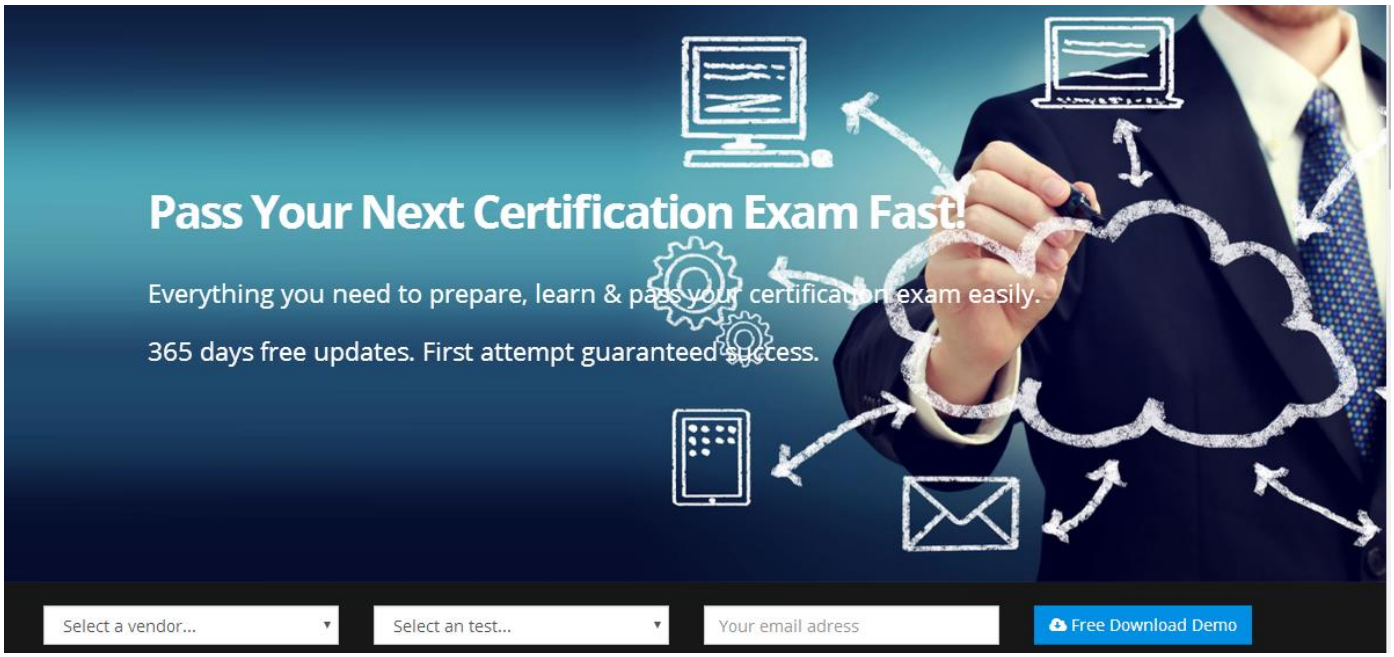
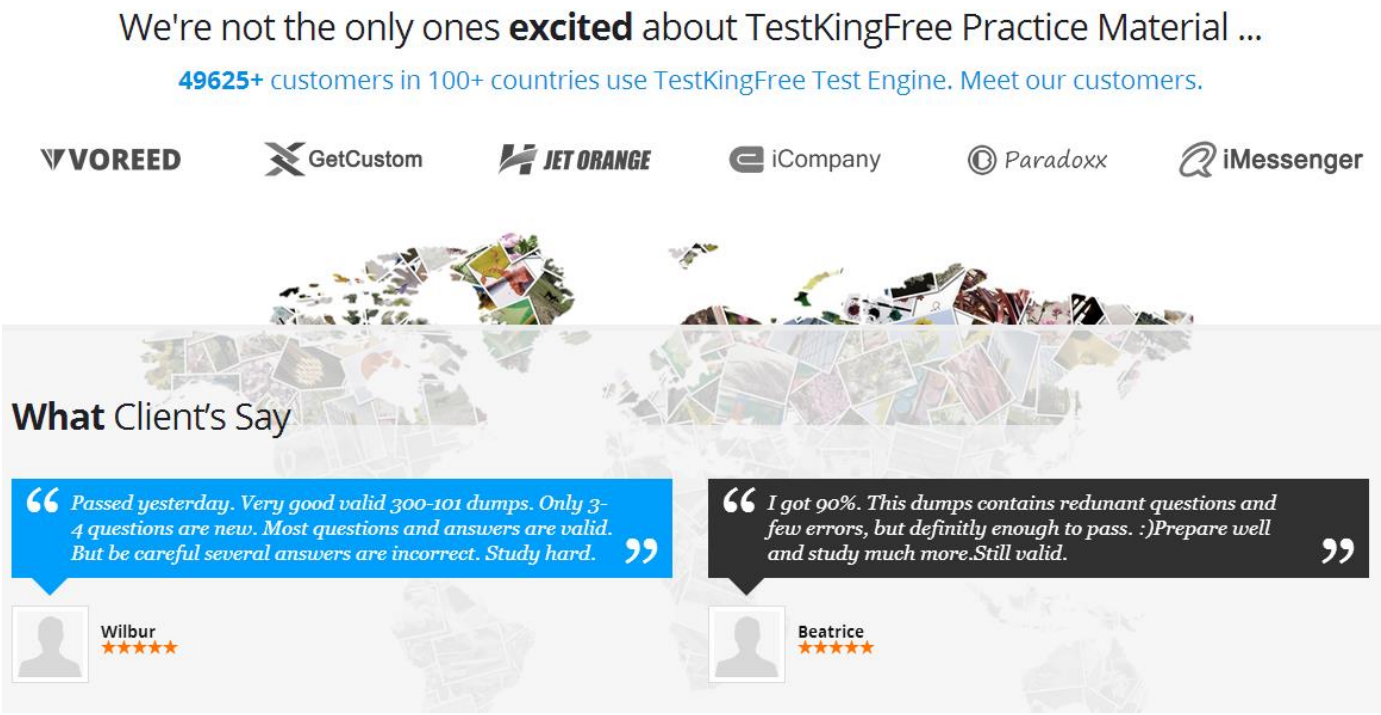
TestKingfree





