when you need to prevent BPDUs from being sent or processed on one or more switch ports, you can use BPDU filtering to effectively disable STP on those ports. By default, BPDU filtering is disabled on all switch ports. You can configure BPDU filtering as a global default, affecting all switch ports with the following global configuration command:

```
Switch(config)# spanning-tree portfast bpdupfilter default
```

All ports that have PortFast enabled also have BPDU filtering automatically enabled. You also can enable or disable BPDU filtering on specific switch ports by using the following interface configuration command:

```
Switch(config-if)# spanning-tree bpdupfilter {enable | disable}
```

Be careful when enabling BPDU filtering. Functionality is different when enabling on a per-port basis or globally. When enabled globally, BPDU filtering is applied only on ports that are in an operational PortFast state. Ports still send a few BPDUs at linkup before they effectively filter outbound BPDUs. If a BPDU is received on an edge port, it immediately loses its operational PortFast status and BPDU filtering is disabled.

Reference:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.1E/native/command/reference/S1.html#wp1180453>

QUESTION NO: 65

Which statement correctly describes enabling BPDU guard on an access port that is also enabled for PortFast?

A. Upon startup, the port transmits 10 BPDUs. If the port receives a BPDU, PortFast and BPDU guard are disabled on that port and it assumes normal STP operation.

- B. The access port ignores any received BPDU.
- C. If the port receives a BPDU, it is placed into the error-disable state.
- D. BPDU guard is configured only globally and the BPDU filter is required for port-level configuration.

Answer: C

Explanation:

When enabled on a port, BPDU Guard shuts down a port that receives a BPDU. When configured globally, BPDU Guard is only effective on ports in the operational PortFast state. In a valid configuration, PortFast Layer 2 LAN interfaces do not receive BPDUs. Reception of a BPDU by a PortFast Layer 2 LAN interface signals an invalid configuration, such as connection of an unauthorized device. BPDU Guard provides a secure response to invalid configurations, because the administrator must manually put the Layer 2 LAN interface back in service. With release 12.1(11b)E, BPDU Guard can also be configured at the interface level. When configured at the interface level, BPDU Guard shuts the port down as soon as the port receives a BPDU, regardless of the PortFast configuration.

Reference:

http://www.cisco.com/en/US/docs/routers/7600/ios/12.1E/configuration/guide/stp_enha.html#wp1020395

QUESTION NO: 66 DRAG DROP

Place the DTP mode with its correct description.

Trunk	specifies that DTP packets are not sent out this interface
Nonegotiate	sets the switch port to trunk mode and negotiates to become a trunk
Access	sets a switch port to permanent nontrunking mode
Dynamic Auto	sets the switch port to respond, but not actively send DTP frames
Dynamic Desirable	makes the interface actively attempt to convert the link to a trunk link

Answer:

Place the DTP mode with its correct description.

Trunk	Nonegotiate
Nonegotiate	Trunk
Access	Access
Dynamic Auto	Dynamic Auto
Dynamic Desirable	Dynamic Desirable

Explanation:

1) Trunk: Set the switch port to trunk mode and negotiate to become a trunk. 2) Nonegotiate: Specify that the DTP packets are not sent out of this interface. 3) Access: Set a switch port to permanent nontrunking mode. 4) Dynamic Auto: Set the switch port to respond, but not actively send DTP frames. 5) Dynamic Desirable: Make the interface actively attempt to convert the link to a trunk link. (This means the interface is ready to autonegotiate trunking encapsulation and form a trunk link (using DTP) with a neighbor port in desirable, auto, or on mode.)

Dynamic Trunking Protocol (DTP) is the Cisco-proprietary that actively attempts to negotiate a trunk link between two switches. Below is the switchport modes (or DTP modes) for easy reference:

Mode	Function
Dynamic Auto	Creates the trunk based on the DTP request from the neighboring switch.
Dynamic Desirable	Communicates to the neighboring switch via DTP that the interface would like to become a trunk if the neighboring switch interface is able to become a trunk.
Trunk	Automatically enables trunking regardless of the state of the neighboring switch and regardless of any DTP requests sent from the neighboring switch.
Access	Trunking is not allowed on this port regardless of the state of the neighboring switch interface and regardless of any DTP requests sent from the neighboring switch.
Nonegotiate	Prevents the interface from generating DTP frames. This command can be used only when the interface switchport mode is access or trunk. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

QUESTION NO: 67 DRAG DROP

Drag the port states to their correct description.

blocking	sends and receives BPDUs to determine root, but does not update the MAC address table
listening	does not participate in frame forwarding or in STP
learning	does not participate in frame forwarding
forwarding	sends and receives data frames
disabled	populates the MAC address table, but will not forward user data

Answer:

Drag the port states to their correct description.

blocking	listening
listening	disabled
learning	blocking
forwarding	forwarding
disabled	learning

Explanation:

blocking	forwarding
listening	disabled
learning	

Drag the port states to their correct description.

sends and receives BPDUs, but does not learn MAC addresses	listening	is the root, but does not forward traffic
does not participate in STP	disabled	or in STP
does not forward traffic	blocking	forwarding
sends and receives BPDUs	forwarding	s
populates the MAC address table	learning	will not forward traffic

After the bridges have determined which ports are Root Ports, Designated Ports, and non-Designated Ports, STP is ready to create a loop-free topology. To do this, STP configures Root Ports and Designated Ports to forward traffic. STP sets non-Designated Ports to block traffic. Although Forwarding and Blocking are the only two states commonly seen in a stable network, there are actually five STP states.

This list can be viewed hierarchically in that bridge ports start at the Blocking state and work their way up to the Forwarding state. The Disabled state is the administratively shutdown STP state. It is not part of the normal STP port processing. After the switch is initialized, ports start in the Blocking state. The Blocking state is the STP state in which a bridge listens for BPDUs.

A port in the Blocking state does the following:

- Discards frames received from the attached segment or internally forwarded through switching
- Receives BPDUs and directs them to the system module
- Has no address database
- Does not transmit BPDUs received from the system module
- Receives and responds to network management messages but does not transmit them

If a bridge thinks it is the Root Bridge immediately after booting or in the absence of BPDUs for a certain period of time, the port transitions into the Listening state. The Listening state is the STP state in which no user data is being passed, but the port is sending and receiving BPDUs in an effort to determine the active topology.

A port in the Listening state does the following:

- Discards frames received from the attached segment or frames switched from another port
- Has no address database

- Receives BPDUs and directs them to the system module
- Processes BPDUs received from the system module (Processing BPDUs is a separate action from receiving or transmitting BPDUs)
- Receives and responds to network management messages

It is during the Listening state that the three initial convergence steps take place – elect a Root Bridge, elect Root Ports, and elect Designated Ports. Ports that lose the Designated Port election become non-Designated Ports and drop back to the Blocking state. Ports that remain Designated Ports or Root Ports after 15 seconds – the default Forward Delay STP timer value – progress into the Learning state. The lifetime of the Learning state is also governed by the Forward Delay timer of 15 seconds, the default setting.

The Learning state is the STP state in which the bridge is not passing user data frames but is building the bridging table and gathering information, such as the source VLANs of data frames. As the bridge receives a frame, it places the source MAC address and port into the bridging table. The Learning state reduces the amount of flooding required when data forwarding begins.

A port in the Learning state does the following:

If a port is still a Designated Port or Root Port after the Forward Delay timer expires for the Learning state, the port transitions into the Forwarding state. The Forwarding state is the STP state in which data traffic is both sent and received on a port. It is the “last” STP state. At this stage, it finally starts forwarding user data frames.

A port in the Forwarding state does the following:

Reference:

CCNP BCMSN Official Exam Certification Guide, Fourth Edition, Chapter 8: Traditional Spanning Tree Protocol, IEEE 802.1D Overview, p. 197

QUESTION NO: 68

Which three items are configured in MST configuration submode? (Select three)

- A. Region name
- B. Configuration revision number
- C. VLAN instance map
- D. IST STP BPDU hello timer
- E. CST instance map
- F. PVST+ instance map

Answer: A,B,C

Explanation:

spanning-tree mst configuration:

Use the spanning-tree mst configuration command to enter the MST configuration submode. Use the no form of this command to return to the default MST configuration.

Defaults:

The default value for the MST configuration is the default value for all its parameters:

Usage Guidelines:

The MST configuration consists of three main parameters:

QUESTION NO: 69

By default, all VLANs will belong to which MST instance when using Multiple STP?

- A.** MST00
- B.** MST01
- C.** The last MST instance configured
- D.** None

Answer: A

Explanation:

Recall that the whole idea behind MST is the capability to map multiple VLANs to a smaller number of STP instances. Inside a region, the actual MST instances (MSTIs) exist alongside the IST. Cisco supports a maximum of 16 MSTIs in each region. IST always exists as MSTI number 0, leaving MSTI 1 through 15 available for use. By default all VLANs are belonged to MST00 instance.

QUESTION NO: 70

Which MST configuration statement is correct?

- A.** MST configurations can be propagated to other switches using VTP.
- B.** After MST is configured on a Switch, PVST+ operations will also be enabled by default.
- C.** MST configurations must be manually configured on each switch within the MST region.
- D.** MST configurations only need to be manually configured on the Root Bridge.
- E.** MST configurations are entered using the VLAN Database mode on Cisco Catalyst switches.

Answer: C

Explanation:

MST configuration must be manually be configured on each switch within the MST region.

QUESTION NO: 71

Which trunking protocol inserts a four byte tag into the Ethernet frame and recalculates the CRC value?

- A. VTP
- B. 802.1Q
- C. DTP
- D. ISL

Answer: B

Explanation:

802.1Q is the IEEE standard for tagging frames on a trunk and supports up to 4096 VLANs. In 802.1Q, the trunking device inserts a 4-byte tag into the original frame and re-computes the frame check sequence (FCS) before the device sends the frame over the trunk link.

Reference:

http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094665.shtml

Topic 2, Implement a Security Extension of a Layer 2 solution, given a network design and a set of requirements

QUESTION NO: 72

Which description correctly describes a MAC address flooding attack?

- A. The attacking device crafts ARP replies intended for valid hosts. The MAC address of the attacking device then becomes the destination address found in the Layer 2 frames sent by the valid network device.
- B. The attacking device crafts ARP replies intended for valid hosts. The MAC address of the attacking device then becomes the source address found in the Layer 2 frames sent by the valid network device.
- C. The attacking device spoofs a destination MAC address of a valid host currently in the CAM table. The switch then forwards frames destined for the valid host to the attacking device.

- D.** The attacking device spoofs a source MAC address of a valid host currently in the CAM table. The switch then forwards frames destined for the valid host to the attacking device.
- E.** Frames with unique, invalid destination MAC addresses flood the switch and exhaust CAM table space. The result is that new entries cannot be inserted because of the exhausted CAM table space, and traffic is subsequently flooded out all ports.
- F.** Frames with unique, invalid source MAC addresses flood the switch and exhaust CAM table space. The result is that new entries cannot be inserted because of the exhausted CAM table space, and traffic is subsequently flooded out all ports.

Answer: F

Explanation: A common Layer 2 or switch attack is MAC flooding, resulting in a switch's CAM table overflow, which causes flooding of regular data frames out all switch ports. This attack can be launched for the malicious purpose of collecting a broad sample of traffic or as a denial of service (DoS) attack.

A switch's CAM tables are limited in size and therefore can contain only a limited number of entries at any one time. A network intruder can maliciously flood a switch with a large number of frames from a range of invalid source MAC addresses. If enough new entries are made before old ones expire, new valid entries will not be accepted. Then, when traffic arrives at the switch for a legitimate device that is located on one of the switch ports that was not able to create a CAM table entry, the switch must flood frames to that address out all ports. This has two adverse effects:

- The switch traffic forwarding is inefficient and voluminous.
- An intruding device can be connected to any switch port and capture traffic that is not normally seen on that port.

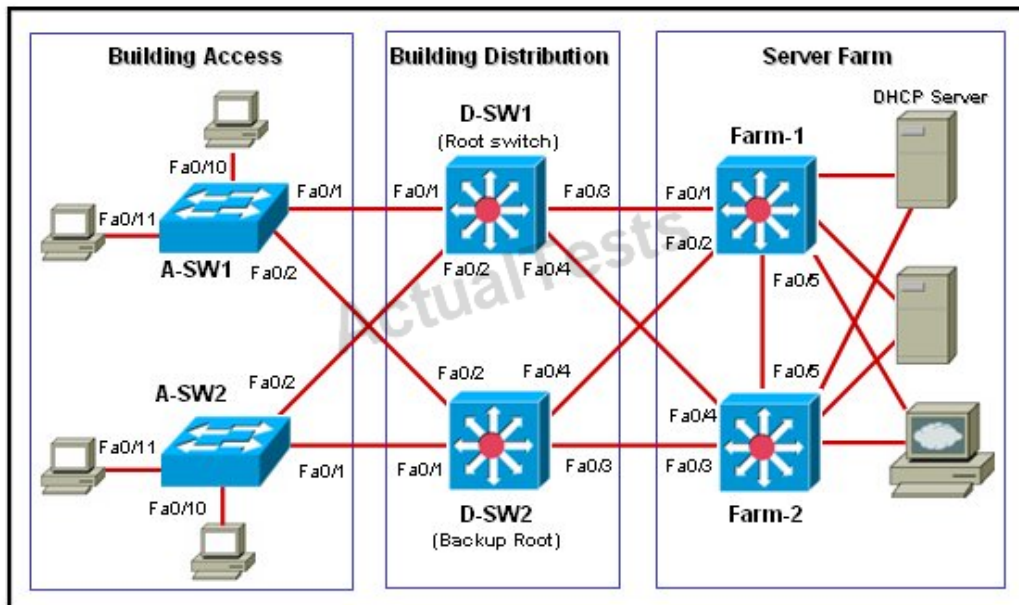
If the attack is launched before the beginning of the day, the CAM table would be full when the majority of devices are powered on. Then frames from those legitimate devices are unable to create CAM table entries as they power on. If this represents a large number of network devices, the number of MAC addresses for which traffic will be flooded will be high, and any switch port will carry flooded frames from a large number of devices.

Reference:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11_603836.htm
|

QUESTION NO: 73

Refer to the exhibit.



An attacker is connected to interface Fa0/11 on switch A-SW2 and attempts to establish a DHCP server for a man-in-middle attack. Which recommendation, if followed, would mitigate this type of attack?

- A. All switch ports in the Building Access block should be configured as DHCP trusted ports.
- B. All switch ports in the Building Access block should be configured as DHCP untrusted ports.
- C. All switch ports connecting to hosts in the Building Access block should be configured as DHCP trusted ports.
- D. All switch ports connecting to hosts in the Building Access block should be configured as DHCP untrusted ports.
- E. All switch ports in the Server Farm block should be configured as DHCP untrusted ports.
- F. All switch ports connecting to servers in the Server Farm block should be configured as DHCP untrusted ports.

Answer: D

Explanation:

One of the ways that an attacker can gain access to network traffic is to spoof responses that would be sent by a valid DHCP server. The DHCP spoofing device replies to client DHCP requests. The legitimate server may reply also, but if the spoofing device is on the same segment as the client, its reply to the client may arrive first.

The intruder's DHCP reply offers an IP address and supporting information that designates the intruder as the default gateway or Domain Name System (DNS) server. In the case of a gateway, the clients will then forward packets to the attacking device, which will in turn send them to the desired destination. This is referred to as a "man-in-the-middle" attack, and it may go entirely undetected as the intruder intercepts the data flow through the network.

Untrusted ports are those that are not explicitly configured as trusted. A DHCP binding table is built for untrusted ports. Each entry contains the client MAC address, IP address, lease time,

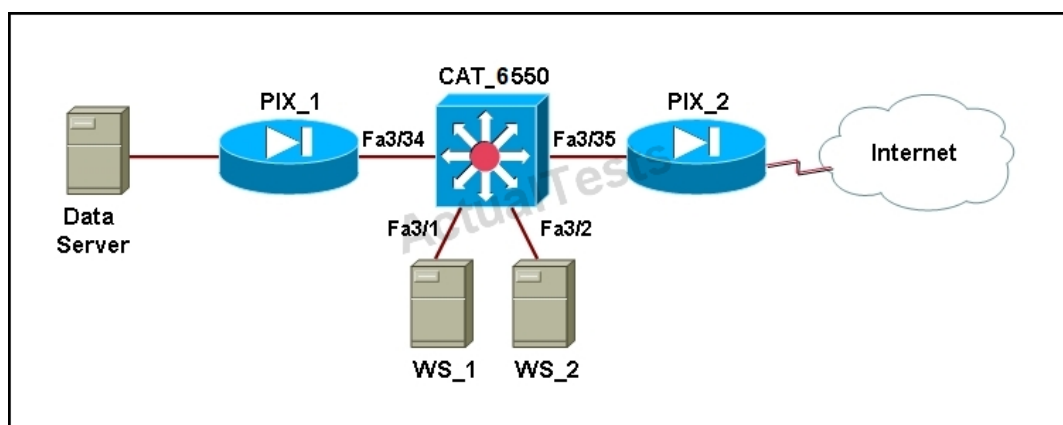
binding type, VLAN number, and port ID recorded as clients make DHCP requests. The table is then used to filter subsequent DHCP traffic. From a DHCP snooping perspective, untrusted access ports should not send any DHCP server responses, such as DHCPOFFER, DHCPACK, DHCPNAK.

Reference: Understanding and Configuring DHCP Snooping

(<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.1/13ew/configuration/guide/dhcp.html>)

QUESTION NO: 74

Refer to the exhibit.



The web servers WS_1 and WS_2 need to be accessed by external and internal users. For security reasons, the servers should not communicate with each other, although they are located on the same subnet. However, the servers do need to communicate with a database server located in the inside network. Which configuration isolates the servers from each other?

- A.** The switch ports 3/1 and 3/2 are defined as secondary VLAN isolated ports. The ports connecting to the two firewalls are defined as primary VLAN promiscuous ports.
- B.** The switch ports 3/1 and 3/2 are defined as secondary VLAN community ports. The ports connecting to the two firewalls are defined as primary VLAN promiscuous ports.
- C.** The switch ports 3/1 and 3/2 and the ports connecting to the two firewalls are defined as primary VLAN promiscuous ports.
- D.** The switch ports 3/1 and 3/2 and the ports connecting to the two firewalls are defined as primary VLAN community ports.

Answer: A

Explanation: Service providers often have devices from multiple clients, in addition to their own

servers, on a single Demilitarized Zone (DMZ) segment or VLAN. As security issues proliferate, it becomes necessary to provide traffic isolation between devices, even though they may exist on the same Layer 3 segment and VLAN. Catalyst 6500/4500 switches implement PVLANS to keep some switch ports shared and some switch ports isolated, although all ports exist on the same VLAN. The 2950 and 3550 support "protected ports," which are functionality similar to PVLANS on a per-switch basis.

A port in a PVLAN can be one of three types:

Isolated. An isolated port has complete Layer 2 separation from other ports within the same PVLAN, except for the promiscuous port. PVLANS block all traffic to isolated ports, except the traffic from promiscuous ports. Traffic received from an isolated port is forwarded to only promiscuous ports.

Promiscuous: A promiscuous port can communicate with all ports within the PVLAN, including the community and isolated ports. The default gateway for the segment would likely be hosted on a promiscuous port, given that all devices in the PVLAN will need to communicate with that port.

Community: Community ports communicate among themselves and with their promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities, or in isolated ports within their PVLAN.

Reference: Configuring Private VLANs

(<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sga/configuration/guide/pvlans.html>)

QUESTION NO: 75

What does the command `udld reset` accomplish?

- A. allows a UDLD port to automatically reset when it has been shut down
- B. resets all UDLD enabled ports that have been shutdown
- C. removes all UDLD configurations from interfaces that were globally enabled
- D. removes all UDLD configurations from interfaces that were enabled per-port

Answer: B

Explanation:

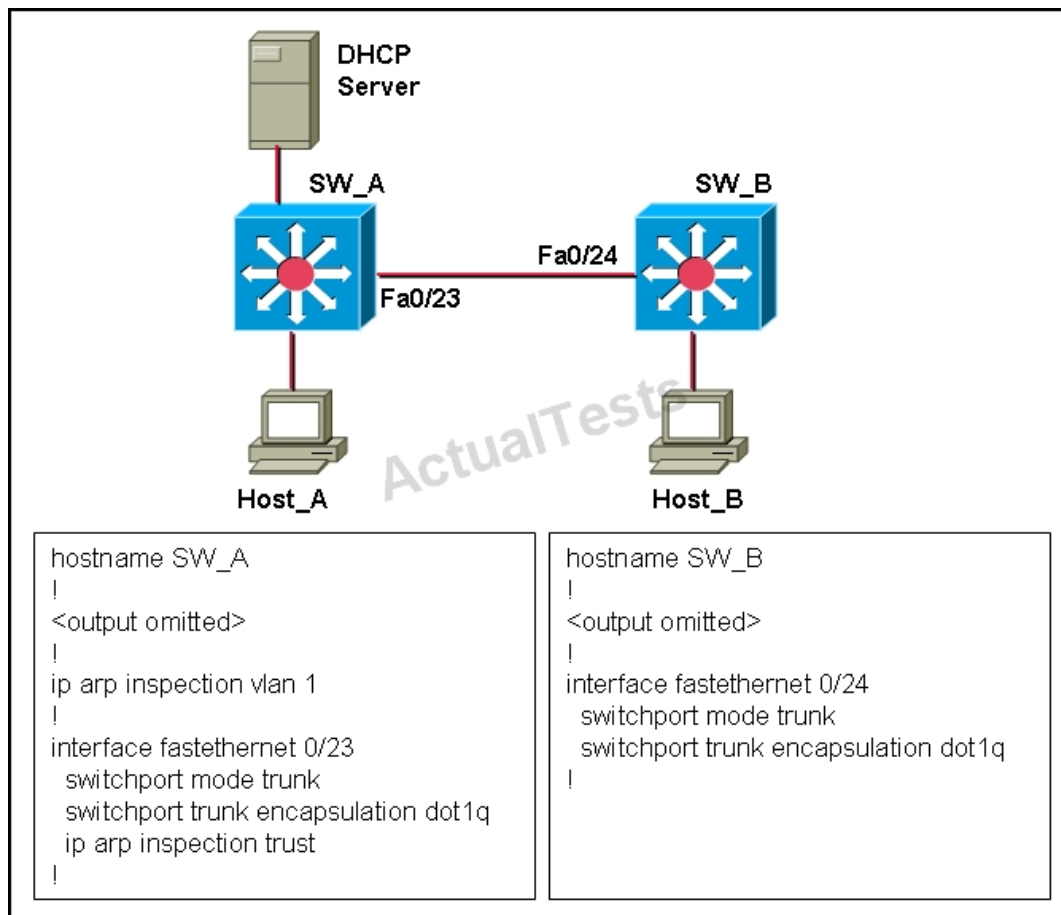
When unidirectional link condition is detected the UDLD set port in error-disabled state. To reinable all ports that UDLD has errdisabled the command:

Switch# `udld reset` is used.

Reference:

QUESTION NO: 76

Refer to the exhibit.



Dynamic ARP Inspection is enabled only on switch SW_A. Host_A and Host_B acquire their IP addresses from the DHCP server connected to switch SW_A. What would the outcome be if Host_B initiated an ARP spoof attack toward Host_A?

- A. The spoof packets are inspected at the ingress port of switch SW_A and are permitted.
- B. The spoof packets are inspected at the ingress port of switch SW_A and are dropped.
- C. The spoof packets are not inspected at the ingress port of switch SW_A and are permitted.
- D. The spoof packets are not inspected at the ingress port of switch SW_A and are dropped.

Answer: C

Explanation:

When configuring DAI, follow these guidelines and restrictions:

- DAI is an ingress security feature; it does not perform any egress checking.
 - DAI is not effective for hosts connected to routers that do not support DAI or that do not have this feature enabled. Because man-in-the-middle attacks are limited to a single Layer 2 broadcast domain, separate the domain with DAI checks from the one with no checking. This action secures the ARP caches of hosts in the domain enabled for DAI.
 - DAI depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses.
 - When DHCP snooping is disabled or in non-DHCP environments, use ARP ACLs to permit or to deny packets.
 - DAI is supported on access ports, trunk ports, EtherChannel ports, and private VLAN ports.
- In our example, since Company2 does not have DAI enabled (bullet point 2 above) packets will not be inspected and they will be permitted.

Reference

<http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SXF/configuration/guide/dynarp.html>

QUESTION NO: 77

Which statement is true about Layer 2 security threats?

- A.** MAC spoofing, in conjunction with ARP snooping, is the most effective counter-measure against reconnaissance attacks that use Dynamic ARP Inspection to determine vulnerable attack points.
- B.** DHCP snooping sends unauthorized replies to DHCP queries.
- C.** ARP spoofing can be used to redirect traffic to counter Dynamic ARP Inspection.
- D.** Dynamic ARP Inspection in conjunction with ARP spoofing can be used to counter DHCP snooping attacks.
- E.** MAC spoofing attacks allow an attacking device to receive frames intended for a different network host.
- F.** Port scanners are the most effective defense against Dynamic ARP Inspection.

Answer: E

Explanation:

First of all, MAC spoofing is not an effective counter-measure against any reconnaissance attack; it IS an attack! Furthermore, reconnaissance attacks don't use dynamic ARP inspection (DAI); DAI is a switch feature used to prevent attacks.

Reference: Layer 2 Security Features on Cisco Catalyst Layer 3 Fixed Configuration Switches

Configuration Example

(http://www.cisco.com/en/US/products/hw/switches/ps5023/products_configuration_example09186a00807c4101.shtml)

QUESTION NO: 78

On a Company switch named R1 you configure the following:

```
ip arp inspection vlan 10-12, 15
```

What is the purpose of this global configuration command made on R1?

- A. Discards ARP packets with invalid IP-to-MAC address bindings on trusted ports
- B. Validates outgoing ARP requests for interfaces configured on VLAN 10, 11, 12, or 15
- C. Intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings
- D. Intercepts all ARP requests and responses on trusted ports
- E. None of the other alternatives apply

Answer: C

Explanation:

The "ip arp inspection" command enables Dynamic ARP Inspection (DAI) for the specified VLANs. DAI is a security feature that validates Address Resolution Protocol (ARP) packets in a network. DAI allows a network administrator to intercept, log, and discard ARP packets with invalid MAC address to IP address bindings. This capability protects the network from certain "man-in-the-middle" attacks.