http://www.testkingfree.com/

Pass For sure Certification Exam Guide and Exam Dumps - TestKingFree

Exam : **642-813**

Title : Implementing Cisco IP Switched Networks

Vendor : Cisco

Version : DEMO

NO.1 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/

NO.2 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

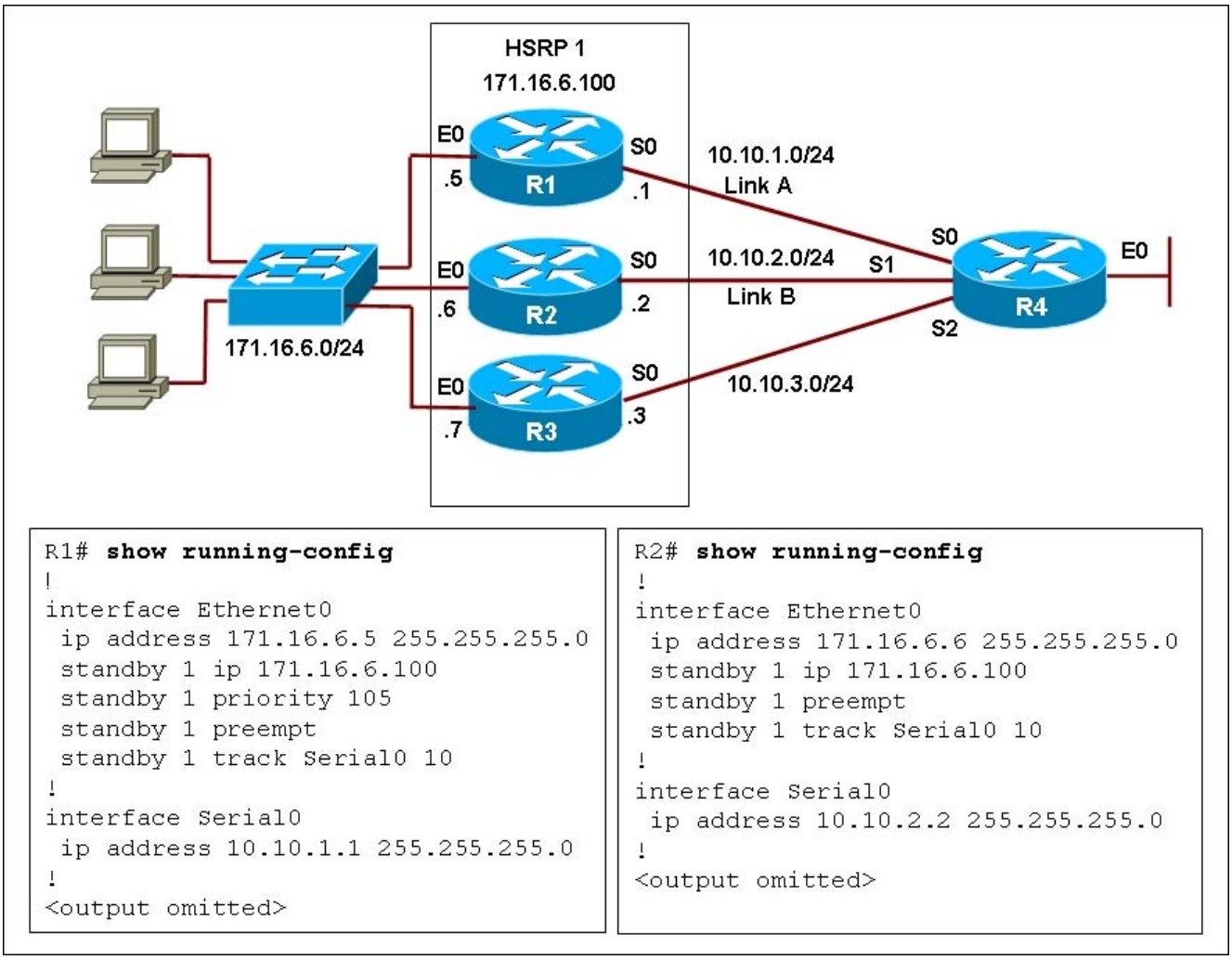
NO.3 Which three items are configured in MST configuration submode? (Select three)
A. Region name
B. Configuration revision number
C. VLAN instance map
D. IST STP BPDU hello timer
E. CST instance map
F. PVST+ instance map
Answer: A,B,C
Explanation:
spanning-tree mst configuration:
Use the spanning-tree 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:

NO.4 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

NO.5 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: A
Explanation:
In addition to propagating VTP information, version 3 can propagate Multiple Spanning Tree (MST) protocol database information. A separate instance of the VTP protocol runs for each application that uses VTP.
Reference:
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/122_52_se/configuration/guide/3560scg/swvtp.html

NO.6 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.

NO.7 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/c hannel.html

NO.8 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.

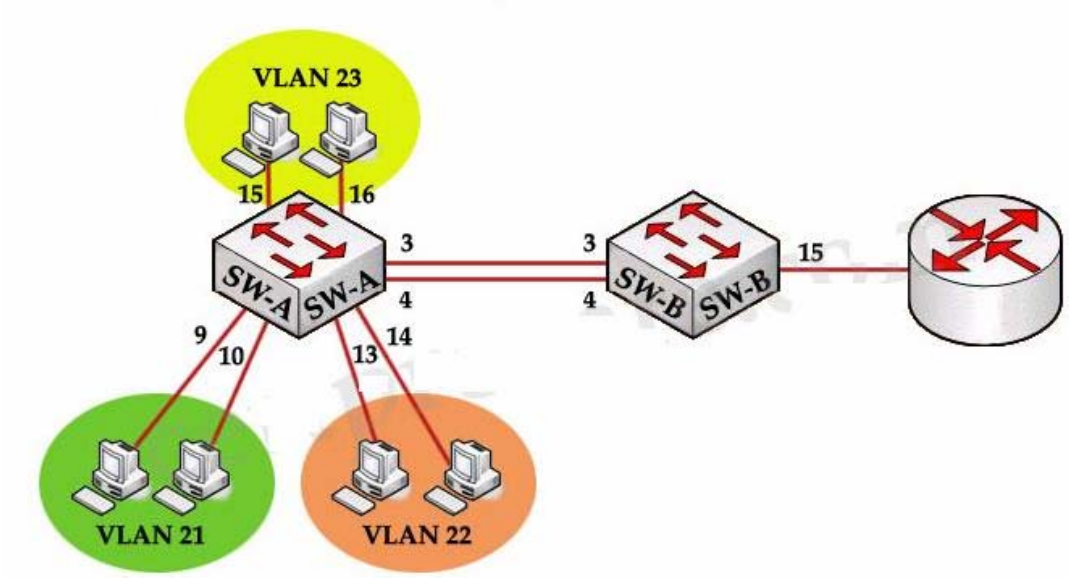
E. Traffic on VLAN 1 that is sent out gigabitethernet 0/1 will have an 802.1q header applied.