Reference: Understanding and Configuring Dynamic ARP Inspection

<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.1/20ew/configuration/guide/dynarp.html>

QUESTION NO: 79

Refer to the exhibit.

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
155
Insertion of option 82 is enabled
Interface          Trusted      Rate limit (pps)
-----
FastEthernet0/35   no          3
FastEthernet0/36   no          3
GigabitEthernet0/1 yes         unlimited
Switch#
```

Which two of the following statements are true? (Choose two)

- A. DHCP snooping is enabled for 155 Vlans
- B. DHCP snooping is enabled for a single Vlan
- C. DHCP Snooping is not enabled for any Vlan
- D. Option 82 is enabled for a VLAN 155
- E. Ports Fa0/5 and Fa0/6 should be kept shutdown as these are untrusted ports

Answer: B,D

Explanation:

As you can see in the exhibit, that DHCP snooping is enabled for a single vlan and an option 82 is enabled for a VLAN 155.

QUESTION NO: 80

What are two methods of mitigating MAC address flooding attacks? (Choose two.)

- A. Place unused ports in a common VLAN.
- B. Implement private VLANs.
- C. Implement DHCP snooping.
- D. Implement port security.
- E. Implement VLAN access maps

Answer: D,E

Explanation:

You can use the port security feature to limit and identify MAC addresses of the stations allowed to access the port. This restricts input to an interface. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port. If a port is configured as a secure port and the maximum number of secure MAC addresses is

reached, when the MAC address of a station that attempts to access the port is different from any of the identified secure MAC addresses, a security violation occurs. Also, if a station with a secure MAC address configured or learned on one secure port attempts to access another secure port, a violation is flagged. By default, the port shuts down when the maximum number of secure MAC addresses is exceeded.

Vlan accesss-map can match frame by MAC addresses and in combination with vlan filter it can be used to mitigate MAC flooding attacks.

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps5023/products_configuration_example09186a00807c4101.shtml#portsecurity

QUESTION NO: 81

What is one method that can be used to prevent VLAN hopping?

- A. Configure ACLs.
- B. Enforce username and password combinations.
- C. Configure all frames with two 802.1Q headers.
- D. Explicitly turn off DTP on all unused ports.
- E. Configure VACLs.

Answer: D

Explanation:

When securing VLAN trunks, also consider the potential for an exploit called VLAN hopping. Here, an attacker positioned on one access VLAN can craft and send frames with spoofed 802.1Q tags so that the packet payloads ultimately appear on a totally different VLAN, all without the use of a router.

For this exploit to work, the following conditions must exist in the network configuration:

The attacker is connected to an access switch port.

The same switch must have an 802.1Q trunk.

The trunk must have the attacker's access VLAN as its native VLAN.

To prevent from VLAN hopping turn off Dynamic Trunking Protocol on all unused ports.

Reference

<http://www.cisco.com/web/CA/events/pdfs/L2-security-Bootcamp-final.pdf>

QUESTION NO: 82

Why is BPDU guard an effective way to prevent an unauthorized rogue switch from altering the spanning-tree topology of a network?

- A. BPDU guard can guarantee proper selection of the root bridge.
- B. BPDU guard can be utilized along with PortFast to shut down ports when a switch is connected to the port.
- C. BPDU guard can be utilized to prevent the switch from transmitting BPDUs and incorrectly altering the root bridge election.
- D. BPDU guard can be used to prevent invalid BPDUs from propagating throughout the network.

Answer: B

Explanation:

As long as a port participates in STP, some device can assume the root bridge function and affect active STP topology. To assume the root bridge function, the device would be attached to the port and would run STP with a lower bridge priority than that of the current root bridge. If another device assumes the root bridge function in this way, it renders the network suboptimal. This is a simple form of a denial of service (DoS) attack on the network. The temporary introduction and subsequent removal of STP devices with low (0) bridge priority cause a permanent STP recalculation.

The STP PortFast BPDU guard enhancement allows network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have STP PortFast enabled are not able to influence the STP topology. At the reception of BPDUs, the BPDU guard operation disables the port that has PortFast configured. The BPDU guard transitions the port into errdisable state, and a message appears on the console.

Reference: Spanning Tree PortFast BPDU Guard Enhancement

http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a008009482f.shtml

QUESTION NO: 83

What two steps can be taken to help prevent VLAN hopping? (Choose two.)

- A. Place unused ports in a common unrouted VLAN.
- B. Enable BPDU guard.
- C. Implement port security.
- D. Prevent automatic trunk configurations.

E. Disable Cisco Discovery Protocol on ports where it is not necessary.

Answer: A,D

Explanation:

To prevent VLAN hopping you should disable unused ports and put them in an unused VLAN, or a separate unrouted VLAN. By not granting connectivity or by placing a device into a VLAN not in use, unauthorized access can be thwarted through fundamental physical and logical barriers. Another method used to prevent VLAN hopping is to prevent automatic trunk configuration. Hackers used 802.1Q and ISL tagging attacks, which are malicious schemes that allow a user on a VLAN to get unauthorized access to another VLAN. For example, if a switch port were configured as DTP auto and were to receive a fake DTP packet, it might become a trunk port and it might start accepting traffic destined for any VLAN. Therefore, a malicious user could start communicating with other VLANs through that compromised port.

Reference: VLAN Security White Paper, Cisco Systems

http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

QUESTION NO: 84

When an attacker is using switch spoofing to perform VLAN hopping, how is the attacker able to gather information?

- A. The attacking station uses DTP to negotiate trunking with a switch port and captures all traffic that is allowed on the trunk.
- B. The attacking station tags itself with all usable VLANs to capture data that is passed through the switch, regardless of the VLAN to which the data belongs.
- C. The attacking station generates frames with two 802.1Q headers to cause the switch to forward the frames to a VLAN that would be inaccessible to the attacker through legitimate means.
- D. The attacking station uses VTP to collect VLAN information that is sent out and then tags itself with the domain information to capture the data.

Answer: A

Explanation:

DTP should be disabled for all user ports on a switch. If the port is left with DTP auto configured (default on many switches), an attacker can connect and arbitrarily cause the port to start trunking and therefore pass all VLAN information.

Reference:

http://www.cisco.com/en/US/solutions/ns340/ns517/ns224/ns376/net_design_guidance0900aecd800ebd1e.pdf

QUESTION NO: 85

Refer to the exhibit.

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP Snooping is configured on the following VLANs:
 10 30-40 100 200-220
Insertion of option 82 information is enabled.
Interface      Trusted      Rate limit (pps)
-----
FastEthernet2/1  yes         none
FastEthernet2/2  yes         none
FastEthernet3/1  no          20
Switch#
```

DHCP snooping is enabled for selected VLANs to provide security on the network. How do the switch ports handle the DHCP messages?

- A. A DHCPOFFER packet from a DHCP server received on Ports Fa2/1 and Fa2/2 is dropped.
- B. A DHCP packet received on ports Fa2/1 and Fa2/2 is dropped if the source MAC address and the DHCP client hardware address does not match Snooping database.
- C. A DHCP packet received on ports Fa2/1 and Fa2/2 is forwarded without being tested.
- D. A DHCPRELEASE message received on ports Fa2/1 and Fa2/2 has a MAC address in the DHCP snooping binding database, but the interface information in the binding database does not match the interface on which the message was received and is dropped.

Answer: C

Explanation:

Trusted ports are allowed to send all types of DHCP messages. Untrusted ports can send only DHCP requests. If a DHCP response is seen on an untrusted port, the port is shut down. In this case, Fa2/1 & Fa2/2 are trusted (can send all types of DHCP messages) while Fa3/1 is untrusted (can only send DHCP requests).

QUESTION NO: 86

Which three statements about Dynamic ARP Inspection are true? (Choose three.)

- A.** It determines the validity of an ARP packet based on the valid MAC address-to-IP address bindings stored in the DHCP snooping database.
- B.** It forwards all ARP packets received on a trusted interface without any checks.
- C.** It determines the validity of an ARP packet based on the valid MAC address-to-IP address bindings stored in the CAM table.
- D.** It forwards all ARP packets received on a trusted interface after verifying and inspecting the packet against the Dynamic ARP Inspection table.
- E.** It intercepts all ARP packets on untrusted ports.
- F.** It is used to prevent against a DHCP snooping attack.

Answer: A,B,E

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps5023/products_configuration_example09186a00807c4101.shtml (background information, 3rd bulleted point)

QUESTION NO: 87

You are tasked with designing a security solution for your network. What information should be gathered before you design the solution?

- A.** IP addressing design plans, so that the network can be appropriately segmented to mitigate potential network threats
- B.** a list of the customer requirements
- C.** detailed security device specifications
- D.** results from pilot network testing

Answer: B

Explanation:

Cisco specific recommendations for designing a security solution for a network include the two points:

- Make sure you have a list of the applications running in the environment
- Have a network audit

And each network application has some requirements for the network in which it works.

Reference:

<http://www.ccnpguide.com/design-documentation/>

QUESTION NO: 88

Which two components should be part of a security implementation plan? (Choose two.)

- A. detailed list of personnel assigned to each task within the plan
- B. a Layer 2 spanning-tree design topology
- C. rollback guidelines
- D. placing all unused access ports in VLAN 1 to proactively manage port security
- E. enabling SNMP access to Cisco Discovery Protocol data for logging and forensic analysis

Answer: B,C

Explanation:

Cisco recommendation for the security implementation plan includes two components:

- A documented rollback plan should be part of any implementation plan
- A Layer 2 spanning tree design topology should be part of a security implementation plan

Reference:

<http://www.ccnpguide.com/design-documentation/>

QUESTION NO: 89

When creating a network security solution, which two pieces of information should you have obtained previously to assist in designing the solution? (Choose two.)

- A. a list of existing network applications currently in use on the network
- B. network audit results to uncover any potential security holes
- C. a planned Layer 2 design solution
- D. a proof-of-concept plan
- E. device configuration templates

Answer: A,B

Explanation:

Cisco specific recommendations for designing a security solution for a network include the two points:

- Make sure you have a list of the applications running in the environment
- Have a network audit

Reference:

<http://www.ccnpguide.com/design-documentation/>

QUESTION NO: 90

What action should you be prepared to take when verifying a security solution?

- A. having alternative addressing and VLAN schemes
- B. having a rollback plan in case of unwanted or unexpected results
- C. running a test script against all possible security threats to insure that the solution will mitigate all potential threats
- D. isolating and testing each security domain individually to insure that the security design will meet overall requirements when placed into production as an entire system

Answer: B

Explanation:

Verifying a security solution includes two points:

- Verification of an implemented security solution requires results from audit testing of the implemented solution
- Verifying a documentation for rollback plan

Reference:

<http://www.ccnpguide.com/design-documentation/>

QUESTION NO: 91

When you enable port security on an interface that is also configured with a voice VLAN, what is the maximum number of secure MAC addresses that should be set on the port?

- A. No more than one secure MAC address should be set.
- B. The default is set.
- C. The IP phone should use a dedicated port, therefore only one MAC address is needed per port.
- D. No value is needed if the switchport priority extend command is configured.
- E. No more than two secure MAC addresses should be set.

Answer: E

Explanation:

Usually, an IP Phone needs two MAC addresses, one for the voice vlan and one for the access

vlan. If you don't want other devices to access this port then you should not set more than two secure MAC addresses.

Below is an example for this configuration:

```
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address
sticky
Switch(config-if)# switchport port-security maximum 1 vlan voice
Switch(config-if)# switchport port-security maximum 1 vlan access
//Configure static MAC addresses for these VLANs
Switch(config-if)# switchport port-security mac-address sticky
0000.0000.0001
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
vlan voice
```

(For more information about this, please

read http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sg/configuration/guide/port_sec.html)

QUESTION NO: 92

Refer to the exhibit.

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport access vlan 21
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 22
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 20
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Switch(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Switch(config-if)# switchport port-security maximum 10 vlan access
Switch(config-if)# switchport port-security maximum 10 vlan voice
```

From the configuration shown, what can be determined?

- A.** The sticky addresses are only those manually configured MAC addresses enabled with the sticky keyword.
- B.** The remaining secure MAC addresses are learned dynamically, converted to sticky secure MAC addresses, and added to the running configuration.
- C.** A voice VLAN is configured in this example, so port security should be set for a maximum of 2.
- D.** A security violation restricts the number of addresses to a maximum of 10 addresses per access VLAN and voice VLAN. The port is shut down if more than 10 devices per VLAN attempt to

access the port.

Answer: B

Explanation:

By enabling sticky port security, you can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration. You might want to do this if you do not expect the user to move to another port, and you want to avoid statically configuring a MAC address on every port. To enable sticky port security, enter the `switchport port-security mac-address sticky` command. When you enter this command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If you save the running config file to the configuration file, the interface does not need to relearn these addresses when the switch restarts. If you do not save the configuration, they are lost.

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/53SG/configuration/port_sec.html#wp1047668

QUESTION NO: 93

By itself, what does the command `aaa new-model` enable?

- A. It globally enables AAA on the switch, with default lists applied to the VTYs.
- B. Nothing; you must also specify which protocol (RADIUS or TACACS) will be used for AAA.
- C. It enables AAA on all dot1x ports.
- D. Nothing; you must also specify where (console, TTY, VTY, dot1x) AAA is being applied.

Answer: A

Explanation:

`aaa new-model` enable the AAA access control model. Access control is the way you control who is allowed access to the network server and what services they are allowed to use once they have access. Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you set up access control on your router or access server.

Reference:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfaaa.html

QUESTION NO: 94

What is needed to verify that a newly implemented security solution is performing as expected?

- A. a detailed physical and logical topology
- B. a cost analysis of the implemented solution
- C. detailed logs from the AAA and SNMP servers
- D. results from audit testing of the implemented solution

Answer: D

Explanation:

Recommended by Cisco verification plan for designing a security solution includes verification of an implemented security solution requires results from audit testing of the implemented solution.

Reference:

<http://www.ccnpguide.com/design-documentation/>

QUESTION NO: 95

When configuring port security on a Cisco Catalyst switch port, what is the default action taken by the switch if a violation occurs?

- A. protect (drop packets with unknown source addresses)
- B. restrict (increment SecurityViolation counter)
- C. shut down (access or trunk port)
- D. transition (the access port to a trunking port)

Answer: C

Explanation:

When configuring port security, the following options for port security violation modes are available:

- protect—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.
- restrict—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the SecurityViolation counter to increment.
- shutdown—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

The default violation mode is shutdown.

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.1E/native/configuration/guide/port_sec.html

QUESTION NO: 96

Refer to the exhibit.

```
Switch# show port-security interface fastethernet 5/1

Port Security: EnabledPort
Status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

What happens when one more user is connected to interface FastEthernet 5/1?

- A.** All secure addresses age out and are removed from the secure address list. The security violation counter increments.
- B.** The first address learned on the port is removed from the secure address list and is replaced with the new address.
- C.** The interface is placed into the error-disabled state immediately, and an SNMP trap notification is sent.
- D.** The packets with the new source addresses are dropped until a sufficient number of secure MAC addresses are removed from the secure address list.

Answer: C

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.1/19ew/configuration/guide/port_sec.pdf

QUESTION NO: 97

Refer to the exhibit.

```
Switch# show ip access-lists net_10
Extended IP access list net_10
  10 permit ip 10.0.0.0 0.255.255.255 any

Switch# conf t
Switch(config)# vlan access-map thor 10
Switch(config-access-map)# match ip address net_10
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan filter thor vlan-list 12-16
```

What happens to traffic within VLAN 14 with a source address of 172.16.10.5?

- A. The traffic is forwarded to the TCAM for further processing.
- B. The traffic is forwarded to the router processor for further processing.
- C. The traffic is dropped.
- D. The traffic is forwarded without further processing.

Answer: C

Explanation:

VLAN maps, also known as VLAN ACLs or VACLs, can filter all traffic traversing a switch. VLAN maps can be configured on the switch to filter all packets that are routed into or out of a VLAN, or are bridged within a VLAN. VLAN maps are used strictly for security packet filtering. Unlike router ACLs, VLAN maps are not defined by direction (input or output).

To create a VLAN map and apply it to one or more VLANs, perform these steps:

- Create the standard or extended IP ACLs or named MAC extended ACLs to be applied to the VLAN. This access-list will select the traffic that will be either forwarded or dropped by the access-map. Only traffic matching the 'permit' condition in an access-list will be passed to the access-map for further processing.
- Enter the `vlan access-map access-map-name [sequence] global configuration` command to create a VLAN ACL map entry. Each access-map can have multiple entries. The order of these

entries is determined by the sequence. If no sequence number is entered, access-map entries are added with sequence numbers in increments of 10.

- In access map configuration mode, optionally enter an action forward or action drop. The default is to forward traffic. Also enter the match command to specify an IP packet or a non-IP packet (with only a known MAC address), and to match the packet against one or more ACLs (standard or extended).
- Use the vlan filter access-map-name vlan-list vlan-list global configuration command to apply a VLAN map to one or more VLANs. A single access-map can be used on multiple VLANs.

QUESTION NO: 98

What does the global configuration command `ip arp inspection vlan 10-12, 15` accomplish?

- A. validates outgoing ARP requests for interfaces configured on VLAN 10, 11, 12, or 15
- B. intercepts all ARP requests and responses on trusted ports
- C. intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings
- D. discards ARP packets with invalid IP-to-MAC address bindings on trusted ports

Answer: C

Explanation:

The function of DAI is:

On untrusted ports, the switch captures all ARP packets (both request and reply) and then validates the Source Protocol and Source Hardware address values against the snooping table database for that port.

If the MAC address and IP address and the corresponding port do not match the snooping database entry, the ARP packets are dropped. DAI thus prevents the node from specifying a non-legitimate IP-MAC address binding which differs from what was given by the DHCP server.

QUESTION NO: 99

The DAI feature has been implemented in the ACME switched LAN. Which three statements are true about the dynamic ARP inspection (DAI) feature? (Select three)

- A. DAI can be performed on ingress ports only.
- B. DAI can be performed on both ingress and egress ports.
- C. DAI is supported on access ports, trunk ports, EtherChannel ports, and private VLAN ports.

- D. DAI should be enabled on the root switch for particular VLANs only in order to secure the ARP caches of hosts in the domain.
- E. DAI should be configured on all access switch ports as untrusted and on all switch ports connected to other switches as trusted.
- F. DAI is supported on access and trunk ports only.

Answer: A,C,E

Explanation:

To prevent ARP spoofing or “poisoning,” a switch must ensure that only valid ARP requests and responses are relayed. DAI prevents these attacks by intercepting and validating all ARP requests and responses. Each intercepted ARP reply is verified for valid MAC-address-to-IP-address bindings before it is forwarded to a PC to update the ARP cache. ARP replies coming from invalid devices are dropped.

DAI determines the validity of an ARP packet based on a valid MAC-address-to-IP-address bindings database built by DHCP snooping. In addition, to handle hosts that use statically configured IP addresses, DAI can also validate ARP packets against user-configured ARP ACLs. To ensure that only valid ARP requests and responses are relayed, DAI takes these actions:

QUESTION NO: 100

You are implementing basic switch security best practices. Which of these is a tactic that you can use to mitigate compromises from being launched through the switch?

- A. Make all ports private VLAN ports.
- B. Place all unused ports in native VLAN 1 until needed.
- C. Proactively configure unused switch ports as access ports.
- D. Disable Cisco Discovery Protocol globally.

Answer: C

Explanation:

Follow these best practices to mitigate compromises through a switch:

QUESTION NO: 101

Which three statements apply to access control of both bridged and routed traffic for VLANs? (Choose three.)

- A. Router ACLs can be applied to the input and output directions of a VLAN interface.
- B. Bridged ACLs can be applied to the input and output directions of a VLAN interface.
- C. Only router ACLs can be applied to a VLAN interface.
- D. VLAN maps can be applied to a VLAN interface.
- E. VLAN maps and router ACLs can be used in combination.

Answer: A,C,E

Explanation:

Bridged ACL are Port ACL, so B is not correct as those are only applied inbound, and in addition VLAN interfaces are layer 3 and port ACL are layer 2. Router ACL's are layer 3 and they may be applied both inbound and outbound, so A is correct.

Also, you can use VACLs alone or a combination of VACLs and ACLs, so D is correct

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/vlan_acls.html#wp1149762

Finally, VACL is applied globally to one or more VLANs listed and not to a VLAN interface (SVI), which makes C correct but at the same time it makes E not correct

<http://www.cathayschool.com/VACL-Configuration-a577.html>

QUESTION NO: 102

```
Sw2#show running-config

-----output omitted-----

aaa new-model
aaa authentication dot1x default group radius
dot1x system-auth-control

-----output omitted-----

interface fastethernet 0/6
dot1x port-control auto
```

Refer to the exhibit. Which statement is true about the show running-config output?

- A. Sw2 is configured for switch-based authentication using RADIUS.
- B. Interface FastEthernet0/6 is configured with a SmartPort macro using RADIUS.
- C. Interface FastEthernet0/6 is configured for 802.1X Authenticated Trunking Protocol (ATP).

- D. Interface FastEthernet0/6 is configured for port-based traffic control.
- E. Interface FastEthernet0/6 is configured for port-based authentication.

Answer: E

Explanation:

Enabling 802.1X Authentication

To enable 802.1X port-based authentication, you must enable AAA and specify the authentication method list. A method list describes the sequence and authentication methods to be queried to authenticate a user.

The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle, the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure 802.1X port-based authentication. This procedure is required.

Command

Purpose

Step 1

configure terminal

Enter global configuration mode.

Step 2

aaa new-model

Enable AAA.

Step 3

aaa authentication dot1x {default}*method1[method2...]*

Create an 802.1X authentication method list.

To create a default list that is used when a named list is *not* specified in the authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.

Enter at least one of these keywords:

-

group radius—Use the list of all RADIUS servers for authentication.

-

none—Use no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.

Step 4

interface *interface-id*

Enter interface configuration mode, and specify the interface connected to the client that is to be enabled for 802.1X authentication.

Step 5

dot1x port-control auto "Pass Any Exam. Any Time." - www.actualtests.com

Enable 802.1X authentication on the interface.

Step 6

end

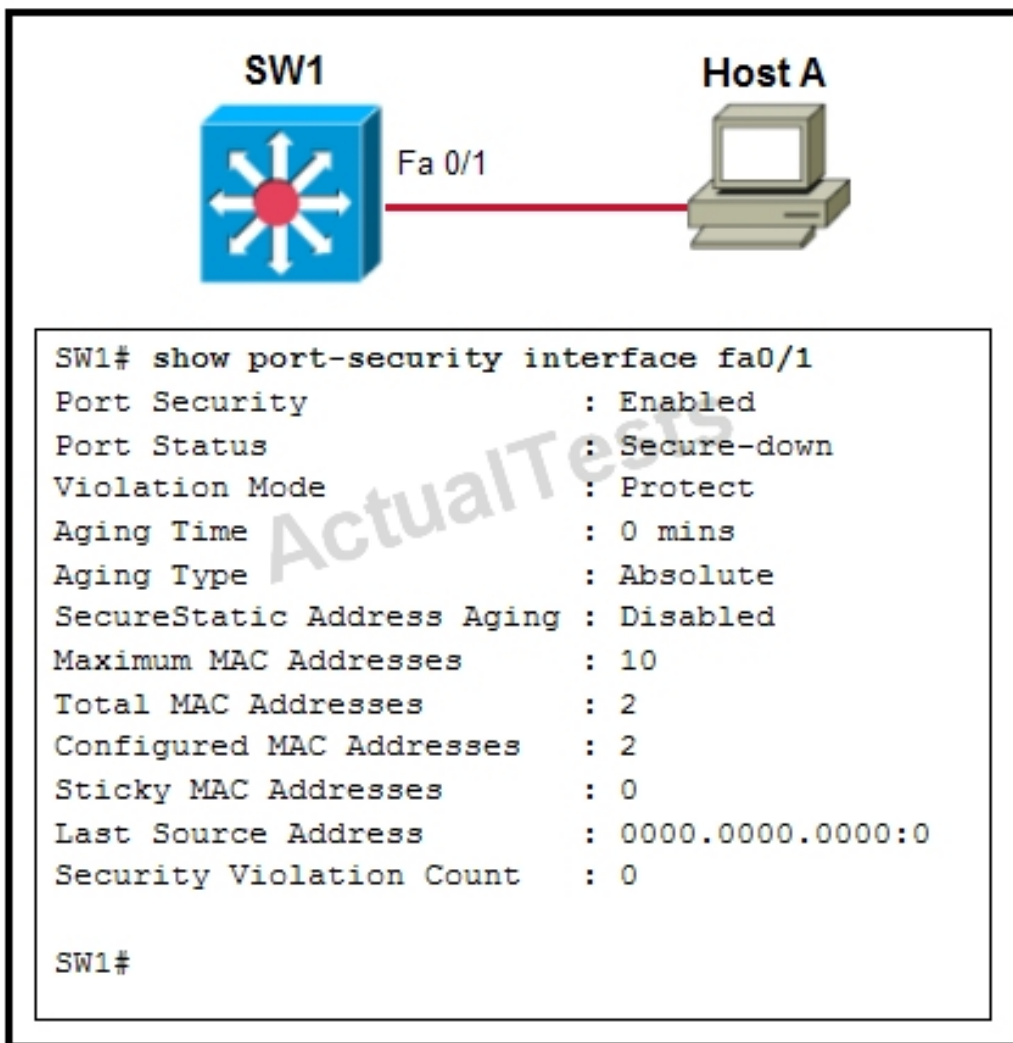
Return to privileged EXEC mode.

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_11_yj4/configuration/guide/Sw8021x.html

QUESTION NO: 103

Refer to the exhibit.



The show port-security interface fa0/1 command was issued on switch SW1. Given the output

that was generated, which two security statement are true? (Choose two.)

- A. Interface FastEthernet 0/1 was configured with the switchport port-security aging command.
- B. Interface FastEthernet 0/1 was configured with the switchport port-security protect command.
- C. Interface FastEthernet 0/1 was configured with the switchport port-security violation restrict command.
- D. When the number of secure IP addresses reaches 10, the interface will immediately shut down.
- E. When the number of secure MAC addresses reaches 10, packets from unknown MAC addresses will be dropped.

Answer: B,E

Explanation:

The "Violation Mode: Protect" tells us this interface has been configured with the switchport port-security protect command. Protect mode drops packets with unknown source addresses when the violation occurs.

QUESTION NO: 104

What is a characteristic of a VLAN map that does not contain a match clause?

- A. implicit deny feature at end of list
- B. implicit forward feature at end of list
- C. can only be implemented by the input direction within the VLAN
- D. can only be implemented by the output direction within the VLAN

Answer: B

Explanation:

If there is a match clause for that type of packet (IP or MAC) in the VLAN map, the default action is to drop the packet if the packet does not match any of the entries within the map. If there is no match clause for that type of packet, the default is to forward the packet.

Reference:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sga/configuration/guide/secure.html>

QUESTION NO: 105

Which three items are types of PVLAN ports? (Choose three.)

- A. community
- B. dedicated
- C. desireable
- D. isolated
- E. native
- F. promiscuous

Answer: A,D,F

Explanation:

Private VLANs (PVLANS) provide layer 2 isolation between ports within the same broadcast domain. There are three types of PVLAN ports:

Promiscuous— A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN.

Isolated— An isolated port has complete Layer 2 separation from the other ports within the same PVLAN, but not from the promiscuous ports. PVLANS block all traffic to isolated ports except traffic from promiscuous ports. Traffic from isolated port is forwarded only to promiscuous ports.

Community— Community ports communicate among themselves and with their promiscuous ports. These interfaces are separated at Layer 2 from all other interfaces in other communities or isolated ports within their PVLAN

Reference: http://www.cisco.com/en/US/tech/tk389/tk814/tk840/tsd_technology_support_sub-protocol_home.html

QUESTION NO: 106

Which optional feature of an Ethernet switch disables a port on a point-to-point link if the port does not receive traffic while Layer 1 status is up?

- A. BackboneFast
- B. UplinkFast
- C. Loop Guard
- D. UDLD aggressive mode
- E. Fast Link Pulse bursts
- F. Link Control Word

Answer: D

Explanation:

UDLD aggressive mode is disabled by default. Configure UDLD aggressive mode only on point-to-point links between network devices that support UDLD aggressive mode. With UDLD aggressive mode enabled, when a port on a bidirectional link that has a UDLD neighbor relationship

established stops receiving UDLD packets, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is disabled.

QUESTION NO: 107

When configuring private VLANs, which configuration task must you do first?

- A. Configure the private VLAN port parameters.
- B. Configure and map the secondary VLAN to the primary VLAN.
- C. Disable IGMP snooping.
- D. Set the VTP mode to transparent.

Answer: D

Explanation:

When you configure private VLANs, the switch must be in VTP transparent mode. Because VTP does not support private VLANs, you must manually configure private VLANs on all switches in the Layer 2 network. If you do not configure the primary and secondary VLAN association in some switches in the network, the Layer 2 databases in these switches are not merged. This can result in unnecessary flooding of private-VLAN traffic on those switches.

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_see/configuration/guide/swpvlan.html

QUESTION NO: 108

Which statement about the configuration and application of port access control lists is true?

- A. PACLs can be applied in the inbound or outbound direction of a Layer 2 physical interface.
- B. At Layer 2, a MAC address PACL takes precedence over any existing Layer 3 PACL.
- C. When you apply a port ACL to a trunk port, the ACL filters traffic on all VLANs present on the trunk port.
- D. PACLs are not supported on EtherChannel interfaces.

Answer: C

Explanation:

The PACL feature provides the ability to perform access control on specific Layer 2 ports. A Layer

2 port is a physical LAN or trunk port that belongs to a VLAN. PACLs are applied only on the ingress traffic. The PACL feature is supported only in hardware (PACLs are not applied to any packets routed in software). When you create a PACL, an entry is created in the ACL TCAM. You can use the show tcam counts command to see how much TCAM space is available. The PACL feature does not affect Layer 2 control packets received on the port.

Reference:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vacl.pdf>

QUESTION NO: 109

Refer to the exhibit.

```
switch# show port-security interface fastethernet 0/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

Which statement about the command output is true?

- A.** If the number of devices attempting to access the port exceeds 11, the port shuts down for 20 minutes, as configured.
- B.** The port has security enabled and has shut down due to a security violation.
- C.** The port is operational and has reached its configured maximum allowed number of MAC addresses.
- D.** The port allows access for 11 MAC addresses in addition to the three configured MAC addresses.

Answer: C

Explanation:

The port is operational (Port status: SecureUp) and has reached its configured maximum allowed number of MAC addresses (Maximum MAC addresses: 11, Total MAC addresses: 11).

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.1E/native/configuration/guide/port_sec.html

QUESTION NO: 110

Refer to the exhibit.

```
Router(config)# vlan access-map pass 10
Router(config-access-map)# match ip address ABC
Router(config-access-map)# action forward
Router(config)# vlan filter pass vlan-list 5-10
```

Which statement is true?

- A. IP traffic matching access list ABC is forwarded through VLANs 5-10.
- B. IP traffic matching VLAN list 5-10 is forwarded, and all other traffic is dropped.
- C. All VLAN traffic matching VLAN list 5-10 is forwarded, and all traffic matching access list ABC is dropped.
- D. All VLAN traffic in VLANs 5-10 that match access list ABC is forwarded, and all other traffic is dropped.

Answer: D

Explanation:

VLAN maps, also known as VLAN ACLs or VACLs, can filter all traffic traversing a switch. VLAN maps can be configured on the switch to filter all packets that are routed into or out of a VLAN, or are bridged within a VLAN. VLAN maps are used strictly for security packet filtering. Unlike router ACLs, VLAN maps are not defined by direction (input or output).

To create a VLAN map and apply it to one or more VLANs, perform these steps:

- Create the standard or extended IP ACLs or named MAC extended ACLs to be applied to the VLAN. This access-list will select the traffic that will be either forwarded or dropped by the access-map. Only traffic matching the 'permit' condition in an access-list will be passed to the access-map

for further processing.

- Enter the `vlan access-map access-map-name [sequence]` global configuration command to create a VLAN ACL map entry. Each access-map can have multiple entries. The order of these entries is determined by the sequence. If no sequence number is entered, access-map entries are added with sequence numbers in increments of 10.
- In access map configuration mode, optionally enter an action `forward` or `drop`. The default is to forward traffic. Also enter the `match` command to specify an IP packet or a non-IP packet (with only a known MAC address), and to match the packet against one or more ACLs (standard or extended).
- Use the `vlan filter access-map-name vlan-list vlan-list` global configuration command to apply a VLAN map to one or more VLANs. A single access-map can be used on multiple VLANs.

Reference:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/vacl.html#wp1061021>

QUESTION NO: 111

Refer to the exhibit.

```
Switch#show vlan private-vlan type
```

Primary	Secondary	Type	Interfaces
202		primary	
200		isolated	

What can be concluded about VLANs 200 and 202?

- A.** VLAN 202 carries traffic from promiscuous ports to isolated, community, and other promiscuous ports in the same VLAN. VLAN 200 carries traffic between community ports and to promiscuous ports.
- B.** VLAN 202 carries traffic from promiscuous ports to isolated, community, and other promiscuous ports in the same VLAN. VLAN 200 carries traffic from isolated ports to a promiscuous port.
- C.** VLAN 200 carries traffic from promiscuous ports to isolated, community, and other promiscuous ports in the same VLAN. VLAN 202 carries traffic between community ports and to promiscuous ports.

D. VLAN 200 carries traffic from promiscuous ports to isolated, community, and other promiscuous ports in the same VLAN. VLAN 202 carries traffic from isolated ports to a promiscuous port.

Answer: B

Explanation: As a Primary VLAN carries traffic from promiscuous ports to isolated, community, and other promiscuous ports in the same primary VLAN as an isolated VLAN carries traffic from isolated ports to a promiscuous port.

Reference:

CCNP BCMSN Official Exam Certification Guide, Fourth Edition, Chapter 16: Securing with VLANs, Private VLANs, p. 414

QUESTION NO: 112

A switch has been configured with PVLANS. With what type of PVLAN port should the default gateway be configured?

- A. isolated
- B. promiscuous
- C. community
- D. primary
- E. trunk

Answer: B

Explanation:

Promiscuous: The switch port connects to a router, firewall, or other common gateway device. This port can communicate with anything else connected to the primary or any secondary VLAN. In other words, the port is in promiscuous mode, in which the rules of private VLANs are ignored.

Reference: Configuring Private VLANs

(<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sga/configuration/guide/pvlans.html>)

QUESTION NO: 113

Refer to the exhibit.

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
```

Which statement about the private VLAN configuration is true?

- A. Only VLAN 503 will be the community PVLAN, because multiple community PVLANS are not allowed.
- B. Users of VLANs 501 and 503 will be able to communicate.
- C. VLAN 502 is a secondary VLAN.
- D. VLAN 502 will be a standalone VLAN, because it is not associated with any other VLANs.

Answer: C

Explanation:

VLAN 502 has been configured as private-vlan community. So it is a secondary PVLAN

QUESTION NO: 114

Which Cisco IOS command globally enables port-based authentication on a switch?

- A. aaa port-auth enable
- B. radius port-control enable
- C. dot1x system-auth-control
- D. switchport aaa-control enable

Answer: C

Explanation:

Configuration of 802.1x authentication is done in 5 steps:

Step 1 Enable AAA on the switch.

By default, AAA is disabled. You can enable AAA for port-based authentication by using the following global configuration command:

```
Switch(config)#aaa new-model
```

Step 2 Define external RADIUS servers.

First, define each server along with its secret shared password. This string is known only to the switch and the server, and provides a key for encrypting the authentication session. Use the following global configuration command:

```
Switch(config)#radius-server host {hostname | ip-address} [key string]
```

Step 3 Define the authentication method for 802.1x.

Using the following command causes all RADIUS authentication servers that are defined on the switch to be used for 802.1x authentication:

```
Switch(config)#aaa authentication dot1x default group radius
```

Step 4 Enable 802.1x on the switch:

```
Switch(config)#dot1x system-auth-control
```

Step 5 Configure each switch port that will use 802.1x:

```
Switch(config)# interface type mod/num
```

```
Switch(config-if)#dot1x port-control {force-authorized | forceunauthorized | auto}
```

Here, the 802.1x state is one of the following:

- force-authorized—The port is forced to always authorize any connected client. No authentication is necessary. This is the default state for all switch ports when 802.1x is enabled.
- force-unauthorized—The port is forced to never authorize any connected client. As a result, the port cannot move to the authorized state to pass traffic to a connected client.
- auto — The port uses an 802.1x exchange to move from the unauthorized to the authorized

state, if successful. This requires an 802.1x-capable application on the client PC.

Reference:

CCNP BCMSN Official Exam Certification Guide, Fourth Edition, Chapter 15: Securing Switch Access, Port-Based Authentication, p. 392

QUESTION NO: 115 CORRECT TEXT

AAAdot1x Lab

Acme is a small shipping company that has an existing enterprise network comprised of 2 switches; DSW1 and

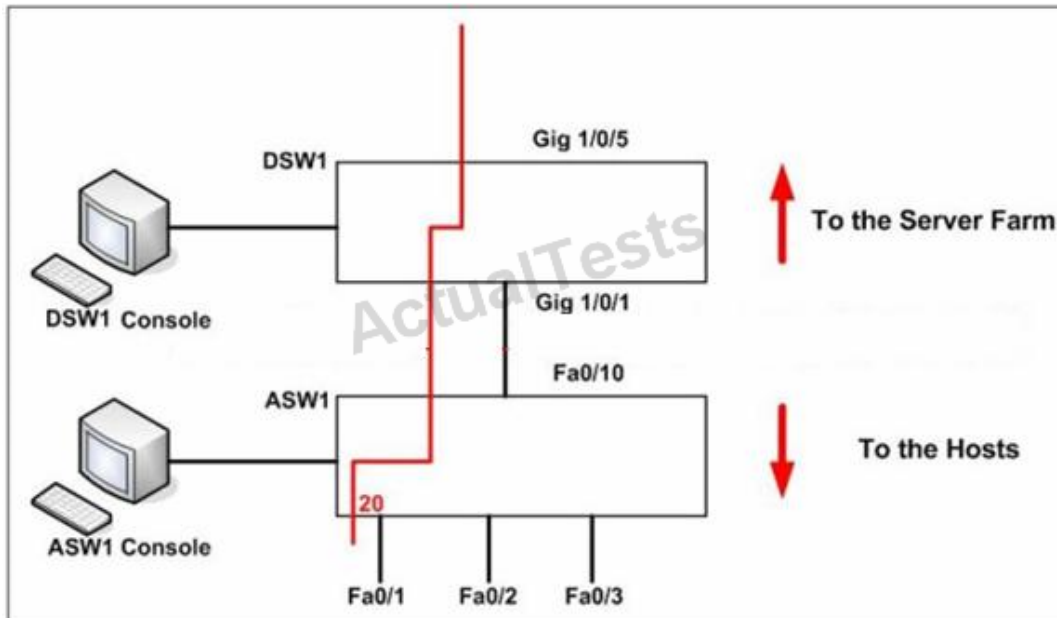
ASW2. The topology diagram indicates their layer 2 mapping. VLAN 40 is a new VLAN that will be used to provide the shipping personnel access to the server. For security reasons, it is necessary to restrict access to

VLAN 20 in the following manner:

- Users connecting to ASW1's port must be authenticate before they are given access to the network.
- Authentication is to be done via a Radius server:
- Radius server host: 172.120.39.46
- Radius key: rad123
- Authentication should be implemented as close to the host device possible.
- Devices on VLAN 20 are restricted to in the address range of 172.120.40.0/24.
- Packets from devices in the address range of 172.120.40.0/24 should be passed on VLAN 20.
- Packets from devices in any other address range should be dropped on VLAN 20.
- Filtering should be implemented as close to the server farm as possible.

The Radius server and application servers will be installed at a future date. You have been tasked with implementing the above access control as a pre-condition to installing the servers. You must use the available

IOS switch features.



Answer: The configuration:

Step1: Console to ASW1 from PC console 1

```
ASW1(config)#aaa new-model
```

```
ASW1(config)#radius-server host 172.120.39.46 key rad123
```

```
ASW1(config)#aaa authentication dot1x default group radius
```

```
ASW1(config)#dot1x system-auth-control
```

```
ASW1(config)#inter fastEthernet 0/1
```

```
ASW1(config-if)#switchport mode access
```

```
ASW1(config-if)#dot1x port-control auto
```

```
ASW1(config-if)#exit
```

```
ASW1#copy run start
```

Step2: Console to DSW1 from PC console 2

```
DSW1(config)#ip access-list standard 10
```

```
DSW1(config-ext-nacl)#permit 172.120.40.0 0.0.0.255
```

```
DSW1(config-ext-nacl)#exit
```

```
DSW1(config)#vlan access-map PASS 10
```

```
DSW1(config-access-map)#match ip address 10
```

```
DSW1(config-access-map)#action forward
```

```
DSW1(config-access-map)#exit
```

```
DSW1(config)#vlan access-map PASS 20
```

```
DSW1(config-access-map)#action drop
```

```
DSW1(config-access-map)#exit
```

```
DSW1(config)#vlan filter PASS vlan-list 20
```

```
DSW1#copy run start
```

QUESTION NO: 116

Private VLANs can be configured as which three of these port types? (Choose three.)

- A. isolated
- B. protected
- C. private
- D. associated
- E. promiscuous
- F. community

Answer: A,E,F

Reference:

<http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/PrivateVLANs.html#wp1182268>

QUESTION NO: 117

What is the method used to filter traffic being bridged within a VLAN?

- A. Ethernet maps
- B. router ACLs
- C. VLAN maps
- D. IP ACLs

Answer: C

Explanation:

You can use VLAN ACLs or VLAN maps to provide access-control for all packets (bridged and routed). You can use VLAN maps to filter traffic between devices in the same VLAN. VLAN maps are configured to provide access control based on Layer 3 addresses for IPv4. Unsupported protocols are access-controlled through MAC addresses using Ethernet ACEs. After a VLAN map is applied to a VLAN, all packets (routed or bridged) entering the VLAN are checked against the VLAN map.

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3750x_3560x/software/release/12.2_55_se/configuration/guide/swacl.html

QUESTION NO: 118

Which statement about when standard access control lists are applied to an interface to control inbound or outbound traffic is true?

- A. The best match of the ACL entries is used for granularity of control.
- B. They use source IP information for matching operations.
- C. They use source and destination IP information for matching operations.
- D. They use source IP information along with protocol-type information for finer granularity of control.

Answer: B

Reference: http://www.cs.odu.edu/~csi/cisco/router_configuration/access_list.html (see create standard access lists)

QUESTION NO: 119

Refer to the exhibit.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip verify source port-security
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface gigabitethernet0/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet0/1
Switch(config)# end
```

Which two statements about this Layer 3 security configuration example are true? (Choose two.)

- A. Static IP source binding can be configured only on a routed port.
- B. Source IP and MAC filtering on VLANs 10 and 11 will occur.
- C. DHCP snooping will be enabled automatically on the access VLANs.
- D. IP Source Guard is enabled.
- E. The switch will drop the configured MAC and IP address source bindings and forward all other traffic.

Answer: B,D

Explanation:

Cisco Catalyst switches can use the IP source guard feature to detect and suppress address spoofing attacks—even if they occur within the same subnet. IP source guard does this by making use of the DHCP snooping database, as well as static IP source binding entries. If DHCP snooping is configured and enabled, the switch learns the MAC and IP addresses of hosts that

use DHCP. Packets arriving on a switch port can be tested for one of the following conditions:

- The source IP address must be identical to the IP address learned by DHCP snooping or a static entry. A dynamic port ACL is used to filter traffic. The switch automatically creates this ACL, adds the learned source IP address to the ACL, and applies the ACL to the interface where the address is learned.
- The source MAC address must be identical to the MAC address learned on the switch port and by DHCP snooping. Port security is used to filter traffic.

For the hosts that don't use DHCP, you can configure a static IP source binding with the following configuration command:

```
Switch(config)#ip source binding mac-address vlan vlan-id ip-address interface type mod/num
```

Here, the host's MAC address is bound to a specific VLAN and IP address, and is expected to be found on a specific switch interface. Next, enable IP source guard on one or more switch interfaces with the following configuration commands:

```
Switch(config)#interface type mod/num
```

```
Switch(config-if)#ip verify source [port-security]
```

The ip verify source command will inspect the source IP address only. You can add the port-security keyword to inspect the source MAC address, too.

Reference:

CCNP BCMSN Official Exam Certification Guide, Fourth Edition, Chapter 15: Securing Switch Access, IP Source Guard, p 397

QUESTION NO: 120 DRAG DROP

Capabilities of SNMP are dependent on the version implemented. Drag the feature descriptions on the left to the respective SNMP versions on the right.

increased 64-bit counters for new data types	SNMPv1
security levels	
get next request	
informed request	SNMPv2
unsolicited agent alarm message	
usernames	
	SNMPv3

Answer:

Capabilities of SNMP are dependent on the version implemented. Drag the feature descriptions on the left to the respective SNMP versions on the right.

Feature Descriptions (Left)	SNMPv1	SNMPv2	SNMPv3
increased 64-bit counters for new data types		increased 64-bit counters for new data types	
security levels			security levels
get next request	get next request		
informed request		informed request	
unsolicited agent alarm message	unsolicited agent alarm message		
usernames			usernames

Explanation:

SNMP Version	Features
SNMPv1	- get next request - unsolicited agent alarm message
SNMPv2	- increased 64-bit counters for new data types - informed request
SNMPv3	- security levels - usernames

Reference:

http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html

<http://en.wikipedia.org/wiki/Snmp>

QUESTION NO: 121

A network administrator wants to configure 802.1x port-based authentication, however, the client workstation is not 802.1x compliant. What is the only supported authentication server that can be used?

- A. TACACS with LEAP extensions
- B. TACACS+
- C. RADIUS with EAP extensions
- D. LDAP

Answer: C

Explanation:

The IEEE 8021x standard defines a port-based access control and authentication protocol that restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports. The authentication server authenticates each workstation that is connected to a switch port before making available any services offered by the switch or the LAN.

Until the workstation is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the workstation is connected. After authentication succeeds, normal traffic can pass through the port.

With 802.1x port-based authentication, the devices in the network have specific roles as, as follows:

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/Sw8021x.html

QUESTION NO: 122

Which statement about 802.1x port-based authentication is true?

- A. Hosts are required to have an 802.1x authentication client or utilize PPPoE.
- B. Before transmitting data, an 802.1x host must determine the authorization state of the switch.
- C. RADIUS is the only supported authentication server type.
- D. If a host initiates the authentication process and does not receive a response, it assumes it is not authorized.

Answer: C

Explanation:

The IEEE 802.1x standard defines a port-based access control and authentication protocol that restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports. The authentication server authenticates each workstation that is connected to a switch port before making available any services offered by the switch or the LAN. Until the workstation is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the workstation is connected. After authentication succeeds, normal traffic can pass through the port.

Authentication server: Performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. The RADIUS security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server.

Reference: Configuring 802.1X Port-Based Authentication

(http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_55_se/configuration/guide/sw8021x.html)

QUESTION NO: 123

In the use of 802.1X access control, which three protocols are allowed through the switch port before authentication takes place? Select three.

- A. STP
- B. CDP
- C. EAP MD5
- D. TACACS+
- E. EAP-over-LAN
- F. protocols not filtered by an ACL

Answer: A,B,E

Explanation:

The IEEE 802.1x standard defines a port-based access control and authentication protocol that restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports. The authentication server authenticates each workstation that is connected to a switch port before making available any services offered by the switch or the LAN. Until the workstation is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN

(EAPOL) traffic through the port to which the workstation is connected. After authentication succeeds, normal traffic can pass through the port.

The Authentication server performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

Spanning-Tree Protocol (STP) is a Layer 2 protocol that utilizes a special-purpose algorithm to discover physical loops in a network and effect a logical loop-free topology. STP creates a loop-free tree structure consisting of leaves and branches that span the entire Layer 2 network. The actual mechanics of how bridges communicate and how the STP algorithm works will be discussed at length in the following topics. Note that the terms bridge and switch are used interchangeably when discussing STP. In addition, unless otherwise indicated, connections between switches are assumed to be trunks.

CDP is a Cisco proprietary protocol that operates at the Data Link layer. One unique feature about operating at Layer 2 is that CDP functions regardless of what Physical layer media you are using (UTP, fiber, and so on) and what Network layer routed protocols you are running (IP, IPX, AppleTalk, and so on). CDP is enabled on all Cisco devices by default, and is multicast every 60 seconds out of all functioning interfaces, enabling neighbor Cisco devices to collect information about each other. Although this is a multicast message, Cisco switches do not flood that out to all their neighbors as they do a normal multicast or broadcast.

For STP, CDP and EAP-over-LAN are allowed before Authentication.

Topic 3, Implement Switch based Layer 3 services, given a network design and a set of requirements

QUESTION NO: 124

Which two characteristics apply to Cisco Catalyst 6500 Series Switch supervisor redundancy using NSF? (Choose two.)

- A.** supported by RIPv2, OSPF, IS-IS, and EIGRP
- B.** uses the FIB table
- C.** supports IPv4 and IPv6 multicast

- D. prevents route flapping
- E. independent of SSO
- F. NSF combined with SSO enables supervisor engine load balancing

Answer: B,D

Explanation:

A key element of NSF is packet forwarding. In a Cisco networking device, packet forwarding is provided by Cisco Express Forwarding (CEF). CEF maintains the FIB, and uses the FIB information that was current at the time of the switchover to continue forwarding packets during a switchover. This feature reduces traffic interruption during the switchover.

During normal NSF operation, CEF on the active supervisor engine synchronizes its current FIB and adjacency databases with the FIB and adjacency databases on the redundant supervisor engine. Upon switchover of the active supervisor engine, the redundant supervisor engine initially has FIB and adjacency databases that are mirror images of those that were current on the active supervisor engine. For platforms with intelligent modules, the modules will maintain the current forwarding information over a switchover. For platforms with forwarding engines, CEF will keep the forwarding engine on the redundant supervisor engine current with changes that are sent to it by CEF on the active supervisor engine. The modules or forwarding engines will be able to continue forwarding after a switchover as soon as the interfaces and a data path are available.

As the routing protocols start to repopulate the RIB on a prefix-by-prefix basis, the updates will cause prefix-by-prefix updates to CEF, which it uses to update the FIB and adjacency databases. Existing and new entries will receive the new version ("epoch") number, indicating that they have been refreshed. The forwarding information is updated on the modules or forwarding engine during convergence. The supervisor engine signals when the RIB has converged. The software removes all FIB and adjacency entries that have an epoch older than the current switchover epoch. The FIB now represents the newest routing protocol forwarding information.

QUESTION NO: 125

Which statement best describes implementing a Layer 3 EtherChannel?

- A. EtherChannel is a Layer 2 feature and not a Layer 3 feature.
- B. Implementation requires switchport mode trunk and matching parameters between switches.
- C. Implementation requires disabling switchport mode.
- D. A Layer 3 address is assigned to the physical interface.

Answer: C

Explanation:

To enable Layer 3 EtherChannel all interfaces participating in channel creation must be in routing mode. To move interface from switching mode to routing mode one uses the command `no switchport`.

Reference:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.1E/native/configuration/guide/channel.html>

QUESTION NO: 126

Refer to the exhibit.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport autostate exclude
Switch(config-if)# exit
```

You have configured an interface to be an SVI for Layer 3 routing capabilities. Assuming that all VLANs have been correctly configured, what can be determined?

- A.** Interface gigabitethernet0/2 will be excluded from Layer 2 switching and enabled for Layer 3 routing.
- B.** The command `switchport autostate exclude` should be entered in global configuration mode, not subinterface mode, to enable a Layer 2 port to be configured for Layer 3 routing.
- C.** The configured port is excluded in the calculation of the status of the SVI.
- D.** The interface is missing IP configuration parameters; therefore, it will only function at Layer 2.

Answer: C

Explanation:

The SVI Autostate exclude feature shuts down (or brings up) the Layer 3 interfaces of a switch when the following port configuration changes occur:

- When the last port on a VLAN goes down, the Layer 3 interface on that VLAN is shut down (SVI-autostated).
- When the first port on the VLAN is brought back up, the Layer 3 interface on the VLAN that was previously shut down is brought up.

SVI Autostate exclude enables you to exclude the access ports/trunks in defining the status of the

SVI (up or down) even if it belongs to the same VLAN. Moreover, even if the excluded access port/trunk is in up state and other ports are in down state in the VLAN, the SVI state is changed to down. At least one port in the VLAN should be up and not excluded to make the SVI state "up." This will help to exclude the monitoring port status when you are determining the status of the SVI.

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/37sg/configuration/guides/l3_int.html#wp1043983

QUESTION NO: 127

Refer to the exhibit.

```
Switch# show ip cef vlan 30 detail
IP CEF with switching (Table Version 11), flags=0x0
10 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 0
13 leaves, 12 nodes, 14248 bytes, 14 inserts, 1 invalidations
0 load sharing elements, 0 bytes, 0 references
universal per-destination load sharing algorithm, id 4B936A24
2(0) CEF resets, 0 revisions of existing leaves
Resolution Timer: Exponential (currently 1s, peak 1s)
0 in-place/0 aborted modifications
refcounts: 1061 leaf, 1052 node
Table epoch: 0 (13 entries at this epoch)
10.1.30.0/24, version 6, epoch 0, attached, connected
0 packets, 0 bytes
via Vlan30, 0 dependencies
valid glean adjacency
```

Which statement is true?

- A. Cisco Express Forwarding load balancing has been disabled.
- B. SVI VLAN 30 connects directly to the 10.1.30.0/24 network due to a valid glean adjacency.
- C. VLAN 30 is not operational because no packet or byte counts are indicated.
- D. The IP Cisco Express Forwarding configuration is capable of supporting IPv6.

Answer: B

Explanation:

Based on the output shown the VLAN 30 connects directly to the 10.1.30.0/24 network and glean adjacency is valid. When a router is connected directly to several hosts, the FIB table on the router maintains a prefix for the subnet rather than for the individual host prefixes. The subnet prefix points to a glean adjacency. When packets need to be forwarded to a specific host, the adjacency database is gleaned for the specific prefix

Reference:

http://www.cisco.com/en/US/docs/ios/ipswitch/command/reference/isw_s1.html#wp1123733

http://www.cisco.com/en/US/products/hw/modules/ps2033/prod_technical_reference09186a00800afeb7.html

QUESTION NO: 128

Refer to exhibit as:

```
Switch# show ip eigrp neighbors
EIGRP-IPv4:(20) neighbors for process 20
```

Which statement about the EIGRP routing being performed by the switch is true?

- A. The EIGRP neighbor table contains 20 neighbors.
- B. EIGRP is running normally and receiving IPv4 routing updates.
- C. EIGRP status cannot be determined. The command show ip eigrp topology would determine the routing protocol status.
- D. The switch has not established any neighbor relationships. Further network testing and troubleshooting must be performed to determine the cause of the problem.

Answer: D

Explanation:

There is no record for EIGRP neighbor in the output of the command. It means that the switch has not established any neighbor relationships and further network testing and troubleshooting must be performed to determine the cause of the problem.

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_25_se/configuration/guide/swiprout.html#wp1067796

QUESTION NO: 129

You have configured a Cisco Catalyst switch to perform Layer 3 routing via an SVI and you have assigned that interface to VLAN 20. To check the status of the SVI, you issue the show interfaces vlan 20 command at the CLI prompt. You see from the output display that the interface is in an up/up state. What must be true in an SVI configuration to bring the VLAN and line protocol up?

- A.** The port must be physically connected to another Layer 3 device.
- B.** At least one port in VLAN 20 must be active.
- C.** The Layer 3 routing protocol must be operational and receiving routing updates from neighboring peer devices.
- D.** Because this is a virtual interface, the operational status is always in an "up/up" state.

Answer: B

Explanation:

The SVI interfaces have to fulfill the following general conditions to be up/up:

- VLAN exists and is in active status on the switch VLAN database.
 - VLAN interface exists on the router and is not administratively down.
 - At least one L2 (access port or trunk) port exists and has a link up on this VLAN. The latest implementation of the autostate feature allows synchronization to Spanning-Tree Protocol (STP) port status.
 - A VLAN interface will be brought up after the L2 port has had time to converge (that is, transition from listening-learning to forwarding). This will prevent routing protocols and other features from using the VLAN interface as if it were fully operational. This also prevents other problems, such as routing black holes, from occurring.
 - At least one L2 (access port or trunk) port is in spanning-tree forwarding state on the VLAN.
- So for SVI to bring the vlan and line protocol up at least one port in that vlan must be active.

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a0080160b14.shtml

QUESTION NO: 130

Refer to the exhibit, which is from a Cisco Catalyst 3560 Series Switch.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.20.135.21 255.255.255.0
Switch(config-if)# no shutdown
```

Which statement about the Layer 3 routing functionality of the interface is true?

- A. The interface is configured correctly for Layer 3 routing capabilities.
- B. The interface needs an additional configuration entry to enable IP routing protocols.
- C. Since the interface is connected to a host device, the spanning-tree portfast command must be added to the interface.
- D. An SVI interface is needed to enable IP routing for network 192.20.135.0.

Answer: A

Explanation:

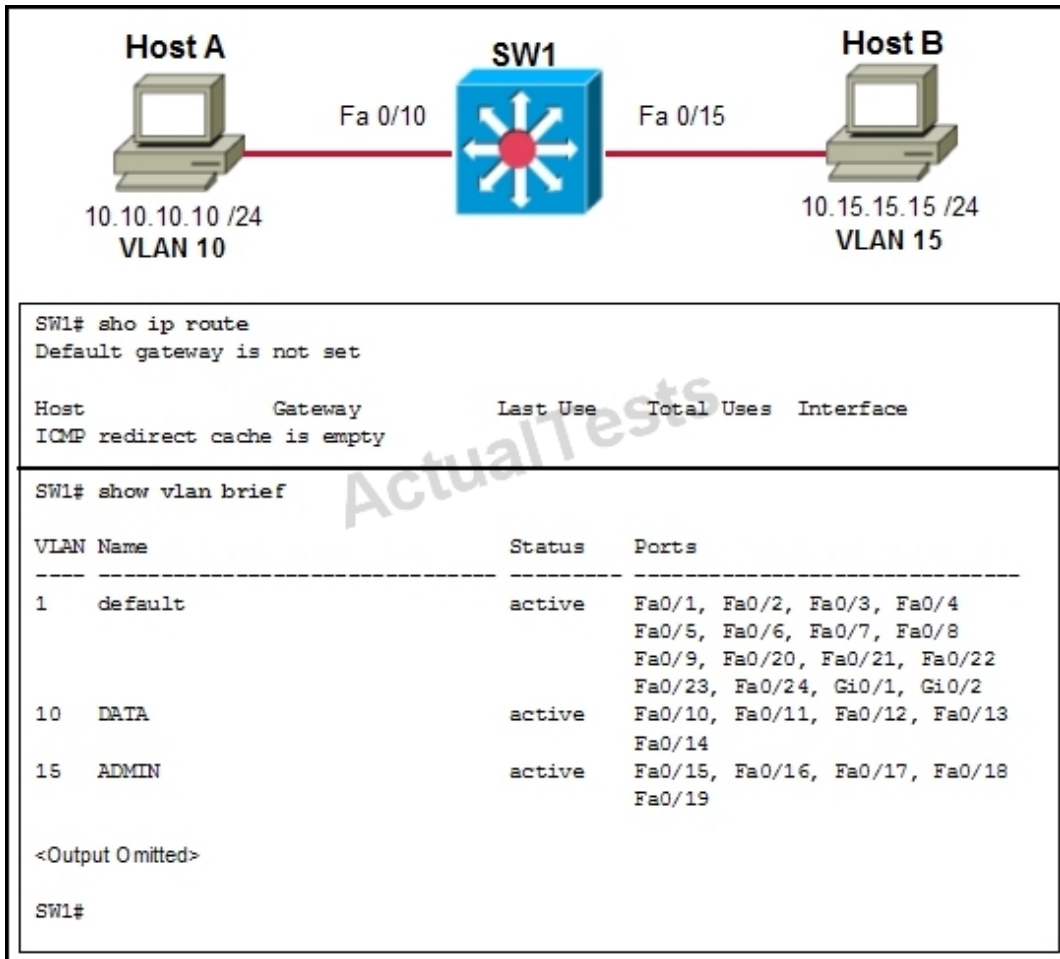
The command “no switchport” indicates that interface gi0/2 is configured correctly for Layer 3 routing capability.

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_50_se/configuration/guide/swint.html#wp2028366

QUESTION NO: 131

Refer to the exhibit.



Host A and Host B are connected to the Cisco Catalyst 3550 switch and have been assigned to their respective VLANs. The rest of the 3550 configuration is the default configuration. Host A is able to ping its default gateway, 10.10.10.1, but is unable to ping Host B. Given the output in the exhibit, which statement is true?

- A. HSRP must be configured on SW1.
- B. A separate router is needed to support inter-VLAN routing.
- C. Interface VLAN 10 must be configured on the SW1 switch.
- D. The global configuration command `ip routing` must be configured on the SW1 switch.
- E. VLANs 10 and 15 must be created in the VLAN database mode.
- F. VTP must be configured to support inter-VLAN routing.

Answer: D

Explanation:

To transport packets between VLANs, you must use a Layer 3 device. Traditionally, this has been a router's function. The router must have a physical or logical connection to each VLAN so that it can forward packets between them. This is known as interVLAN routing.

Multilayer switches can perform both Layer 2 switching and interVLAN routing, as appropriate. Layer 2 switching occurs between interfaces that are assigned to Layer 2 VLANs or Layer 2 trunks. Layer 3 switching can occur between any type of interface, as long as the interface can have a Layer 3 address assigned to it.

Switch(config)#ip routing command enables the routing on Layer 3 Switch

References

http://www.cisco.com/en/US/tech/tk389/tk815/technologies_configuration_example09186a00800949fd.shtml

http://www.net130.com/tutorial/cisco-pdf/howto_L3_intervlanrouting.pdf

QUESTION NO: 132 DRAG DROP

You have a VLAN implementation that requires inter-VLAN routing using Layer 3 switches. Drag the steps from the left to the right that should be part of the verification plan. Not all choices will be used.

Verify that VTP is pruning the proper access ports.	
Verify that there is inter-switch connectivity.	
Verify that the data and voice VLANs are NOT assigned a trunk's native VLAN.	
Verify that the needed switch virtual interfaces have been created.	
Verify that the VLAN ports are in promiscuous mode.	
Verify that the proper ports are assigned to the VLAN.	

Answer:

You have a VLAN implementation that requires inter-VLAN routing using Layer 3 switches. Drag the steps from the left to the right that should be part of the verification plan. Not all choices will be used.

Verify that VTP is pruning the proper access ports.	Verify that there is inter-switch connectivity.
Verify that there is inter-switch connectivity.	Verify that the data and voice VLANs are NOT assigned a trunk's native VLAN.
Verify that the data and voice VLANs are NOT assigned a trunk's native VLAN.	Verify that the needed switch virtual interfaces have been created.
Verify that the needed switch virtual interfaces have been created.	Verify that the proper ports are assigned to the VLAN.
Verify that the VLAN ports are in promiscuous mode.	
Verify that the proper ports are assigned to the VLAN.	

Explanation:

Verify that there is inter-switch connectivity.

Verify that the data and voice VLANs are NOT assigned a trunk's native VLAN.

Verify that the needed switch virtual interfaces have been created.

Verify that the proper ports are assigned to the VLAN.

QUESTION NO: 133

Which three statements about routed ports on a multilayer switch are true? (Choose three.)

- A. A routed port can support VLAN subinterfaces.
- B. A routed port takes an IP address assignment.
- C. A routed port can be configured with routing protocols.
- D. A routed port is a virtual interface on the multilayer switch.
- E. A routed port is associated only with one VLAN.
- F. A routed port is a physical interface on the multilayer switch.

Answer: B,C,F

Explanation: The router must have a separate logical connection (subinterface) for each VLAN that is running between the switch and the router and ISL, or 802.1Q trunking must be enable on the single physical connection between the router and switch.

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_37_se/configuration/guide/swint.html#wp1810955

QUESTION NO: 134

Which two steps are necessary to configure inter-VLAN routing between multilayer switches?
(Choose two.)

- A. Configure a dynamic routing protocol.
- B. Configure SVI interfaces with IP addresses and subnet masks.
- C. Configure access ports with network addresses.
- D. Configure switch ports with the autostate exclude command.
- E. Document the MAC addresses of the switch ports.

Answer: A,B

Explanation:

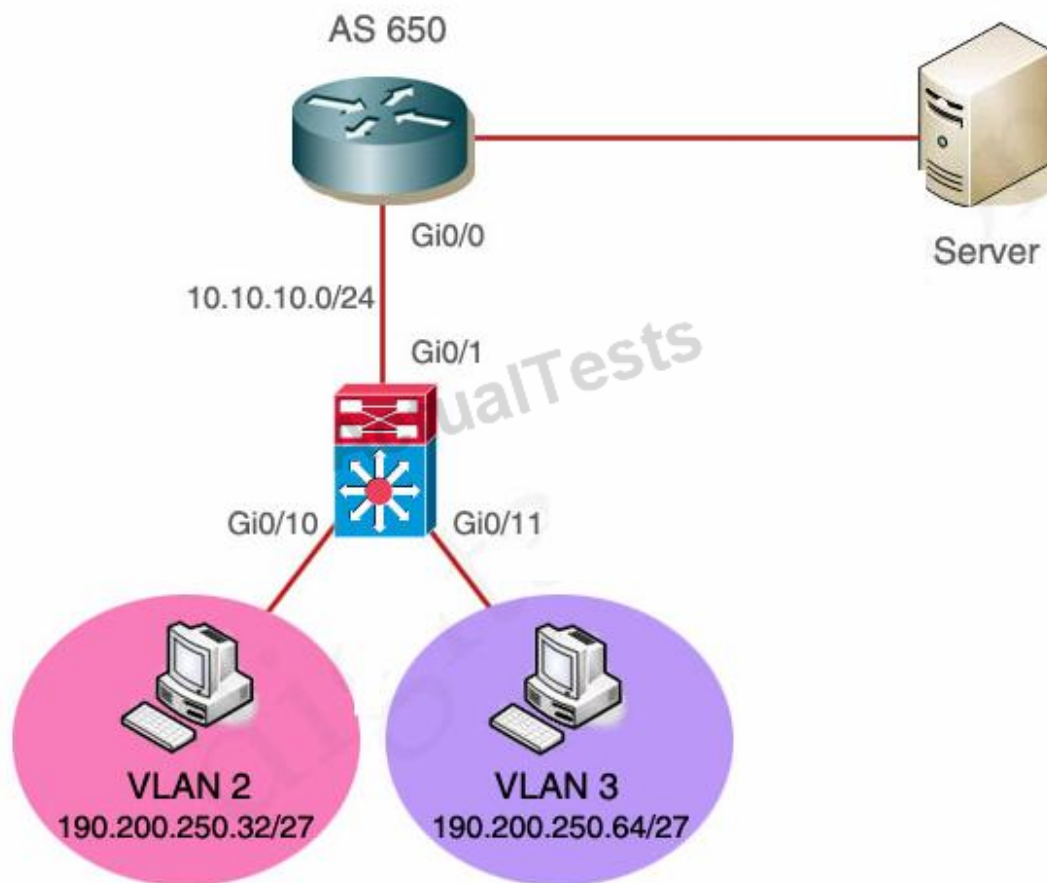
To be honest configuration of dynamic routing protocol is not necessary to enable inter VLAN routing between multilayer switches. The static routing would be enough. But as question requires choosing two answers you are constrained to choose answer A beside the obvious answer B.

Reference:

http://www.cisco.com/en/US/tech/tk389/tk815/technologies_configuration_example09186a008019e74e.shtml

QUESTION NO: 135 CORRECT TEXT

Configure the Multilayer Switch so that PCs from VLAN 2 and VLAN 3 can communicate with the Server.



Answer: mls>enable

mls# configure terminal

mls(config)# int gi0/1

mls(config-if)#no switchport -> not sure about this command line, but you should use this command if the simulator does not let you assign IP address on Gi0/1 interface.

mls(config-if)# ip address 10.10.10.2 255.255.255.0

mls(config-if)# no shutdown

mls(config-if)# exit

mls(config)# int vlan 2

mls(config-if)# ip address 190.200.250.33 255.255.255.224

mls(config-if)# no shutdown

mls(config-if)# int vlan 3

mls(config-if)# ip address 190.200.250.65 255.255.255.224

mls(config-if)# no shutdown

mls(config-if)#exit

mls(config)#interface gig 0/10

mls(config)#switchport mode access

mls(config)#switchport access vlan 2

mls(config)#no shutdown

mls(config)#exit

```
mls(config)#interface gig 0/11
mls(config)#switchport mode access
mls(config)#switchport access vlan 3
mls(config)#no shutdown
mls(config)# ip routing (Notice: MLS will not work without this command)
mls(config)# router eigrp 650
mls(config-router)# network 10.10.10.0 0.0.0.255
mls(config-router)# network 190.200.250.32 0.0.0.31
mls(config-router)# network 190.200.250.64 0.0.0.31
```

NOTE : THE ROUTER IS CORRECTLY CONFIGURED, so you will not miss within it in the exam , also don't modify/delete any port just do the above configuration.

in order to complete the lab , you should expect the ping to SERVER to succeed from the MLS , and from the PCs as well.

If the above configuration does not work, you should configure EIGRP with "no auto-summary" command:

```
no auto-summary
```

QUESTION NO: 136

When configuring a routed port on a Cisco multilayer switch, which configuration task is needed to enable that port to function as a routed port?

- A.** Enable the switch to participate in routing updates from external devices with the router command in global configuration mode.
- B.** Enter the no switchport command to disable Layer 2 functionality at the interface level.
- C.** Each port participating in routing of Layer 3 packets must have an IP routing protocol assigned on a per-interface level.
- D.** Routing is enabled by default on a multilayer switch, so the port can become a Layer 3 routing interface by assigning the appropriate IP address and subnet information.

Answer: B

Explanation:

To disable Layer 2 functionality at the interface level the command no switchport is used. This command switches the port status from switched to routed.

Reference:

http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_s7.html#wp1012629

Topic 4, Prepare infrastructure to support advanced services**QUESTION NO: 137**

A standalone wireless AP solution is being installed into the campus infrastructure. The access points appear to boot correctly, but wireless clients are not obtaining correct access. You verify that this is the local switch configuration connected to the access point:

```
interface ethernet 0/1
```

```
switchport access vlan 10
```

```
switchport mode access
```

```
spanning-tree portfast
```

```
mls qos trust dscp
```

What is the most likely cause of the problem?

- A. QoS trust should not be configured on a port attached to a standalone AP.
- B. QoS trust for switchport mode access should be defined as "cos".
- C. switchport mode should be defined as "trunk" with respective QoS.
- D. switchport access vlan should be defined as "1".

Answer: C

Explanation:

VLANs could be extended into a wireless LAN by adding IEEE 802.11Q tag awareness to the access point. Frames destined for different VLANs are transmitted by the access point wirelessly on different SSIDs with different WEP keys. Only the clients associated with that VLAN receive those packets. Conversely, packets coming from a client associated with a certain VLAN are 802.11Q tagged before they are forwarded onto the wired network. If 802.1q is configured on the FastEthernet interface of an access point, the access point always sends keepalives on VLAN1 even if VLAN 1 is not defined on the access point. As a result, the Ethernet switch connects to the access point and generates a warning message. There is no loss of function on both the access point and the switch. However, the switch log contains meaningless messages that may cause more important messages to be wrapped and not be seen.

This behavior creates a problem when all SSIDs on an access point are associated to mobility networks. If all SSIDs are associated to mobility networks, the Ethernet switch port the access

point is connected to can be configured as an access port. The access port is normally assigned to the native VLAN of the access point, which is not necessarily VLAN1, which causes the Ethernet switch to generate warning messages saying that traffic with an 802.1q tag is sent from the access point.

Reference:

http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg124_10b-chap14-vlan.html

http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg124_10b-chap15-qos.html

QUESTION NO: 138

During the implementation of a voice solution, which two required items are configured at an access layer switch that will be connected to an IP phone to provide VoIP communication? (Choose two.)

- A. allowed codecs
- B. untagged VLAN
- C. auxiliary VLAN
- D. Cisco Unified Communications Manager IP address
- E. RSTP

Answer: B,C

Reference: <http://networkingnerd.net/2012/05/09/switchport-voice-vlan-post/>

QUESTION NO: 139

Which two statements best describe Cisco IOS IP SLA? (Choose two.)

- A. only implemented between Cisco source and destination-capable devices
- B. statistics provided by syslog, CLI, and SNMP
- C. measures delay, jitter, packet loss, and voice quality
- D. only monitors VoIP traffic flows
- E. provides active monitoring

Answer: C,E

Explanation:

Cisco IOS IP SLAs allows you to monitor, analyze and verify IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce occurrences of network congestion or outages. IP SLAs uses active traffic monitoring for measuring network performance. IP SLAs can be configured to react to certain measured network conditions. For example, if IP SLAs measures too much jitter on a connection, IP SLAs can generate a notification to a network management application, or trigger another IP SLAs operation to gather more data. IP SLAs includes the capability for triggering SNMP notifications based on defined thresholds. This allows for proactive monitoring in an environment where IT departments can be alerted to potential network problems, rather than having to manually examine data. IP SLAs supports threshold monitoring for performance parameters such as average jitter, unidirectional latency and bidirectional round trip time and connectivity. This proactive monitoring capability provides options for configuring reaction thresholds for important VoIP related parameters including unidirectional jitter, unidirectional packet loss, and unidirectional VoIP voice quality scoring (MOS scores). For packet loss and jitter, notifications can be generated for violations in either direction (source to destination and destination to source) or for round trip values. Packet loss, jitter and MOS statistics are specific to IP SLAs Jitter operations. Notifications can also be triggered for other events, such as round-trip-time violations, for most IP SLAs monitoring operations.

Reference:

http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsoverv.html

QUESTION NO: 140

Which two items best describe a Cisco IOS IP SLA responder? (Choose two.)

- A. required at the destination to implement Cisco IOS IP SLA services
- B. improves measurement accuracy
- C. required for VoIP jitter measurements
- D. provides security on Cisco IOS IP SLA messages via LEAP or EAP-FAST authentication
- E. responds to one Cisco IOS IP SLA operation per port
- F. stores the resulting test statistics

Answer: B,C**Explanation:**

The Cisco IOS IP SLAs Responder is a component embedded in the destination Cisco routing device that allows the system to anticipate and respond to Cisco IOS IP SLAs request packets. The Cisco IOS IP SLAs Responder provides an enormous advantage with accurate measurements without the need for dedicated probes and additional statistics not available via

standard ICMP-based measurements. The patented Cisco IOS IP SLAs Control Protocol is used by the Cisco IOS IP SLAs Responder providing a mechanism through which the responder can be notified on which port it should listen and respond. Only a Cisco IOS device can be a source for a destination IP SLAs Responder. For IP SLAs VoIP UDP Jitter Operations your networking devices on both ends of the connection must support Cisco IOS IP SLAs.

Reference:

http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsoverv.html

QUESTION NO: 141

What does the interface subcommand `switchport voice vlan 222` indicate?

- A. The port is configured for both data and voice traffic.
- B. The port is fully dedicated to forwarding voice traffic.
- C. The port operates as an FXS telephony port.
- D. Voice traffic is directed to VLAN 222.

Answer: A

Explanation:

The interface subcommand:

```
Switch(config-if)# switchport voice vlan {vlan-id | dot1p | untagged | none}
```

is used to select the voice VLAN mode that will be used when PC is connected to the switch port through Cisco IP phone.

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_20_se/configuration/guide/swvoip.html

QUESTION NO: 142 DRAG DROP

This is a drag and drop question which is about the correct sequence of steps that a wireless client takes during the process of association with an access point (AP). Drag the items to the proper locations.

A --- Client initiates association process.	1
B --- Access point accepts association of the client.	2
C --- Client sends probe request.	3
D --- Access point sends probe response or beacon.	4
E --- AP adds client MAC address to association table.	5

Answer:

A --- Client initiates association process.	C --- Client sends probe request.
B --- Access point accepts association of the client.	D --- Access point sends probe response or beacon.
C --- Client sends probe request.	A --- Client initiates association process.
D --- Access point sends probe response or beacon.	B --- Access point accepts association of the client.
E --- AP adds client MAC address to association table.	E --- AP adds client MAC address to association table.

Explanation:

A --- Client initiates association process.	C --- Client sends probe request.
B --- Access point accepts association of the client.	D --- Access point sends probe response or beacon.
C --- Client sends probe request.	A --- Client initiates association process.
D --- Access point sends probe response or beacon.	B --- Access point accepts association of the client.
E --- AP adds client MAC address to association table.	E --- AP adds client MAC address to association table.

1. Client sends probe request.
2. Access point sends probe response.
3. Client initiates association.
4. Access point accepts association.
5. Access point adds client MAC address to association table

References

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_white_paper09186a0080901caa.shtml

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_white_paper09186a0080901caa.shtml

QUESTION NO: 143

A campus infrastructure supports wireless clients via Cisco Aironet AG Series 1230, 1240, and 1250 access points. With DNS and DHCP configured, the 1230 and 1240 access points appear to boot and operate normally. However, the 1250 access points do not seem to operate correctly.

What is the most likely cause of this problem?

- A. DHCP with option 150
- B. DHCP with option 43
- C. PoE
- D. DNS
- E. switch port does not support gigabit speeds

Answer: C

Explanation:

Cisco Aironet 1250 Series Access Point can be powered locally by the 1250 DC power module or an IEEE 802.3af compliant Power-over-Ethernet (PoE) power source. However, if the access point is powered by an 802.3af source, only one radio is supported because the two radio operation requires 18.5 watts. Two radio operation is supported only by the 1250 series power injector and an 802.at compliant PoE switch.

Reference:

http://www.cisco.com/en/US/docs/wireless/access_point/1250/quick/guide/ap1250qs.html

QUESTION NO: 144

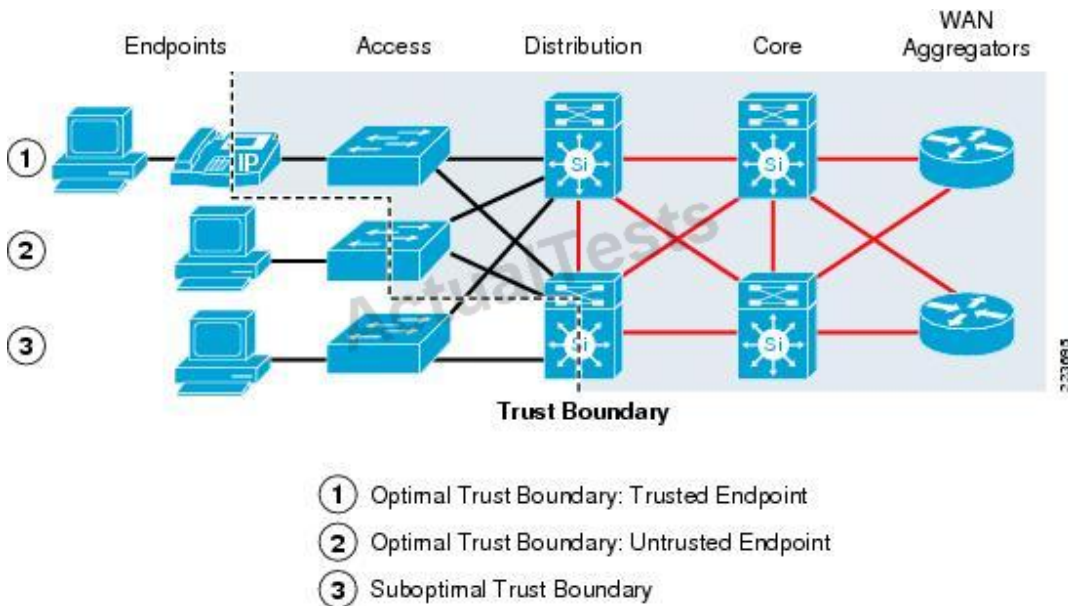
A network is deployed using recommended practices of the enterprise campus network model, including users with desktop computers connected via IP phones. Given that all components are QoS-capable, where are the two optimal locations for trust boundaries to be configured by the network administrator? (Choose two.)

- A. host
- B. IP phone
- C. access layer switch

- D. distribution layer switch
- E. core layer switch

Answer: B,C

Explanation:



In the current campus QoS design, the access ports of each switch are configured to not trust the QoS markings of any traffic arriving on that port—unless it is on the auxiliary or voice VLAN and the switch has detected that there is a phone (trusted device) on that VLAN. The decision to trust or not trust the endpoints traffic is binary; either the traffic is from the phone and trusted or from any other device and not trusted. This model works well in an environment with dedicated phones, but as the trends in Unified Communications continue and voice/video applications start merging with other PC applications, the need to selectively and intelligently trust certain application flows from the untrusted PC is becoming necessary. The use of per VLAN and per port traffic policers is one mechanism that is used to selectively trust traffic in certain port ranges and at certain data rates. Each edge port can be configured to detect traffic within a specific port range and, for all traffic that is less than a defined normal rate, mark that traffic with the correct DSCP values. All traffic in excess of this rate is dropped, which provides a safety mechanism to protect against one application masquerading as another more mission critical one (by using the more important application's port numbers for communication). While this policer-based approach has proven to work well and is still valid for certain environments, the increasingly complex list of applications that share port numbers and applications that might be hijacking other applications trusted port ranges requires that we consider a more sophisticated approach.

Reference:

<http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html#wp709277>

QUESTION NO: 145 DRAG DROP

Prioritize the traffic types by dragging them from the left to the appropriate Cisco priority level on the right. Put the highest priority at the top and the lowest priority at the bottom.

network management	
video - interactive	
IP routing	
voice	
video - streaming	
call signaling	

Answer:

Prioritize the traffic types by dragging them from the left to the appropriate Cisco priority level on the right. Put the highest priority at the top and the lowest priority at the bottom.

network management	voice
video - interactive	video - interactive
IP routing	video - streaming
voice	call signaling
video - streaming	IP routing
call signaling	network management

Explanation:

voice
video - interactive
video - streaming
call signaling
IP routing
network management

Topic 5, Implement High Availability, given a network design and a set of requirements**QUESTION NO: 146**

Refer to the exhibit.

```
Switch_A(config-if)# ip address 10.10.10.1 255.255.255.0
Switch_A(config-if)# standby 1 priority 200
Switch_A(config-if)# standby 1 preempt
Switch_A(config-if)# standby 1 track interface fa 1/1
Switch_A(config-if)# standby 1 ip 10.10.10.10
```

Assume that Switch_A is active for the standby group and the standby device has only the default HSRP configuration. Which statement is true?

- A.** If port Fa1/1 on Switch_A goes down, the standby device takes over as active.
- B.** If the current standby device had the higher priority value, it would take over the role of active for the HSRP group.
- C.** If port Fa1/1 on Switch_A goes down, the new priority value for the switch would be 190.
- D.** If Switch_A had the highest priority number, it would not take over as active router.

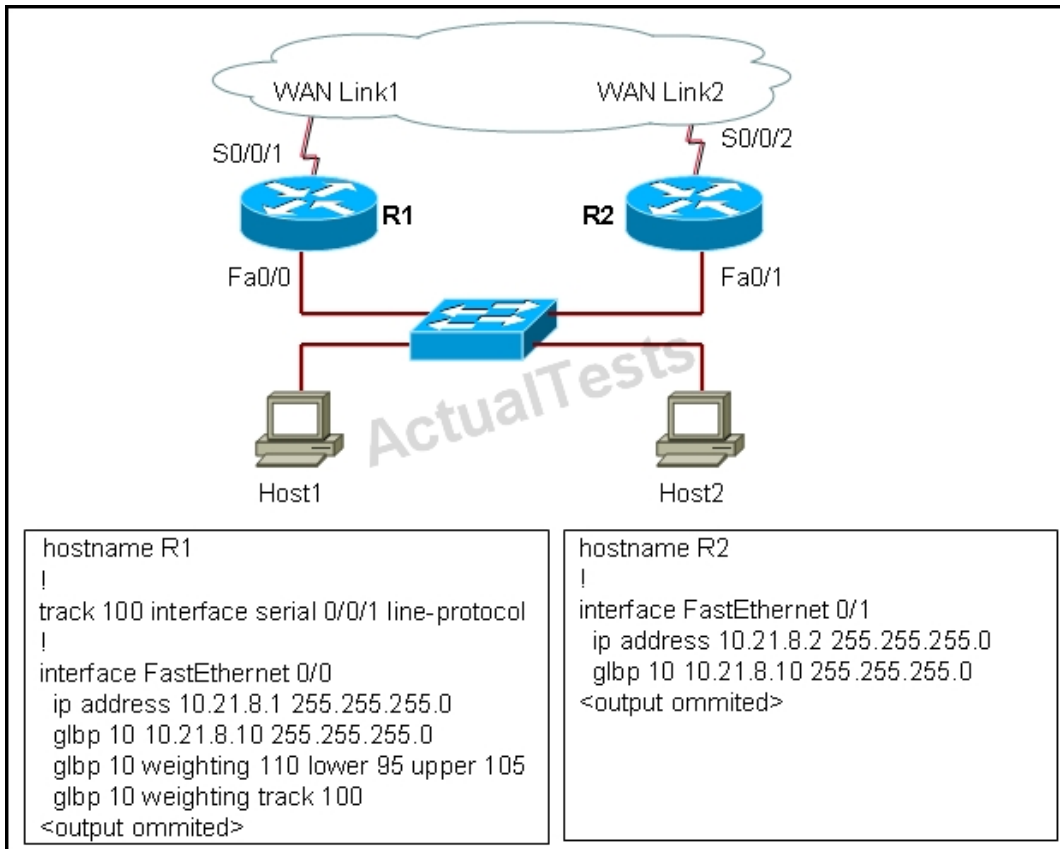
Answer: C

Explanation:

Switch_A is not configured standby track priority value so it will use the default track priority of 10 -
> When Switch_A goes down, its priority is $200 - 10 = 190$

QUESTION NO: 147

Refer to the exhibit.



GLBP has been configured on the network. When the interface serial0/0/1 on router R1 goes down, how is the traffic coming from Host1 handled?

- A. The traffic coming from Host1 and Host2 is forwarded through router R2 with no disruption.
- B. The traffic coming from Host2 is forwarded through router R2 with no disruption. Host1 sends an ARP request to resolve the MAC address for the new virtual gateway.
- C. The traffic coming from both hosts is temporarily interrupted while the switchover to make R2 active occurs.
- D. The traffic coming from Host2 is forwarded through router R2 with no disruption. The traffic from Host1 is dropped due to the disruption of the load balancing feature configured for the GLBP group.

Answer: A

Explanation: The Gateway Load Balancing Protocol (GLBP) is a Cisco-proprietary protocol designed to overcome the limitations of existing redundant router protocols. Some of the concepts are the same as with HSRP/VRRP, but the terminology is different and the behavior is much more dynamic and robust and allows for load balancing.

The trick behind this load balancing lies in the GLBP group. One router is elected the active virtual gateway (AVG). This router has the highest priority value, or the highest IP address in the group, if there is no highest priority. The AVG answers all ARP requests for the virtual router address.

Which MAC address it returns depends on which load-balancing algorithm it is configured to use.

In any event, the virtual MAC address supported by one of the routers in the group is returned.

According to exhibit, Company1 is the active virtual gateway and Company2 is the standby virtual

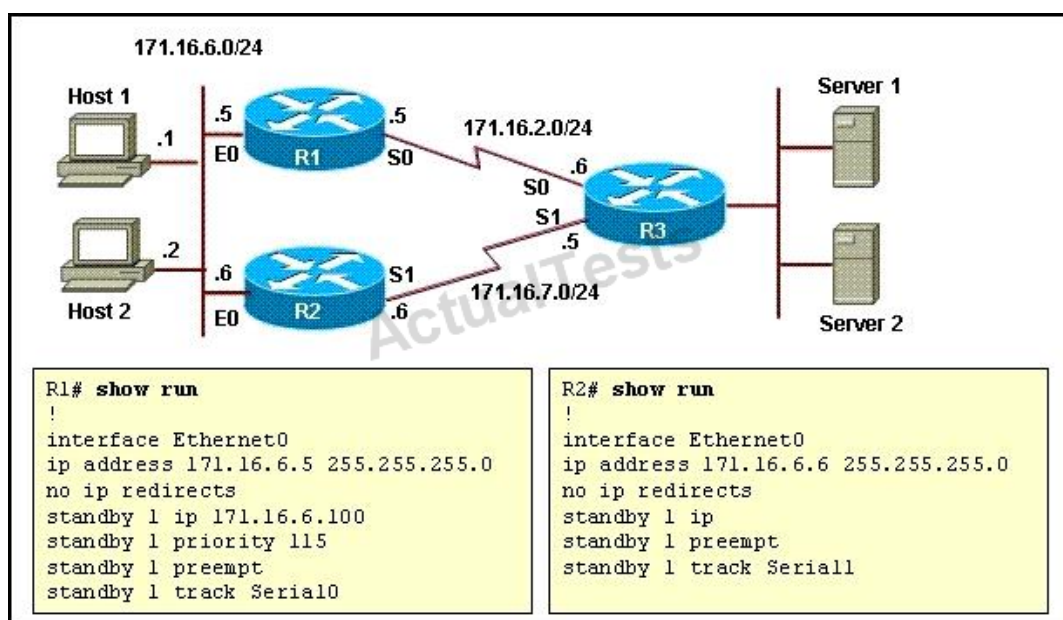
gateway. So, when Company1 goes down, Company2 will become active virtual gateway and all data goes through Company2.

Reference: Configuring GLBP

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_glb_p6922_TSD_Products_Configuration_Guide_Chapter.html#wp1055542

QUESTION NO: 148

Refer to the exhibit and the partial configuration on routers R1 and R2.



HSRP is configured on the network to provide network redundancy for the IP traffic. The network administrator noticed that R2 does not become active when the R1 serial0 interface goes down. What should be changed in the configuration to fix the problem?

- A. R2 should be configured with an HSRP virtual address.
- B. R2 should be configured with a standby priority of 100.
- C. The Serial0 interface on router R2 should be configured with a decrement value of 20.
- D. The Serial0 interface on router R1 should be configured with a decrement value of 20.

Answer: D

Explanation:

You can configure a router to preempt or immediately take over the active role if its priority is the highest at any time. Use the following interface configuration command to allow preemption:

Switch(config-if)# standby group preempt [delay seconds]

By default, the router can preempt another immediately, without delay. You can use the delay keyword to force it to wait for seconds before becoming active. This is usually done if there are routing protocols that need time to converge.

Reference: Configuring HSRP

(http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_12c_ea1/configuration/guide/swhsrp.html)

QUESTION NO: 149

The following command was issued on a router that is being configured as the active HSRP router.

```
standby ip 10.2.1.1
```

Which statement about this command is true?

- A. This command will not work because the HSRP group information is missing.
- B. The HSRP MAC address will be 0000.0c07.ac00.
- C. The HSRP MAC address will be 0000.0c07.ac01.
- D. The HSRP MAC address will be 0000.070c.ac11.
- E. This command will not work because the active parameter is missing.

Answer: B

Explanation:

The full syntax of the command above is:

```
standby [group-number] ip [ip-address [secondary]]
```

Therefore in the command "standby ip 10.2.1.1 we recognize it is using the default group-number, which is 0 -> The last two-digit hex value of HSRP MAC address should be "00.

QUESTION NO: 150

```
hostname Switch1
```

```
interface Vlan10
ip address 172.16.10.32 255.255.255.0
no ip redirects
standby 1 ip 172.16.10.110
standby 1 timers msec 200 msec 700
standby 1 preempt
```

hostname Switch2

```
interface Vlan10
ip address 172.16.10.33 255.255.255.0
no ip redirects
standby 1 ip 172.16.10.110
standby 1 timers msec 200 msec 750
standby 1 priority 110
standby 1 preempt
```

hostname Switch3

```
interface Vlan10
ip address 172.16.10.34 255.255.255.0
no ip redirects
standby 1 ip 172.16.10.110
standby 1 timers msec 200 msec 750
standby 1 priority 150
standby 1 preempt
```

Refer to the above. Three switches are configured for HSRP.

Switch1 remains in the HSRP listen state. What is the most likely cause of this status?

- A. This is normal operation.
- B. The standby group number does not match the VLAN number.
- C. IP addressing is incorrect.
- D. Priority commands are incorrect.
- E. Standby timers are incorrect.

Answer: A

Explanation:

This is expected behavior. When HSRP is configured on an interface, the router progresses through a series of states before becoming active. This forces a router to listen for others in a group and see where it fits into the pecking order. Devices participating in HSRP must progress their interfaces through the following state sequence:

1. Disabled
2. Init
3. Listen
4. Speak
5. Standby
6. Active

Only the standby (the one with the second-highest priority) router monitors the hello message from the active router. By default, hellos are sent every 3 seconds. If hellos are missed for the duration of the holdtime timer (default 10 seconds, or three times the hello timer), the active router is presumed to be down. The standby router is then clear to assume the active role. At that point, if other routers are sitting in the Listen state, the next-highest priority router is allowed to become the new standby router.

Reference:

CCNP BCMSN Official Exam Certification Guide, Fourth Edition, Chapter 13: Router, Supervisor, and Power Redundancy, p. 318

QUESTION NO: 151

Three Cisco Catalyst switches have been configured with a first-hop redundancy protocol. While reviewing some show commands, debug output, and the syslog, you discover the following information:

Jan 9 08:00:42.623: %STANDBY-6-STATECHANGE. Standby: 49:

Vlan149 state Standby -> Active

Jan 9 08:00:56.011: %STANDBY-6-STATECHANGF. Standby: 49:

Vlan149 state Active -> Speak

Jan 9 08:01:03.011: %STANDBY-6-STATECHANGF. Standby: 49:

Vlan149 state Speak -> Standby

Jan 9 08:01:29.427: %STANDBY-6-STATECHANGF. Standby: 49:

Vlan149 state Standby -> Active

Jan 9 08:01:36.808: %STANDBY-6-STATECHANGF. Standby: 49:

Vlan149 state Active -> Speak

Jan 9 08:01:43.808: %STANDBY-6-STATECHANGF. Standby: 49:

Vlan149 state Speak -> Standby

What conclusion can you infer from this information?

- A. VRRP is initializing and operating correctly.
- B. HSRP is initializing and operating correctly.
- C. GLBP is initializing and operating correctly.
- D. VRRP is not exchanging three hello messages properly.
- E. HSRP is not exchanging three hello messages properly.
- F. GLBP is not exchanging three hello messages properly.

Answer: E

Explanation:

These error messages describe a situation in which a standby HSRP router did not receive three successive HSRP hello packets from its HSRP peer. The output shows that the standby router moves from the standby state to the active state. Shortly thereafter, the router returns to the standby state. Unless this error message occurs during the initial installation, an HSRP issue probably does not cause the error message. The error messages signify the loss of HSRP hellos between the peers. When you troubleshoot this issue, you must verify the communication between the HSRP peers. A random, momentary loss of data communication between the peers is the most common problem that results in these messages. HSRP state changes are often due to High CPU Utilization. If the error message is due to high CPU utilization, put a sniffer on the network and trace the system that causes the high CPU utilization. There are several possible causes for the loss of HSRP packets between the peers. The most common problems are physical layer problems, excessive network traffic caused by spanning tree issues or excessive traffic caused by each VLAN.

Reference:

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094afd.shtml#t1

QUESTION NO: 152

Refer to the exhibit.

Switch# show ip arp					
Protocol	Address	Age(min)	Hardware Addr	Type	Interface
Internet	172.16.233.22	9	0000.0c59.f892	ARPA	Vlan10
Internet	172.16.233.21	8	0000.0c63.1300	ARPA	Vlan10
Internet	172.16.233.19	-	0000.0c07.ac0b	ARPA	Vlan10

Which statement best describes first-hop redundancy protocol status?

- A. The first-hop redundancy protocol is not configured for this interface.
- B. HSRP is configured for group 10.
- C. HSRP is configured for group 11.
- D. VRRP is configured for group 10.
- E. VRRP is configured for group 11.
- F. GLBP is configured with a single AVF.

Answer: C

Explanation:

MAC address will be a virtual MAC address composed of 0000.0C07.ACxy, where xy is the HSRP group number in hexadecimal based on the respective interface. When examining the following line: xy value is 0b means the virtual group is 11. Internet 172.16.233.19 0000.0c07.ac0b ARPA Vlan10. So answer "HSRP is configured for group 11" is correct.

Reference:

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094a91.shtml

QUESTION NO: 153

In the hardware address 0000.0c07.ac0a, what does 07.ac represent?

- A. vendor code
- B. HSRP group number
- C. HSRP router number
- D. HSRP well-known physical MAC address
- E. HSRP well-known virtual MAC address

Answer: E

Explanation:

HSRP code (HSRP well-known virtual MAC address) – The fact that the MAC address is for an HSRP virtual router is indicated in the next two bytes of the address. The HSRP code is always 07.ac. The HSRP protocol uses a virtual MAC address, which always contains the 07.ac numerical value.

Reference: Cisco Hot Standby Router Protocol (HSRP)

(<http://tools.ietf.org/html/rfc2281#page-13>)

QUESTION NO: 154

Which protocol will enable a group of routers to form a single virtual router and will use the real IP address of a router as the gateway address?

- A. Proxy ARP
- B. HSRP
- C. IRDP
- D. VRRP
- E. GLBP

Answer: D

Explanation:

The correct answer is VRRP whereby either a virtual or physical address can be chosen as the gateway address. If the physical address of R2 is the gateway address, then R2 will become the gateway. If R2 goes down, R3 (or R4 etc) will become the gateway and will assume the IP address which, to it, will be a virtual one as none of its interfaces are configured with that address. In this scenario, R2, R3 and R4 form one virtual router whereby R1's physical address is used as the gateway address. HSRP does not use physical addresses for the gateway at all.

Reference: Virtual Router Redundancy Protocol

(http://www.cisco.com/en/US/docs/ios/12_0st/12_0st18/feature/guide/st_vrrpx.html)

QUESTION NO: 155

Refer to the exhibit.

```
*Mar 1 00:12:16.871: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:16.871: SB11: V111 Active router is 172.16.11.112
*Mar 1 00:12:18.619: %LINK-3-UPDOWN: Interface Vlan11, changed state to up
*Mar 1 00:12:18.623: SB: V111 Interface up
*Mar 1 00:12:18.623: SB11: V111 Init: a/HSRP enabled
*Mar 1 00:12:18.623: SB11: V111 Init -> Listen
*Mar 1 00:12:19.619: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan11, changed state to up
*Mar 1 00:12:19.819: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:19.819: SB11: V111 Listen: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar 1 00:12:22.815: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:22.815: SB11: V111 Listen: h/Hello rcvd from lower pri Active router
*Mar 1 00:12:25.683: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:25.683: SB11: V111 Listen: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar 1 00:12:28.623: SB11: V111 Listen: d/Standby timer expired (unknown)
*Mar 1 00:12:28.623: SB11: V111 Listen -> Speak
*Mar 1 00:12:28.623: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 1 00:12:28.659: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:28.659: SB11: V111 Speak: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar 1 00:12:31.539: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:31.539: SB11: V111 Speak: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar 1 00:12:31.575: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 1 00:12:34.491: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
```

What can be determined about the HSRP relationship from the displayed debug output?

- A. The preempt feature is not enabled on the 172.16.11.111 router.
- B. The nonpreempt feature is enabled on the 172.16.11.112 router.
- C. Router 172.16.11.111 will be the active router because its HSRP priority is preferred over router 172.16.11.112.
- D. Router 172.16.11.112 will be the active router because its HSRP priority is preferred over router 172.16.11.111.
- E. The IP address 172.16.11.111 is the virtual HSRP router IP address.
- F. The IP address 172.16.11.112 is the virtual HSRP router IP address.

Answer: A

Explanation:

The standby preempt interface configuration command allows the router to become the active router when its priority is higher than all other HSRP-configured routers in this Hot Standby group. The configurations of both routers include this command so that each router can be the standby router for the other router. The 1 indicates that this command applies to Hot Standby group 1. If you do not use the standby preempt command in the configuration for a router, that router cannot

become the active router.

Reference: Configuring HSRP

(http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.1_19_ea1/configuration/guide/swhsrp.html)

QUESTION NO: 156

Refer to the exhibit.

```
*Mar 1 00:16:43.095: %LINK-3-UPDOWN: Interface Vlan11, changed state to up
*Mar 1 00:16:43.099: SB: V111 Interface up
*Mar 1 00:16:43.099: SB11: V111 Init: a/HSRP enabled
*Mar 1 00:16:43.099: SB11: V111 Init -> Listen
*Mar 1 00:16:43.295: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:16:43.295: SB11: V111 Active router is 172.16.11.112
*Mar 1 00:16:43.295: SB11: V111 Listen: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar 1 00:16:43.295: SB11: V111 Active router is local, was 172.16.11.112
*Mar 1 00:16:43.299: %STANDBY-6-STATECHANGE: Vlan11 Group 11 state Listen -> Active
*Mar 1 00:16:43.299: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:43.303: SB11: V111 Hello in 172.16.11.112 Speak pri 50 ip 172.16.11.115
*Mar 1 00:16:46.207: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:49.095: SB11: V111 Hello in 172.16.11.112 Speak pri 50 ip 172.16.11.115
```

Based on the debug output, which three statements about HSRP are true? (Choose three.)

- A. The final active router is the router with IP address 172.16.11.111.
- B. The router with IP address 172.16.11.111 has preempt configured.
- C. The priority of the router with IP address 172.16.11.112 is preferred over the router with IP address 172.16.11.111.
- D. The IP address 172.16.11.115 is the virtual HSRP IP address.
- E. The router with IP address 172.16.11.112 has nonpreempt configured.
- F. The router with IP address 172.16.11.112 is using default HSRP priority.

Answer: A,B,D

Explanation:

In this debug, we can see that a new active HSRP router has been established. The router priority of the old active router was 50, but the local router's priority is 100. Because a new active router was established, we know that pre-emption must be enabled. The local router is 172.16.11.112, with the HSRP address being 172.16.11.115.

QUESTION NO: 157

Refer to the exhibit.

```
Vlan8 - Group 8
Local state is Active, priority 110, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:01.168
Hot standby IP address is 10.1.2.2 configured
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac08
5 state changes, last state change 00:05:03
```

Which two problems are the most likely cause of the exhibited output? (Choose two.)

- A. spanning tree issues
- B. HSRP misconfiguration
- C. VRRP misconfiguration
- D. physical layer issues
- E. transport layer issues

Answer: B,D

Explanation:

When you see this error, it means the local router fails to receive HSRP hellos from neighbor router. Two things you should check first are the physical layer connectivity and verify the HSRP configuration. An example of HSRP misconfiguration is the mismatched of HSRP standby group and standby IP address.

Another thing you should check is the mismatched VTP modes.

QUESTION NO: 158

Which two statements about HSRP, VRRP, and GLBP are true? (Choose two.)

- A. GLBP allows for router load balancing of traffic from a network segment without the different host IP configurations needed to achieve the same results with HSRP.
- B. GLBP allows for router load balancing of traffic from a network segment by utilizing the creation of multiple standby groups.
- C. GLBP and VRRP allow for MD5 authentication, whereas HSRP does not.
- D. Unlike HSRP and VRRP, GLBP allows automatic selection and simultaneous use of multiple available gateways.

E. HSRP allows for multiple upstream active links being simultaneously used, whereas GLBP does not.

Answer: A,D

Explanation:

1. GLBP

To provide a virtual router, multiple switches (routers) are assigned to a common GLBP group. Rather than having just one active router performing forwarding for the virtual router address, all routers in the group can participate and offer load balancing by forwarding a portion of the overall traffic.

2. VRRP

The Virtual Router Redundancy Protocol (VRRP) is a standards-based alternative to HSRP, defined in IETF standard RFC 2338. VRRP is so similar to HSRP that you need to learn only slightly different terminology and a couple of slight functional differences.

- VRRP provides one redundant gateway address from a group of routers. The active router is called the master router, while all others are in the backup state. The master router is the one with the highest router priority in the VRRP group.
- VRRP group numbers range from 0 to 255; router priorities range from 1 to 254 (254 is the highest; 100 is the default).
- The virtual router MAC address is of the form 0000.5e00.01xx, where xx is a two-digit hex VRRP group number.
- VRRP advertisements are sent at 1-second intervals. Backup routers can optionally learn the advertisement interval from the master router.
- By default, all VRRP routers are configured to preempt the current master router, if their priorities are greater.
- VRRP has no mechanism for tracking interfaces to allow more capable routers to take over the master role.

3. HSRP

HSRP is a Cisco-proprietary protocol developed to allow several routers (or multilayer switches) to appear as a single gateway address. RFC 2281 describes this protocol in more detail. Basically, each of the routers that provides redundancy for a given gateway address is assigned to a common HSRP group. One router is elected as the primary, or active, HSRP router, another is elected as the standby HSRP router, and all the others remain in the listen HSRP state. The routers exchange HSRP hello messages at regular intervals, so they can remain aware of each other's existence, as well as that of the active router.

Reference: First Hop Redundancy protocol comparison (HSRP, VRRP, GLBP

(<http://cciethebeginning.wordpress.com/2008/08/23/router-high-availability-protocol-comparison-2/>)

First Hop Redundancy

(http://packetlife.net/media/library/3/First_Hop_Redundancy.pdf)

QUESTION NO: 159

Which two statements about HSRP are true? (Choose two.)

- A. Load sharing with HSRP is achieved by creating multiple subinterfaces on the HSRP routers.
- B. Load sharing with HSRP is achieved by creating HSRP groups on the HSRP routers.
- C. Routers configured for HSRP must belong only to one group per HSRP interface.
- D. Routers configured for HSRP can belong to multiple groups and multiple VLANs.
- E. All routers configured for HSRP load balancing must be configured with the same priority.

Answer: B,D

Explanation:

HSRP is a Cisco-proprietary protocol developed to allow several routers (or multilayer switches) to appear as a single gateway address. RFC 2281 describes this protocol in more detail. Basically, each of the routers that provides redundancy for a given gateway address is assigned to a common HSRP group. One router is elected as the primary, or active, HSRP router, another is elected as the standby HSRP router, and all the others remain in the listen HSRP state. The routers exchange HSRP hello messages at regular intervals, so they can remain aware of each other's existence, as well as that of the active router.

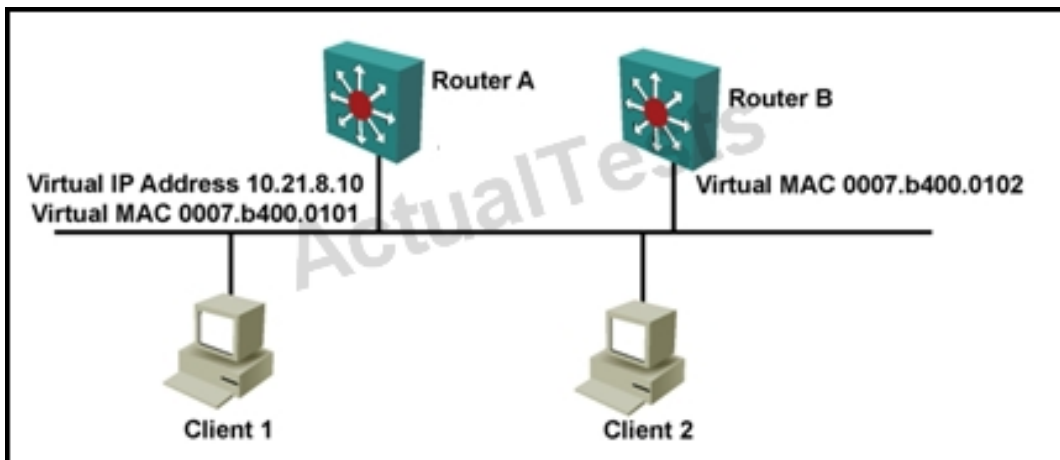
An HSRP group can be assigned an arbitrary group number, from 0 to 255. If you configure HSRP groups on several VLAN interfaces, it can be handy to make the group number the same as the VLAN number. However, most Catalyst switches support only up to 16 unique HSRP group numbers. If you have more than 16 VLANs, you will quickly run out of group numbers. An alternative is to make the group number the same (that is, 1) for every VLAN interface. This is perfectly valid because the HSRP groups are only locally significant on an interface. HSRP Group 1 on interface VLAN 10 is unique from HSRP Group 1 on interface VLAN 11.

Reference: Configuring HSRP

(http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.1_19_ea1/configuration/guide/swhsrp.html)

QUESTION NO: 160

Refer to the exhibit.



Both routers are configured for the GLBP. Which statement is true?

- A. The default gateway addresses of both hosts should be set to the IP addresses of both routers.
- B. The default gateway address of each host should be set to the virtual IP address.
- C. The hosts learn the proper default gateway IP address from router A.
- D. The hosts have different default gateway IP addresses and different MAC addresses for each router.

Answer: B

Explanation:

GLBP performs a similar, but not identical, function for the user as the HSRP and VRRP. Both HSRP and VRRP protocols allow multiple routers to participate in a virtual router group configured with a virtual IP address. One member is elected to be the active router to forward packets sent to the virtual IP address for the group. The other routers in the group are redundant until the active router fails. With standard HSRP and VRRP, these standby routers pass no traffic in normal operation - which is wasteful. Therefore the concept came about for using multiple virtual router groups, which are configured for the same set of routers. But to share the load, the hosts must be configured for different default gateways, which results in an extra administrative burden of going around and configuring every host and creating 2 or more groups of hosts that each use a different default gateway.

GLBP is similar in that it provides load balancing over multiple routers (gateways) - but it can do this using only ONE virtual IP address!!! Underneath that one virtual IP address is multiple virtual MAC addresses, and this is how the load is balanced between the routers. Instead of the hassle of configuring all the hosts with a static Default Gateway, you can let them use ARP's to find their own. Multiple gateways in a "GLBP redundancy group" respond to client Address Resolution Protocol (ARP) requests in a shared and ordered fashion, each with their own unique virtual MAC addresses. As such, workstation traffic is divided across all possible gateways. Each host is

configured with the same virtual IP address, and all routers in the virtual router group participate in forwarding packets

Reference: HSRP, GLBP, and VRRP

<http://www.infocellar.com/networks/Routers/HSRP-GLBP-VRRP.htm>

QUESTION NO: 161

```
hostname Switch1
```

```
interface Vlan10
```

```
ip address 172.16.10.32 255.255.255.0
```

```
no ip redirects
```

```
standby 1 ip 172.16.10.110
```

```
standby 1 timers 1 5
```

```
standby 1 priority 130
```

```
hostname Switch2
```

```
interface Vlan10
```

```
ip address 172.16.10.33 255.255.255.0
```

```
no ip redirects
```

```
standby 1 ip 172.16.10.110
```

```
standby 1 timers 1 5
```

```
standby 1 priority 120
```

Refer to the above. HSRP was implemented and configured on two switches while scheduled network maintenance was performed.

After the two switches have finished rebooting, you notice via show commands that Switch2 is the HSRP active router. Which two items are the most likely cause of Switch1 not becoming the active router? (Choose two.)

- A. Booting has been delayed.
- B. The standby group number does not match the VLAN number.
- C. IP addressing is incorrect.
- D. Preemption is disabled.
- E. Standby timers are incorrect.
- F. IP redirect is disabled.

Answer: A,D

Explanation:

If Switch2 starts before Switch1 it becomes the active HSRP router. When Switch1 start to works it does not preempt the active status from the Switch2 also Switch1 has better HSRP priority. This is expected behavior in the absence of the standby 1 preempt command.

Reference:

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094e8c.shtml

QUESTION NO: 162

Which protocol allows for the automatic selection and simultaneous use of multiple available gateways as well as automatic failover between those gateways?

- A. IRDP
- B. HSRP
- C. GLBP
- D. VRRP

Answer: C

Explanation:

To provide a virtual router, multiple switches (routers) are assigned to a common GLBP group. Rather than having just one active router performing forwarding for the virtual router address, all routers in the group can participate and offer load balancing by forwarding a portion of the overall traffic. The advantage is that none of the clients have to be pointed toward a specific gateway address—they can all have the same default gateway set to the virtual router IP address. The load balancing is provided completely through the use of virtual router MAC addresses in ARP replies returned to the clients. As a client sends an ARP request looking for the virtual router address, GLBP sends back an ARP reply with the virtual MAC address of a selected router in the group. The result is that all clients use the same gateway address but have differing MAC addresses for it.

Reference: Configuring GLBP

QUESTION NO: 163 DRAG DROP

Match the HSRP states on the left with the correct definition on the right.

Select from these**Learn****Listen****Speak****Standby****Active****Initial****Place here**

State from which the routers begin the HSRP process

A candidate to become the next active router

The router is still waiting to hear from the active router

The router is currently forwarding packets

Listens for hello messages from the active and standby router

Participates in the election for the active or standby router

Answer:

Select from these

Learn

Listen

Speak

Standby

Active

Initial

Place here

Initial

State from which the routers begin the HSRP process

Standby

A candidate to become the next active router

Learn

The router is still waiting to hear from the active router

Active

The router is currently forwarding packets

Listen

Listens for hello messages from the active and standby router

Speak

Participates in the election for the active or standby router

Explanation:

Select from these

Place here

Initial

State from which the routers begin the HSRP process

Standby

A candidate to become the next active router

Learn

The router is still waiting to hear from the active router

Active

The router is currently forwarding packets

Listen

Listens for hello messages from the active and standby router

Speak

Participates in the election for the active or standby router

HSRP defines six states in which an HSRP-enabled router can exist:

Reference: Cisco Hot Standby Router Protocol (HSRP)

(<http://tools.ietf.org/html/rfc2281#page-8>)

QUESTION NO: 164 DRAG DROP

Categorize the high availability network resources or feature items on the left by dragging them to the appropriate resiliency or management level on the right.

Resources/Feature Items	Management Level	Network Level	System Level
dual power supplies			
RSTP			
IP SLA responder			
NSF			
NTP			
SSO			

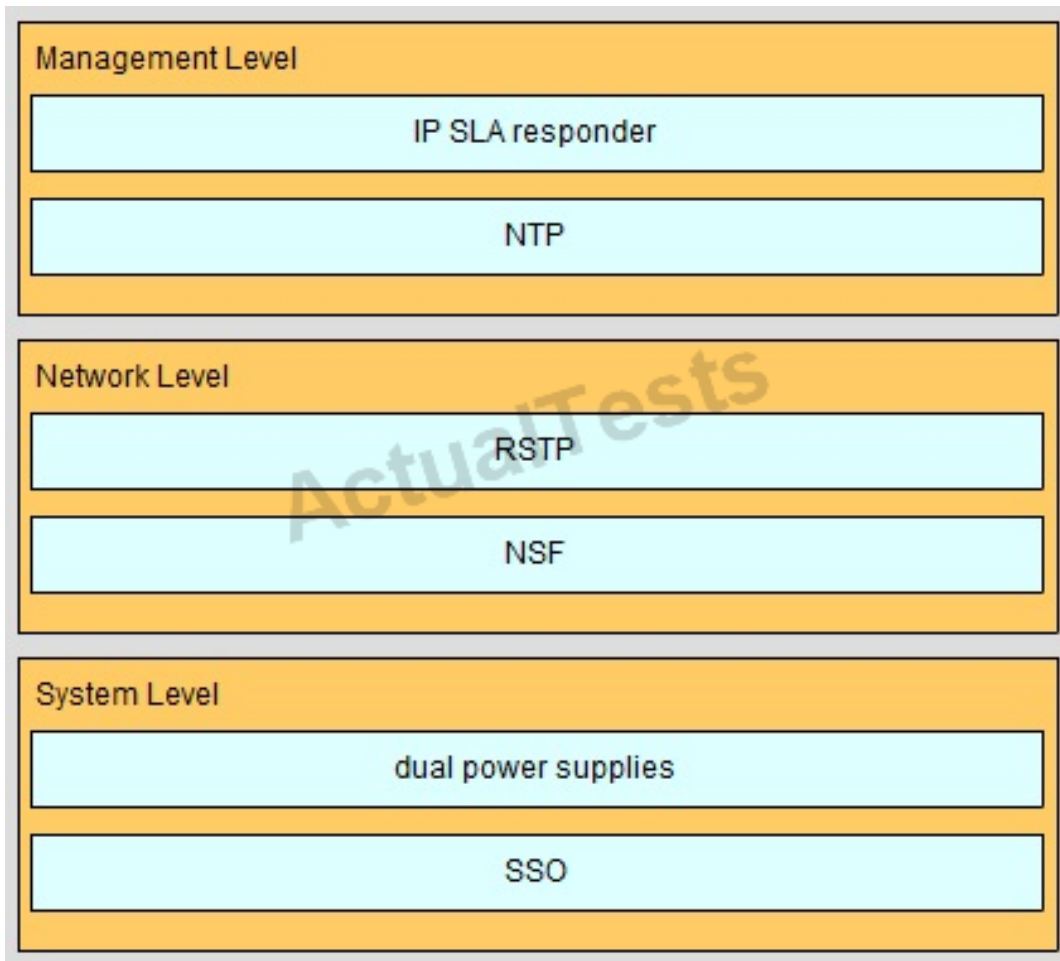
Answer:

Categorize the high availability network resources or feature items on the left by dragging them to the appropriate resiliency or management level on the right.

Resources/Feature Items	Management Level	Network Level	System Level
dual power supplies			
RSTP			
IP SLA responder			
NSF			
NTP			
SSO			

Management Level	Network Level	System Level
IP SLA responder		
NTP		
	RSTP	
	NSF	
		dual power supplies
		SSO

Explanation:



Cisco Nonstop Forwarding (NSF) with Stateful Switchover (SSO) is a Cisco innovation for routers with dual route processors. Cisco NSF with SSO allows a router, which has experienced a hardware or software failure of an active route processor, to maintain data link layer connections and continue forwarding packets during the switchover to the Standby route processor. This forwarding can continue despite the loss of routing protocol peering arrangements with other routers. Routing information is recovered dynamically, in the background, while packet forwarding proceeds uninterrupted.

Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol (802.1D standard) and provides for faster spanning tree convergence after a topology change. The standard also includes features equivalent to Cisco PortFast, UplinkFast and BackboneFast for faster network reconvergence.

Cisco IOS IP Service Level Agreements (SLAs) enables customers to assure new business-critical IP applications, as well as IP services that utilize data, voice, and video, in an IP network. Cisco has augmented traditional service level monitoring and advanced the IP infrastructure to become IP application-aware by measuring both end-to-end and at the IP layer. With Cisco IOS IP SLAs, users can verify service guarantees, increase network reliability by validating network

performance, proactively identify network issues, and increase Return on Investment (ROI) by easing the deployment of new IP services. Cisco IOS IP SLAs uses active monitoring to generate traffic in a continuous, reliable, and predictable manner, thus enabling the measurement of network performance and health.

NTP is designed to synchronize the time on a network of machines. NTP runs over the User Datagram Protocol (UDP), using port 123 as both the source and destination, which in turn runs over IP. NTP Version 3 RFC 1305 is used to synchronize timekeeping among a set of distributed time servers and clients. A set of nodes on a network are identified and configured with NTP and the nodes form a synchronization subnet, sometimes referred to as an overlay network. While multiple masters (primary servers) may exist, there is no requirement for an election protocol.

Reference:

http://www.cisco.com/en/US/technologies/tk648/tk365/technologies_white_paper0900aecd8023df74_ps6599_Products_White_Paper.html

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a00807b0670.shtml

http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsthresh.html

http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

QUESTION NO: 165 HOTSPOT

Instructions

This item contains several questions that you must answer. You can view these questions by clicking on the corresponding button to the left. Changing questions can be accomplished by clicking the numbers to the left of each question. In order to complete the questions, you will need to refer to the topology.

To gain access to the topology, click on the topology button at the bottom of the screen. When you have finished viewing the topology, you can return to your questions by clicking on the Questions button to the left.

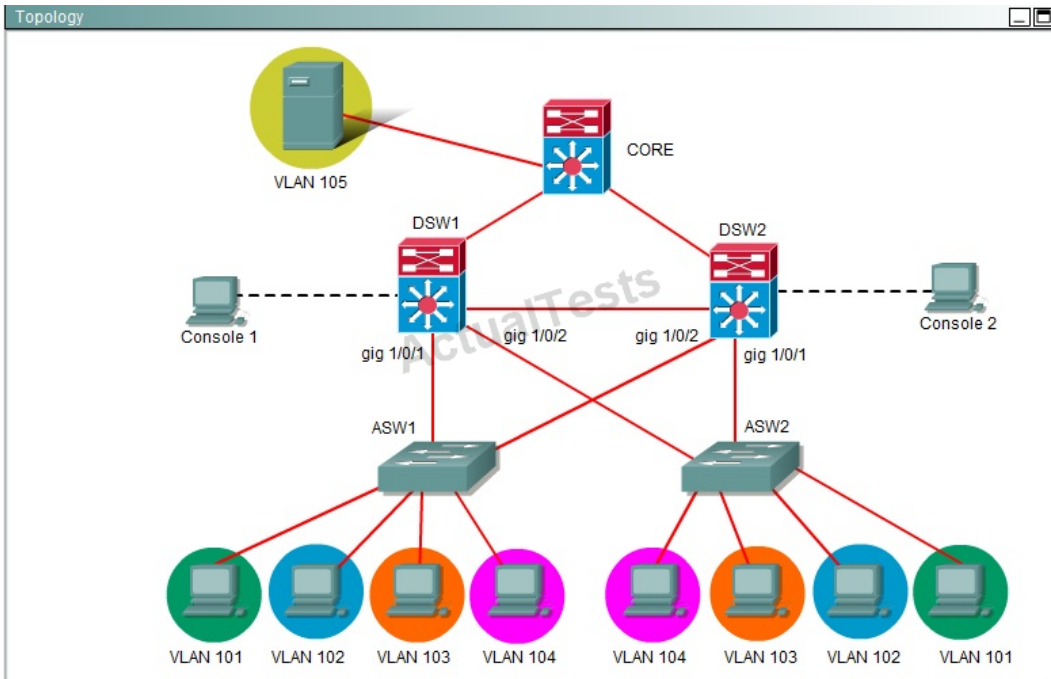
Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

Scenario

Ferris Plastics, Inc. is a medium sized company, with an enterprise network (access, distribution and core switches) that provides LAN connectivity from user PCs to corporate servers. The distribution switches are configured to use HSRP to provide a high availability solution.

- DSW1 - primary device for VLAN 101 VLAN 102 and VLAN 105
- DSW2 - primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthernet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

Troubleshooting has identified several issues. Currently all interfaces are up. Using the running configurations and **show** commands, you have been asked to investigate and respond to the following questions.



Question #5

What is the priority value of the VLAN 105 HSRP group on DSW2?

- ☐ 50
- ☐ 100
- ☐ 150
- ☐ 200

Answer:

Question #5

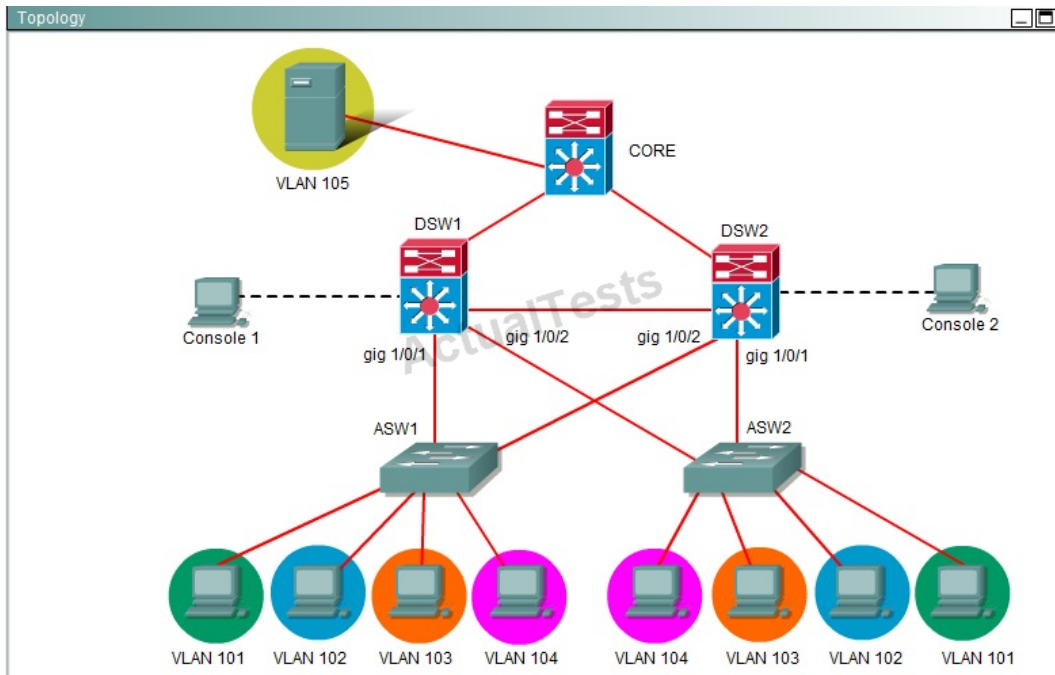
What is the priority value of the VLAN 105 HSRP group on DSW2?

- ☐ 50
- ☒ 100
- ☐ 150
- ☐ 200

Explanation:

100

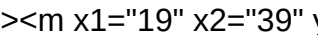
The priority value for VLAN 105 is not explicitly configured on DSW2, so it will take the default value of 100. Use the “show standby” command to verify this on DSW2.



Question #3

All interfaces are active. DSW2 has not become the active device for the VLAN 103 HSRP group. As related to the VLAN 103 HSRP group, what can be done to make the group function properly?

- ☐ On DSW1, disable preempt.
- ☐ On DSW1, decrease the priority value to a value less than 190 and greater than 150.
- ☐ On DSW2, increase the priority value to a value greater 200 and less than 250.
- ☐ On DSW2, increase the decrement value in the track command to a value greater than 10 and less than 50.

Answer: 

On DSW1, decrease the priority value to a value less than 190 and greater than 150.

The priority value on DSW1 is set to 200 while it is set to 190 on DSW2. Lowering the value on DSW1 will enable DSW2 to become the primary router for VLAN 103 while enabling the DSW1 to become active if Gig 1/0/1 is down on DSW2.

QUESTION NO: 166 HOTSPOT

Instructions

This item contains several questions that you must answer. You can view these questions by clicking on the corresponding button to the left. Changing questions can be accomplished by clicking the numbers to the left of each question. In order to complete the questions, you will need to refer to the topology.

To gain access to the topology, click on the topology button at the bottom of the screen. When you have finished viewing the topology, you can return to your questions by clicking on the Questions button to the left.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

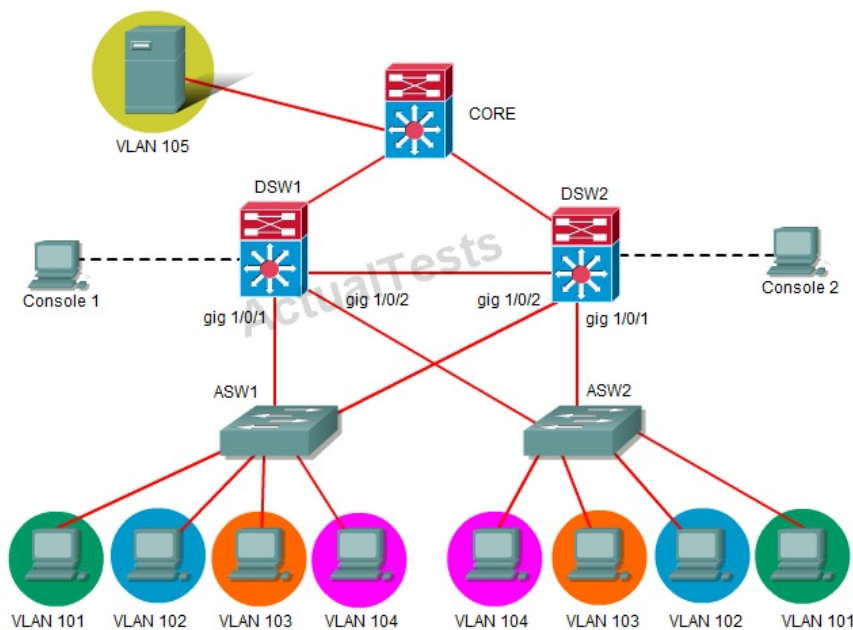
Scenario

Ferris Plastics, Inc. is a medium sized company, with an enterprise network (access, distribution and core switches) that provides LAN connectivity from user PCs to corporate servers. The distribution switches are configured to use HSRP to provide a high availability solution.

- DSW1 - primary device for VLAN 101 VLAN 102 and VLAN 105
- DSW2 - primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthernet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

Troubleshooting has identified several issues. Currently all interfaces are up. Using the running configurations and **show** commands, you have been asked to investigate and respond to the following questions.

Topology



Question #4

During routine maintenance, it became necessary to shut down the GigabitEthernet1/0/1 interface on DSW1 and DSW2. All other interfaces were up. During this time, DSW1 became the active router for the VLAN 104 HSRP group. As related to the VLAN 104 HSRP group, what can to be done to make the group function properly?

- ☐ On DSW1, disable preempt.
- ☐ On DSW2 decrease the priority value to a value less than 150.
- ☐ On DSW1, increase the decrement value in the track command to a value greater than 6.
- ☐ On DSW1, decrease the decrement value in the track command to a value less than 1.

Answer:

Question #4

During routine maintenance, it became necessary to shut down the GigabitEthernet1/0/1 interface on DSW1 and DSW2. All other interfaces were up. During this time, DSW1 became the active router for the VLAN 104 HSRP group. As related to the VLAN 104 HSRP group, what can to be done to make the group function properly?

- ☐ On DSW1, disable preempt.
- ☐ On DSW2 decrease the priority value to a value less than 150.
- ☒ On DSW1, increase the decrement value in the track command to a value greater than 6.
- ☐ On DSW1, decrease the decrement value in the track command to a value less than 1.

Explanation:

On DSW1, increase the decrement value in the track command to a value greater than 6.

For VLAN 104, the priority is 200 on DSW2 and 150 on DSW1. The decrement value is set to 1 on DSW1 and 55 on VLAN 104. We need to increase the decrement value on DSW1.

QUESTION NO: 167

What are three possible router states of HSRP routers on a LAN? (Choose three.)

- A. standby
- B. established
- C. active
- D. idle
- E. backup
- F. initial

Answer: A,C,F

Explanation:

Internally, each router in the standby group implements a state machine. The State field describes the current state of the router sending the message. Possible values are:

- 0 - Initial
- 1 - Learn
- 2 - Listen
- 4 - Speak
- 8 - Standby
- 16 - Active

Reference: <http://www.ietf.org/rfc/rfc2281.txt>

QUESTION NO: 168

Which statement describes Virtual Router Redundancy Protocol (VRRP)?

- A. A VRRP group has one master and at least one standby virtual router.
- B. A VRRP group has one master and one or more backup virtual routers.
- C. A VRRP group has one active and one or more standby virtual routers.
- D. A VRRP group has one active and one backup virtual router.

Answer: B

Explanation:

A VRRP group has one master and one or more backup virtual routers and is the open standard implementation of HSRP.

Reference: CCNA Routing and Switching Guide, Todd Lammle, page 715.

QUESTION NO: 169

What three tasks will a network administrator perform to successfully configure Hot Standby Routing Protocol (HSRP)? (Choose three.)

- A. Define the encapsulation type
- B. Define the standby router
- C. Define the standby IP address
- D. Enable the standby mode
- E. Enable HSRP

Answer: B,C,E

Explanation:

The basic steps to configure HSRP are as follows:

QUESTION NO: 170

Which three protocols have been developed for IP routing redundancy to protect against first-hop router failure? (Choose three.)

- A. HSRP
- B. MSTP
- C. ICMP
- D. VRRP
- E. GLBP

Answer: A,D,E

Explanation:

A First Hop Redundancy Protocol (FHRP) is a computer networking protocol which is designed to protect the default gateway used on a subnetwork by allowing two or more routers to provide backup for that address; in the event of failure of the/an active router, the backup router will take over the address, usually within a few seconds. In practice, such protocols can also be used to protect other services operating on a single IP address, not just routers.

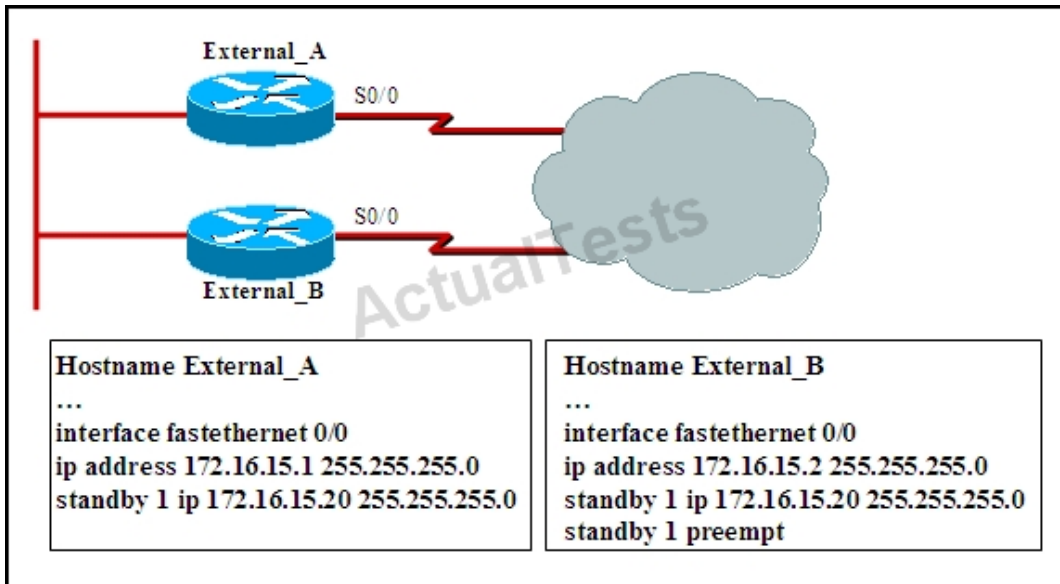
Examples of such protocols include (in approximate order of creation):

Hot Standby Router Protocol (HSRP) - Cisco's initial, proprietary standard

Virtual Router Redundancy Protocol (VRRP) - an open standard protocol

Gateway Load Balancing Protocol (GLBP) - a more recent proprietary standard from Cisco that permits load balancing as well as redundancy

QUESTION NO: 171



Which command will ensure that External_B will be the primary router for traffic using the gateway address of 172.16.15.20?

- A. On External_B add the command standby 1 priority 80.
- B. On External_A add the command standby 1 priority 110.
- C. On External_A add the command standby 1 priority 80.
- D. On External_B remove the command standby 1 preempt

Answer: C

Explanation:

The default HSRP router priority is 100, and the router with the highest priority will become active. Lowering the priority of External_A to 80 would ensure that External_B would become the active router with its default value of 100.

QUESTION NO: 172

Which describes the default load balancing scheme used by the Gateway Load Balancing Protocol (GLBP)?

- A. per host basis using a round-robin scheme
- B. per host basis using a strict priority scheme
- C. per session using a round-robin scheme
- D. per session using a strict priority scheme
- E. per GLBP group using a round-robin scheme
- F. per GLBP group using a strict priority scheme

Answer: A

Explanation:

GLBP allows a group of routers to join a virtual GLBP group and load balance traffic by distributing the forwarding between all routers in the group. The load balancing is performed using ARP replies generated from the virtual gateway address. When a host sends an ARP request for the default gateway, GLBP will respond with the virtual MAC address of one of the routers in the GLBP group.

Each client in the network will use the same gateway IP address, but use different MAC addresses for that gateway. Per host – round robin is the default GLBP load-balancing scheme.

QUESTION NO: 173

Which First Hop Redundancy protocol cannot be configured for interface tracking?

- A. HSRP
- B. GLBP
- C. VRRP
- D. SLB
- E. RPR
- F. RPR+

Answer: C

Explanation:

Although VRRP cannot track interfaces as the RFC does not specify any mechanism to do so, object tracking can be used instead. VRRP is the best answer.

QUESTION NO: 174

Which high availability service is verified by the show standby command?

- A. VRRP
- B. GLBP
- C. HSRP
- D. MSTP
- E. PVRST

Answer: C

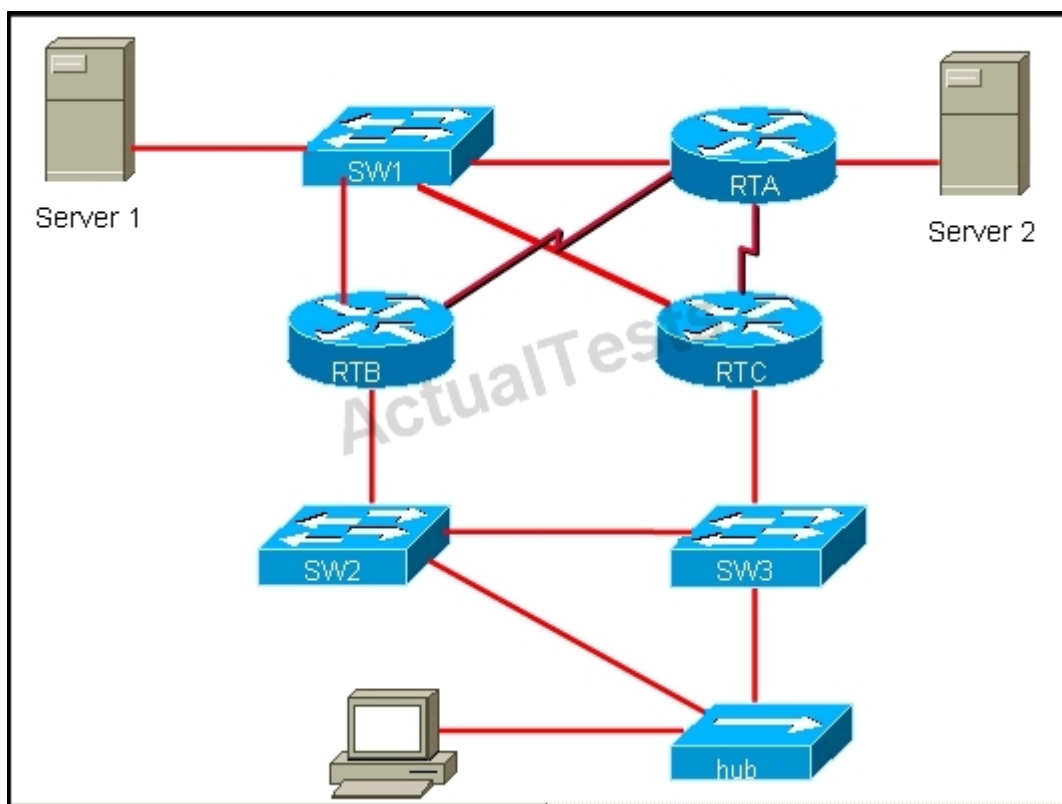
Explanation:

show standby

To display Hot Standby Router Protocol (HSRP) information, use the show standby command in user EXEC or privileged EXEC mode.

show standby [type number [group]] [all | brief]

Reference: http://www.cisco.com/en/US/docs/ios/ipapp/command/reference/iap_s4.html

QUESTION NO: 175

Observe the topology in the exhibit. HSRP is configured between RTB and RTC with RTC as the active router. SW2 is configured as the root bridge for the Spanning Tree Protocol. What will happen if the serial connection on RTC is down?

- A. STP will not need to be recalculated because RTB will take over as active router.
- B. RTB and RTC will flap between active and standby because the timers for STP are greater than the timers for HSRP.
- C. All traffic will automatically forward to RTB.
- D. SW3 will take over as the new root bridge.

Answer: B

Explanation:

When you run the Hot Standby Router Protocol (HSRP) between two routers connected via a LAN switch, you may observe instability in HSRP. This often happens during a network disruption or an active router transition; such as an HSRP router with a higher priority and preemption configured being added to the LAN. In the reference link this problem is described and one of the solutions is to change the HSRP timers so that the spanning tree forward delay (default of 15 seconds) is less than half the HSRP holdtime (default of 10 seconds).

Reference: "Avoiding HSRP Instability in a Switching Environment with Various Router Platforms"

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_configuration_example09186a0080093f93.shtml

QUESTION NO: 176

What is the maximum number of HSRP standby groups that can be configured on a Cisco router?

- A. 16
- B. 32
- C. 64
- D. 128
- E. 256

Answer: E

Explanation:

The limit of 256 is an HSRP protocol limit with respect to the range that the HSRP group can be set to. If you look at RFC 2281 Cisco HSRP, you'll see this specified in section 5.1:

Group: 1 octet

This field identifies the standby group. For Token Ring, values between 0 and 2 inclusive are valid. For other media values between 0 and 255 inclusive are valid.

QUESTION NO: 177

```
R1# show running-config interface GigabitEthernet 0/0
```

```
Current configuration: 205 bytes
!
Interface GigabitEthernet0/0
 ip address 10.1.7.5 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 negotiation auto
 glbp 7 ip 10.1.7.1
 glbp 7 timers msec 250 msec 750
 glbp 7 priority 150
```

```
R2# show running-config interface GigabitEthernet 0/0
```

```
Current configuration: 174 bytes
!
Interface GigabitEthernet0/0
 ip address 10.1.7.6 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 negotiation auto
 glbp 7 timers msec 250 msec 750
```

Refer to the exhibit. What statement is true based upon the configuration of router R1 and router R2?

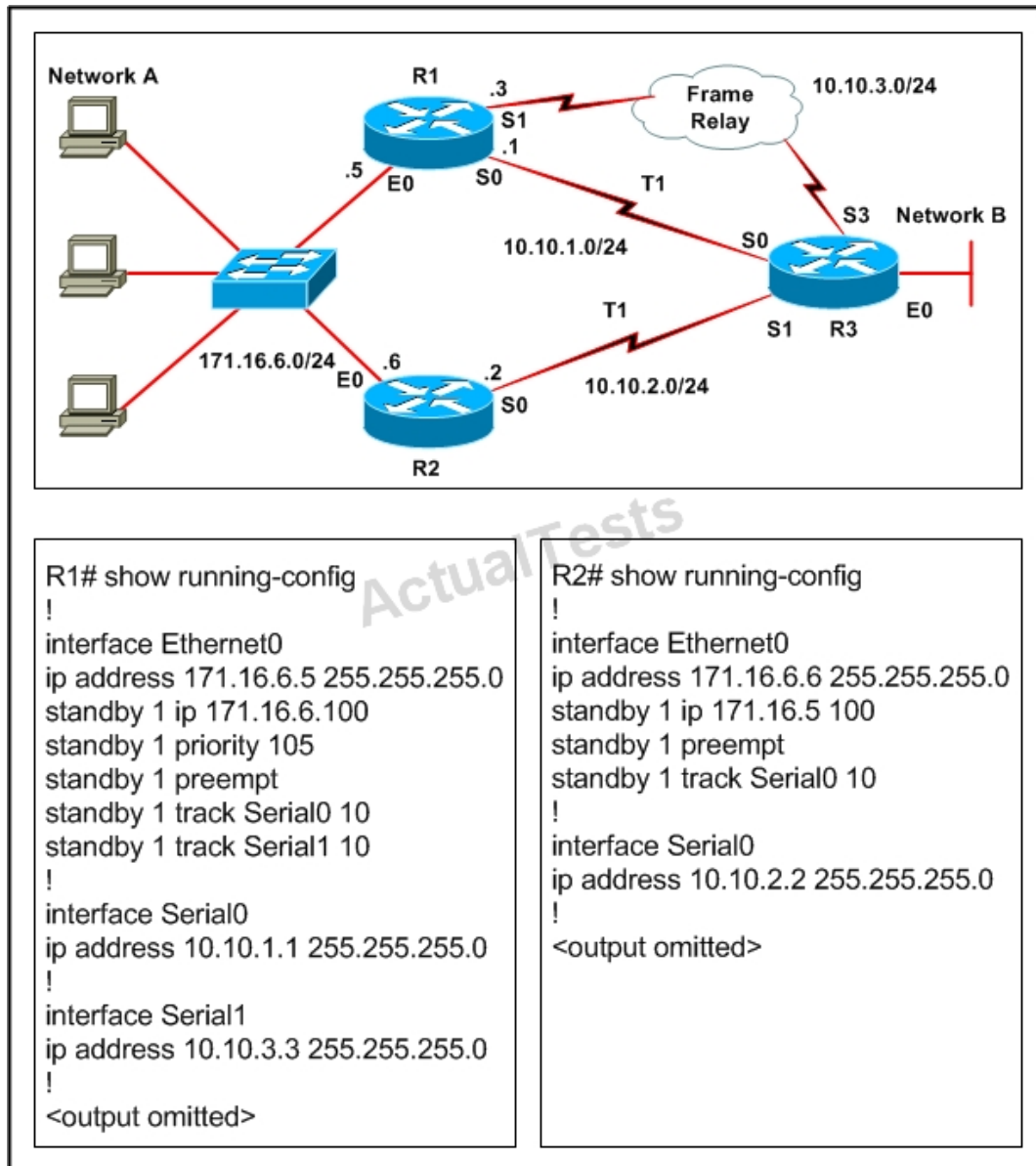
- A. Router R1 will become the active virtual gateway.
- B. Router R2 will become the active virtual gateway.
- C. The hello and hold timers are incompatible with multi-homed BGP.
- D. The hello and hold timers are incompatible with OSPF type 5 LSAs.
- E. Router R1 will become the master for Virtual Router 1, and router R2 will become the backup for Virtual Router 2.
- F. Router R2 will become the master for Virtual Router 1, and router R1 will become the backup for Virtual Router 2.

Answer: A

Explanation:

R2 is not configured with the "priority" command so it will use the default priority value of 100, which is smaller than that of R1 so R1 will be the active virtual gateway.

QUESTION NO: 178



Refer to the exhibit. Routers R1 and R2 are configured in an HSRP group to provide redundancy for the users on Network A. The T1 link between R1 and Network B has failed. How will HSRP respond to the failure?

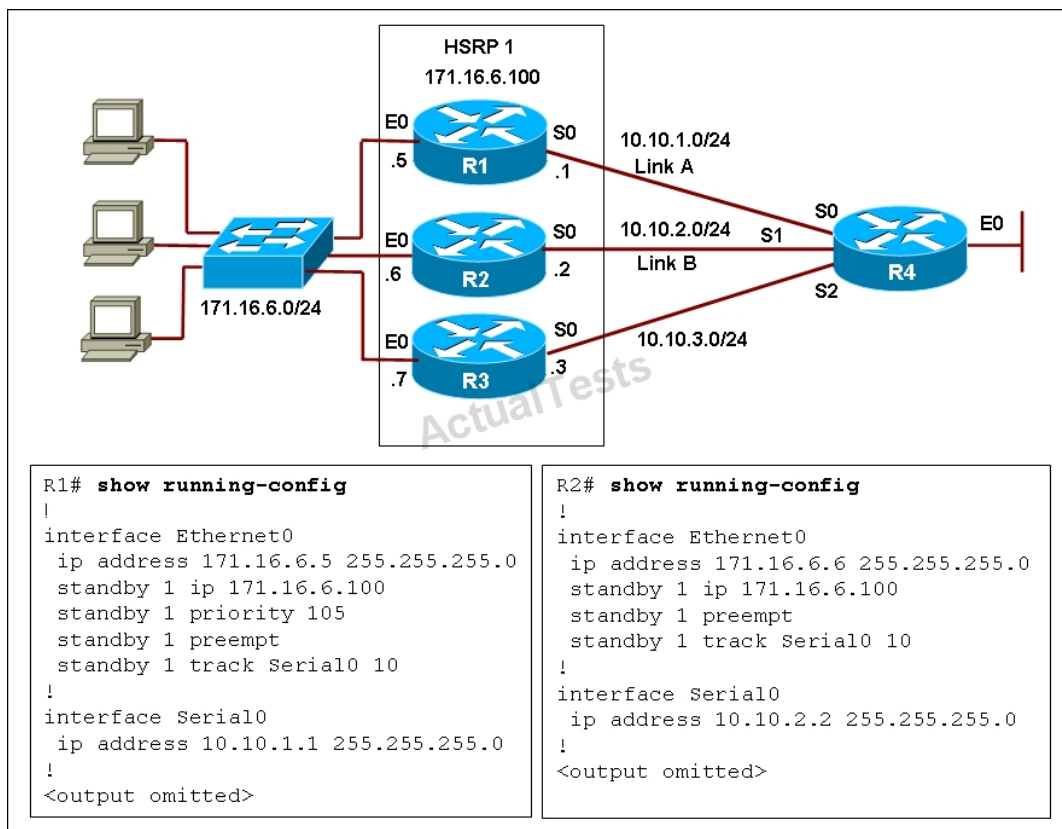
- A.** R1 will change its priority but will remain active using the Frame Relay backup link to forward the traffic to Network B.
- B.** R2 will assume the role of active router and will use its T1 link to forward the traffic to Network B.
- C.** Both routers R1 and R2 will be active, and the traffic will be load balanced between the T1 links.
- D.** Both routers R1 and R2 will be inactive, and the users on Network A will lose the connectivity to Network B.

Answer: B

Explanation:

R1 is configured to decrement the HSRP priority by 10 when S0 goes down, so it will then have a priority of 95 (105-10). R2 is using the default priority of 100 so it will then become the active router.

QUESTION NO: 179



Refer to the exhibit. HSRP has been configured and Link A is the primary route to router R4. When Link A fails, router R2 (Link B) becomes the active router. Which router will assume the active role when Link A becomes operational again?

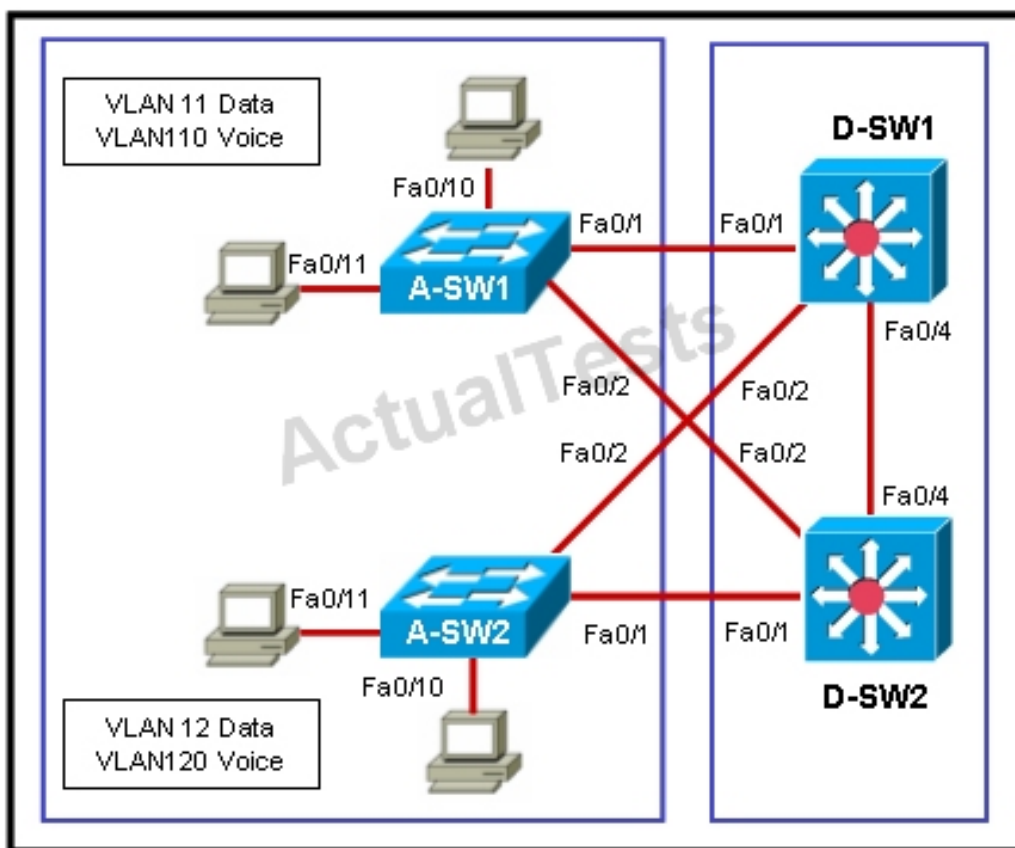
- A. The primary router R1 will reassume the active role when it comes back online.
- B. The standby router R2 will remain active and will forward the active role to router R1 only in the event of its own failure.
- C. The standby router R2 will remain active and will forward the active role to router R1 only in the event of Link B failure.
- D. The third member of the HSRP group, router R3, will take over the active role only in event of router R2 failure.

Answer: A

Explanation:

When Link A goes down, the HSRP priority value of R1 goes down to 95 (105-10) so R2 will be the active router as it is using the default priority of 100. When Link A comes back up, R1's priority is then 105 again and since pre-emption is enabled, it will take back over the active role again.

QUESTION NO: 180



Refer to the exhibit. Which two sets of procedures are best practices for Layer 2 and 3 failover alignment? (Choose two.)

- A.** Configure the D-SW1 switch as the active HSRP router and the STP root for all VLANs. Configure the D-SW2 switch as the standby HSRP router and backup STP root for all VLANs.
- B.** Configure the D-SW2 switch as the active HSRP router and the STP root for all VLANs. Configure the D-SW1 switch as the standby HSRP router and backup STP root for all VLANs.
- C.** Configure the D-SW1 switch as the active HSRP router and the STP root for VLANs 11 and 110. Configure the D-SW2 switch as the active HSRP router and the STP root for VLANs 12 and 120.

- D.** Configure the D-SW1 switch as the standby HSRP router and the backup STP root for VLANs 12 and 120. Configure the D-SW2 switch as the standby HSRP router and the backup STP root for VLANs 11 and 110.
- E.** Configure the D-SW1 switch as the standby HSRP router and the STP root for VLANs 11 and 110. Configure the D-SW2 switch as the standby HSRP router and the STP root for VLANs 12 and 120.
- F.** Configure the D-SW1 switch as the active HSRP router and the backup STP root for VLANs 11 and 110. Configure the D-SW2 switch as the active HSRP router and the backup STP root for VLANs 12 and 120.

Answer: C,D

Explanation:

The “best practices for Layer 2 and 3 failover alignment” here means using load sharing of HSRP where different VLANs use different active routers to load balance the traffic.

To load sharing with HSRP, we can divide traffic into two HSRP groups, where one group assigns the active state for one switch and the other group assigns the active state for the other switch

QUESTION NO: 181

Which two statements about HSRP priority are true? (Choose two.)

- A.** Assuming that preempting has also been configured, the router with the lowest priority in an HSRP group becomes the active router.
- B.** The default priority of a router is zero (0).
- C.** The no standby priority command assigns a priority of 100 to the router.
- D.** To assign the HSRP router priority in a standby group, the standby group-number priority priority-value global configuration command must be used.
- E.** When two routers in an HSRP standby group are configured with identical priorities, the router with the highest configured IP address becomes the active router.

Answer: C,E

Explanation:

From Cisco.com “Hot Standby Router Protocol (HSRP): Frequently Asked Questions”

Q. If there is no priority configured for a standby group, what determines which router is active?

A. The priority field is used to elect the active router and the standby router for the specific group. In the case of an equal priority, the router with the highest IP address for the respective group is elected as active. Furthermore, if there are more than two routers in the group, the second highest IP address determines the standby router and the other router/routers are in the listen state.

Note: If no priority is configured, it uses the default of 100.

Reference:

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_q_and_a_item09186a00800a9679.shtml

QUESTION NO: 182

Which two items are most important for managing the long-term success of high availability?
(Choose two.)

- A. completing aggressive implementation schedule
- B. Stateful Switchover
- C. company and user expectations
- D. Nonstop Forwarding
- E. change control processes
- F. dual devices and dual links

Answer: C,E

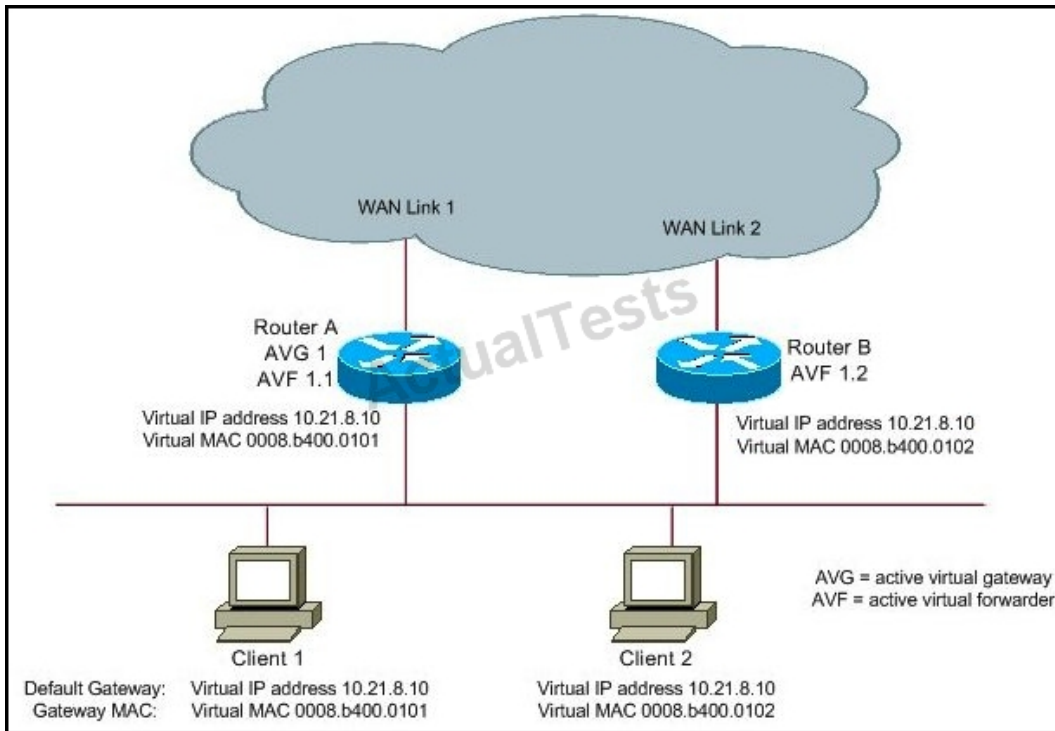
Explanation:

As customer expectations and demands rise, network operations teams are focusing on IT service-quality improvement and achieving higher levels of availability by re-examining processes and procedures-particularly in the area of change management-because changes to the network are often a source of downtime.

Reference: http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11-458050.html

QUESTION NO: 183

Refer to the exhibit.



Which four statements about this GLBP topology are true? (Choose four.)

- A. Router A is responsible for answering ARP requests sent to the virtual IP address.
- B. If router A becomes unavailable, router B forwards packets sent to the virtual MAC address of router A.
- C. If another router is added to this GLBP group, there would be two backup AVGs.
- D. Router B is in GLBP listen state.
- E. Router A alternately responds to ARP requests with different virtual MAC addresses.
- F. Router B transitions from blocking state to forwarding state when it becomes the AVG.

Answer: A,B,C,E

Explanation:

With GLBP the following is true:

With GLB, there is 1 AVG and 1 standby VG. In this case Company1 is the AVG and Company2 is the standby. Company2 would act as a VRF and would already be forwarding and routing packets. Any additional routers would be in a listen state.

As the role of the Active VG and load balancing, Company1 responds to ARP requests with different virtual MAC addresses.

In this scenario, Company2 is the Standby VF for the VMAC 0008.b400.0101 and would become the Active VF if Company1 were down.

As the role of the Active VG, the primary responsibility is to answer ARP requests to the virtual IP address.

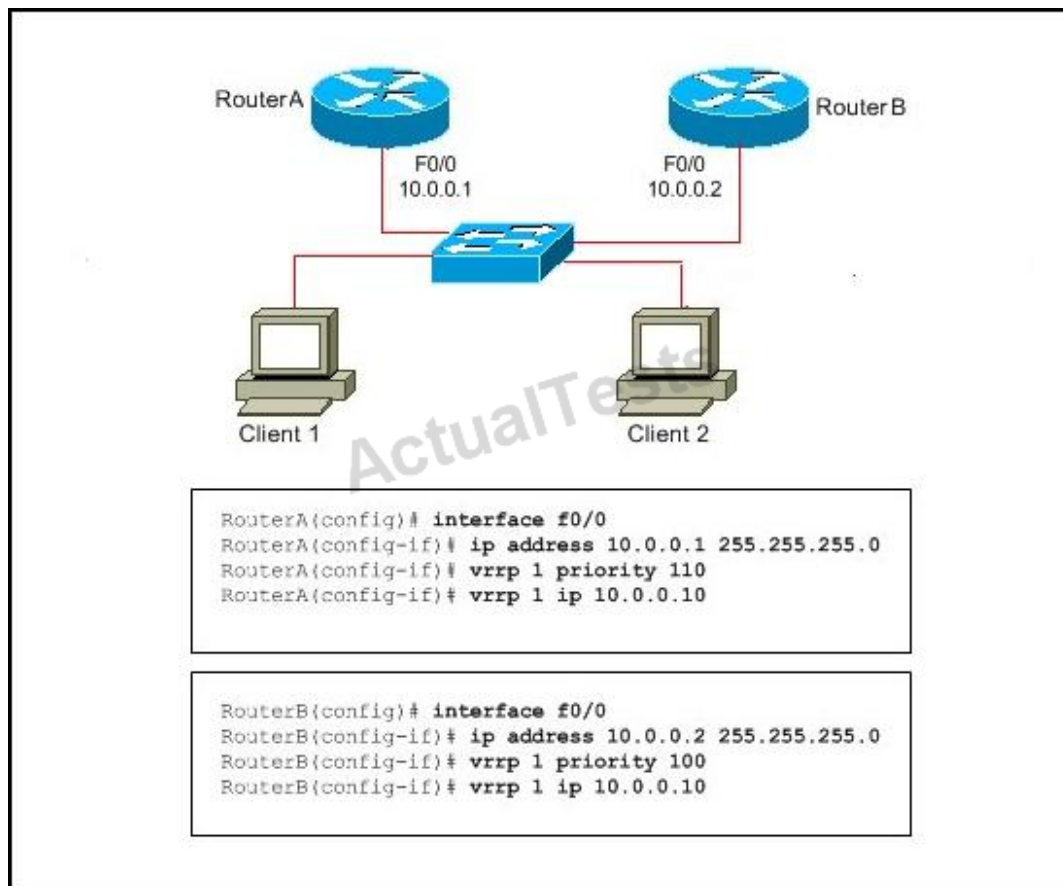
As an AVF router Company2 is already forwarding/routing packets

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a00807d2520.shtml

QUESTION NO: 184

Refer to the exhibit.



Which VRRP statement about the roles of the master virtual router and the backup virtual router is true?

- A.** Router A is the master virtual router, and router B is the backup virtual router. When router A fails, router B becomes the master virtual router. When router A recovers, router B maintains the role of master virtual router.
- B.** Router A is the master virtual router, and Router B is the backup virtual router. When Router A fails, Router B will become the master virtual router. When Router A recovers, it will regain the master virtual router role.
- C.** Router B is the master virtual router, and router A is the backup virtual router. When router B fails, router A becomes the master virtual router. When router B recovers, router A maintains the role of master virtual router.
- D.** Router B is the master virtual router, and router A is the backup virtual router. When router B fails, router A becomes the master virtual router. When router B recovers, it becomes the master virtual router role.

Answer: B

Explanation: An important aspect of the VRRP redundancy scheme is VRRP router priority. Priority determines the role that each VRRP router plays and what happens if the master virtual router fails.

If a VRRP router owns the IP address of the virtual router and the IP address of the physical interface, this router functions as a master virtual router.

Priority also determines if a VRRP router functions as a backup virtual router and determines the order of ascendancy to becoming a master virtual router if the master virtual router fails. You can configure the priority of each backup virtual router with a value of 1 through 254, using the `vrrp priority` command.

For example, if Router A, the master virtual router in a LAN topology, fails, an election process takes place to determine if backup virtual Routers B or C should take over. If Routers B and C are configured with the priorities of 101 and 100, respectively, Router B is elected to become master virtual router because it has the higher priority. If Routers B and C are both configured with the priority of 100, the backup virtual router with the higher IP address is elected to become the master virtual router.

By default, a preemptive scheme is enabled whereby a higher-priority backup virtual router that becomes available takes over for the backup virtual router that was elected to become master virtual router. You can disable this preemptive scheme using the `no vrrp preempt` command. If preemption is disabled, the backup virtual router that is elected to become master virtual router remains the master until the original master virtual router recovers and becomes master again.

ce: Implementing VRRP on Cisco IOS XR Software

http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.5/addr_serv/configuration/guide/ic35vrrp.htm
|

QUESTION NO: 185

In the MAC address 0000.0c07.ac03, what does the "03" represent?

- A. HSRP router number 3
- B. Type of encapsulation
- C. HSRP group number
- D. VRRP group number
- E. GLBP group number

Answer: C

Explanation:

Each router keeps a unique MAC address for its interface. This MAC address is always associated with the unique IP address configured on the interface. For the virtual router address, HSRP defines a special MAC address of the form 0000.0c07.acxx, where xx represents the HSRP group

number as a two-digit hex value. For example, HSRP Group 1 appears as 0000.0c07.ac01, HSRP Group 16 appears as 0000.0c07.ac10.

Reference: Cisco Hot Standby Router Protocol (HSRP)

(<http://tools.ietf.org/html/rfc2281#page-13>)

QUESTION NO: 186 HOTSPOT

Instructions

This item contains several questions that you must answer. You can view these questions by clicking on the corresponding button to the left. Changing questions can be accomplished by clicking the numbers to the left of each question. In order to complete the questions, you will need to refer to the topology.

To gain access to the topology, click on the topology button at the bottom of the screen. When you have finished viewing the topology, you can return to your questions by clicking on the Questions button to the left.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

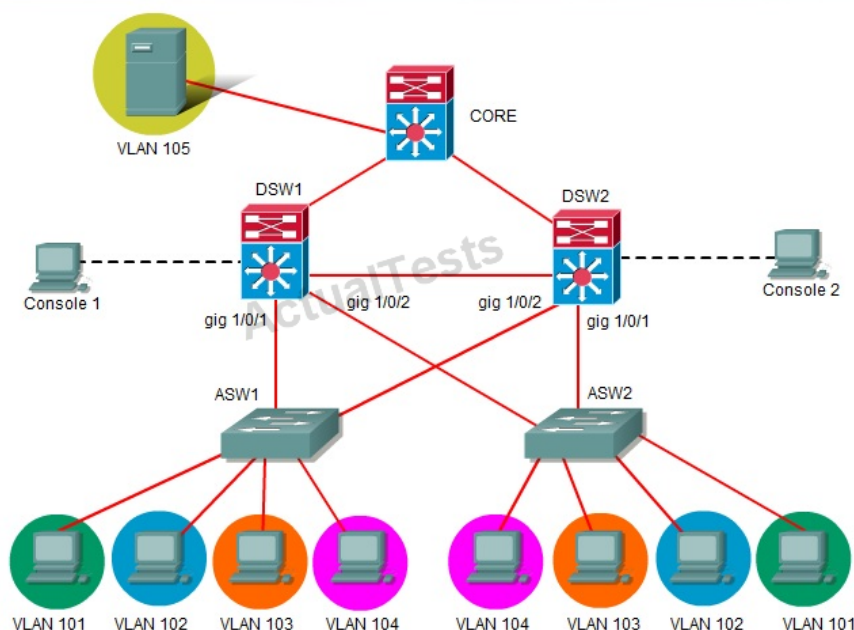
Scenario

Ferris Plastics, Inc. is a medium sized company, with an enterprise network (access, distribution and core switches) that provides LAN connectivity from user PCs to corporate servers. The distribution switches are configured to use HSRP to provide a high availability solution.

- DSW1 - primary device for VLAN 101 VLAN 102 and VLAN 105
- DSW2 - primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthernet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

Troubleshooting has identified several issues. Currently all interfaces are up. Using the running configurations and **show** commands, you have been asked to investigate and respond to the following questions.

Topology



Question #1



During routine maintenance, GigabitEthernet1/0/1 on DSW1 was shut down. All other interfaces were up. DSW2 became the active HSRP device for VLAN 101 as desired. However, after GigabitEthernet1/0/1 on DSW1 was reactivated, DSW1 did not become the active router for VLAN 101 as desired. What needs to be done to make the group for VLAN 101 function properly?

- ☐ Enable preempt in the VLAN 101 HSRP group on DSW1.
- ☐ Disable preempt in the VLAN 101 HSRP group on DSW2's.
- ☐ In the VLAN 101 HSRP group on DSW1, decrease the priority value to a value that is less than the priority value configured in the VLAN 101 HSRP group on DSW2.
- ☐ Decrease the decrement value in the track command for the VLAN 101 HSRP group on DSW1's to a values less than the value in the track command for the VLAN 101 HSRP group on DSW2.

Answer:

Question #1



During routine maintenance, GigabitEthernet1/0/1 on DSW1 was shut down. All other interfaces were up. DSW2 became the active HSRP device for VLAN 101 as desired. However, after GigabitEthernet1/0/1 on DSW1 was reactivated, DSW1 did not become the active router for VLAN 101 as desired. What needs to be done to make the group for VLAN 101 function properly?

- ☒ Enable preempt in the VLAN 101 HSRP group on DSW1.
- ☐ Disable preempt in the VLAN 101 HSRP group on DSW2's.
- ☐ In the VLAN 101 HSRP group on DSW1, decrease the priority value to a value that is less than the priority value configured in the VLAN 101 HSRP group on DSW2.
- ☐ Decrease the decrement value in the track command for the VLAN 101 HSRP group on DSW1's to a values less than the value in the track command for the VLAN 101 HSRP group on DSW2.

Explanation:

Enable preempt on the VLAN 101 HSRP group on DSW1

Issue the "show run" command and you can see that the "standby 1 preempt" configuration command is missing on DSW1. This is needed for it to become the active HSRP router immediately.

QUESTION NO: 187 HOTSPOT

Instructions

This item contains several questions that you must answer. You can view these questions by clicking on the corresponding button to the left. Changing questions can be accomplished by clicking the numbers to the left of each question. In order to complete the questions, you will need to refer to the topology.

To gain access to the topology, click on the topology button at the bottom of the screen. When you have finished viewing the topology, you can return to your questions by clicking on the Questions button to the left.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

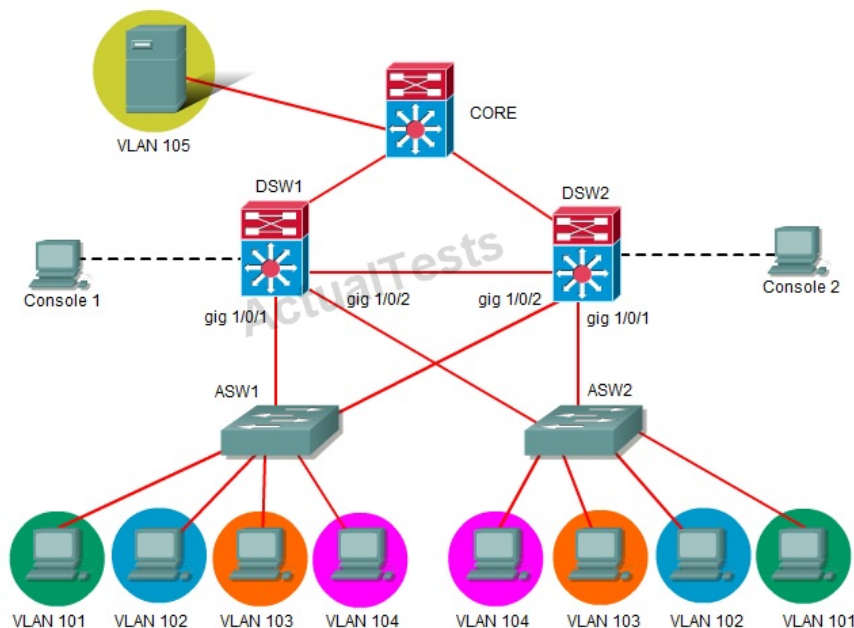
Scenario

Ferris Plastics, Inc. is a medium sized company, with an enterprise network (access, distribution and core switches) that provides LAN connectivity from user PCs to corporate servers. The distribution switches are configured to use HSRP to provide a high availability solution.

- DSW1 - primary device for VLAN 101 VLAN 102 and VLAN 105
- DSW2 - primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthernet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

Troubleshooting has identified several issues. Currently all interfaces are up. Using the running configurations and **show** commands, you have been asked to investigate and respond to the following questions.

Topology



Question #2

During routine maintenance, it became necessary to shut down the GigabitEthernet1/0/1 interface on DSW1. All other interfaces were up. During this time, DSW1 remained the active device for the VLAN 102 HSRP group. You have determined that there is an issue with the decrement value in the track command for the VLAN 102 HSRP group. What needs to be done to make the group function properly?

- ☐ The decrement value on DSW1 should be greater than 5 and less than 15.
- ☐ The decrement value on DSW1 should be greater than 9 and less than 15.
- ☐ The decrement value on DSW1 should be greater than 11 and less than 19.
- ☐ The decrement value on DSW1's should be greater than 190 and less than 200.
- ☐ The decrement value on DSW1's should be greater than 195 and less than 205.

Answer:**Question #2**

During routine maintenance, it became necessary to shut down the GigabitEthernet1/0/1 interface on DSW1. All other interfaces were up. During this time, DSW1 remained the active device for the VLAN 102 HSRP group. You have determined that there is an issue with the decrement value in the track command for the VLAN 102 HSRP group. What needs to be done to make the group function properly?

- ☐ The decrement value on DSW1 should be greater than 5 and less than 15.
- ☐ The decrement value on DSW1 should be greater than 9 and less than 15.
- ☒ The decrement value on DSW1 should be greater than 11 and less than 19.
- ☐ The decrement value on DSW1's should be greater than 190 and less than 200.
- ☐ The decrement value on DSW1's should be greater than 195 and less than 205.

Explanation:

The decrement value on DSW1 should be greater than 11 and less than 19.

The decrement value is currently set to 5 on DSW1 and the priority value is 200. The priority value for VLAN 102 on DSW2 is 190 so the decrement value on DSW should be greater than 11 in order for DSW2 to become active.

QUESTION NO: 188 HOTSPOT**Instructions**

This item contains several questions that you must answer. You can view these questions by clicking on the corresponding button to the left. Changing questions can be accomplished by clicking the numbers to the left of each question. In order to complete the questions, you will need to refer to the topology.

To gain access to the topology, click on the topology button at the bottom of the screen. When you have finished viewing the topology, you can return to your questions by clicking on the Questions button to the left.

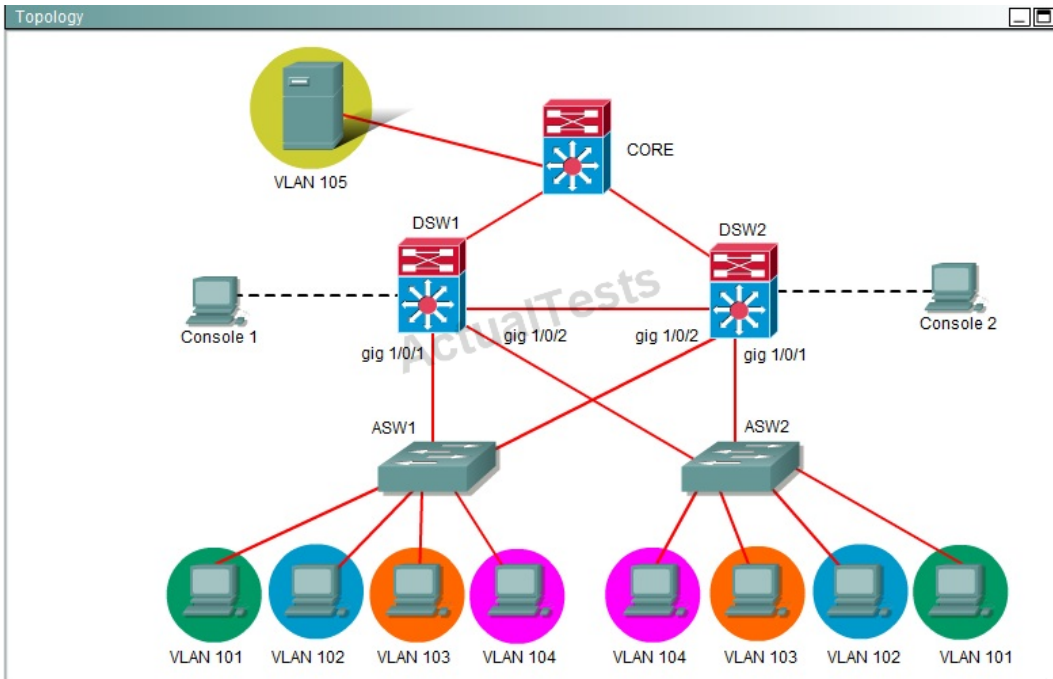
Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

Scenario

Ferris Plastics, Inc. is a medium sized company, with an enterprise network (access, distribution and core switches) that provides LAN connectivity from user PCs to corporate servers. The distribution switches are configured to use HSRP to provide a high availability solution.

- DSW1 - primary device for VLAN 101 VLAN 102 and VLAN 105
- DSW2 - primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthernet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

Troubleshooting has identified several issues. Currently all interfaces are up. Using the running configurations and **show** commands, you have been asked to investigate and respond to the following questions.



Question #6

If GigabitEthernet1/0/1 on DSW2 is shut down, what will be the resulting priority value of the VLAN 105 HSRP group on router DSW2?

- ☐ 90
- ☐ 100
- ☐ 150
- ☐ 200

Answer:

Question #6

If GigabitEthernet1/0/1 on DSW2 is shut down, what will be the resulting priority value of the VLAN 105 HSRP group on router DSW2?

- ☒ 90
- ☐ 100
- ☐ 150
- ☐ 200

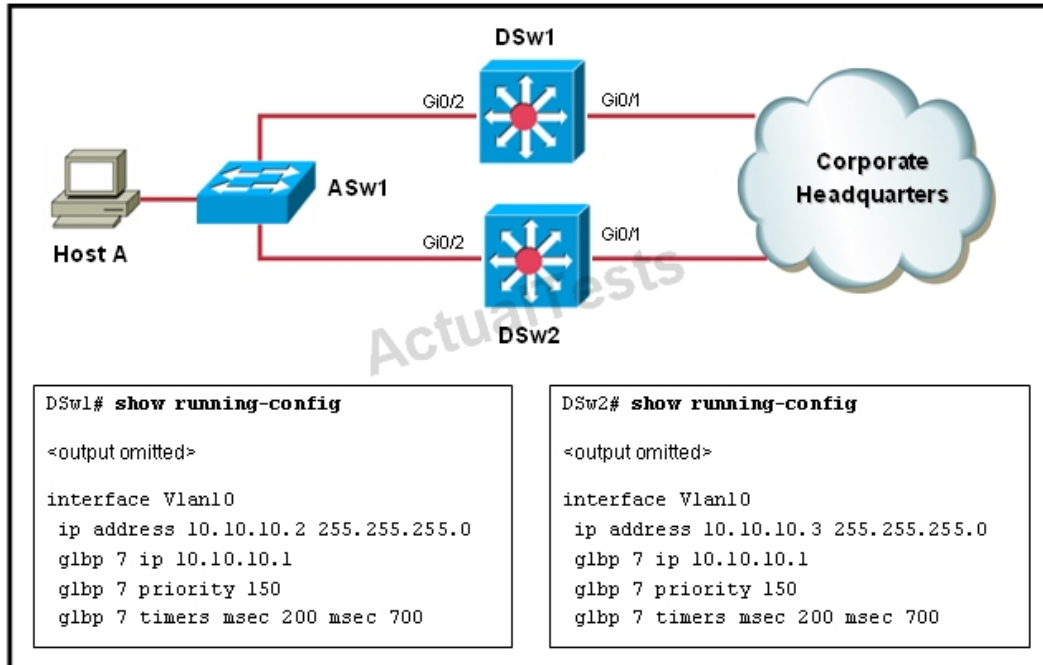
Explanation:

90

The priority and decrement values are not explicitly set for VLAN 105 on DSW2, so it will take the default value of 100 and the default decrement value of 10 for the Gig 1/0/1 interface.

QUESTION NO: 189

Refer to the exhibit.



Host A has sent an ARP message to the default gateway IP address 10.10.10.1. Which statement is true?

- A. Because of the invalid timers that are configured, DSw1 does not reply.
- B. DSw1 replies with the IP address of the next AVF.
- C. DSw1 replies with the MAC address of the next AVF.
- D. Because of the invalid timers that are configured, DSw2 does not reply.
- E. DSw2 replies with the IP address of the next AVF.
- F. DSw2 replies with the MAC address of the next AVF.

Answer: F

Explanation:

The Gateway Load Balancing Protocol (GLBP) is a Cisco-proprietary protocol designed to overcome the limitations of existing redundant router protocols. Some of the concepts are the same as with HSRP/VRRP, but the terminology is different and the behavior is much more dynamic and robust.

The trick behind this load balancing lies in the GLBP group. One router is elected the active virtual gateway (AVG). This router has the highest priority value, or the highest IP address in the group, if there is no highest priority. The AVG answers all ARP requests for the virtual router address.

Which MAC address it returns depends on which load-balancing algorithm it is configured to use. In any event, the virtual MAC address supported by one of the routers in the group is returned. According to exhibit, Router Company2 is the Active Virtual Gateway (AVG) router because it has highest IP address even having equal priority. When router Company1 sends the ARP message to 10.10.10.1 Router Company2 will reply to Company1 as a Active Virtual Router.

Reference: Configuring GLBP

(http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_glb.html)

QUESTION NO: 190

In which three HSRP states do routers send hello messages? (Choose three.)

- A. standby
- B. learn
- C. listen
- D. speak
- E. active

Answer: A,D,E

Explanation:

When HSRP is configured on an interface, the router progresses through a series of states before becoming active. This forces a router to listen for others in a group and see where it fits into the pecking order. The HSRP state sequence is Disabled, Init, Listen, Speak, Standby, and, finally, Active.

Only the standby (second highest priority) router monitors the hello messages from the active router. By default, hellos are sent every 3 seconds. If hellos are missed for the duration of the holdtime timer (default 10 seconds, or 3 times the hello timer), the active router is presumed down. The standby router is then clear to assume the active role. If other routers are sitting in the Listen state, the next-highest priority router is allowed to become the new standby router.

Reference: Cisco Hot Standby Router Protocol (HSRP)

(<http://tools.ietf.org/html/rfc2281#page-8>)