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.

NO.9 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 accress vlan 21
spanning-tree portfast
no shut
interface rang fastethernet 0/13-14
switchport mode access
switchport accress vlan 22
spanning-tree portfast
no shut
interface rang fastethernet 0/15-16
switchport mode access
switchport accress 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

NO.10 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

NO.11 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.

NO.12 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

NO.13 Refer to the exhibit.

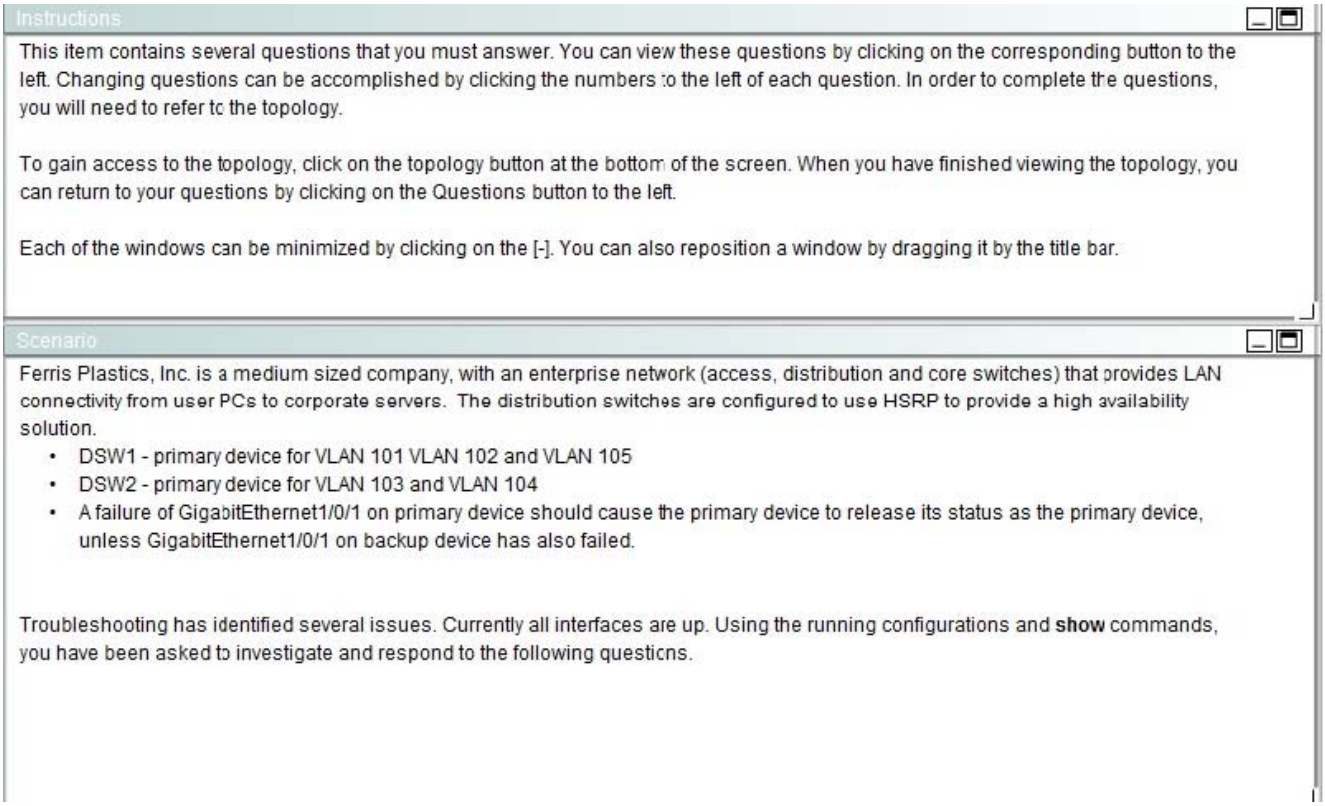
```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# private-vlan community
Switch(config-vlan)#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

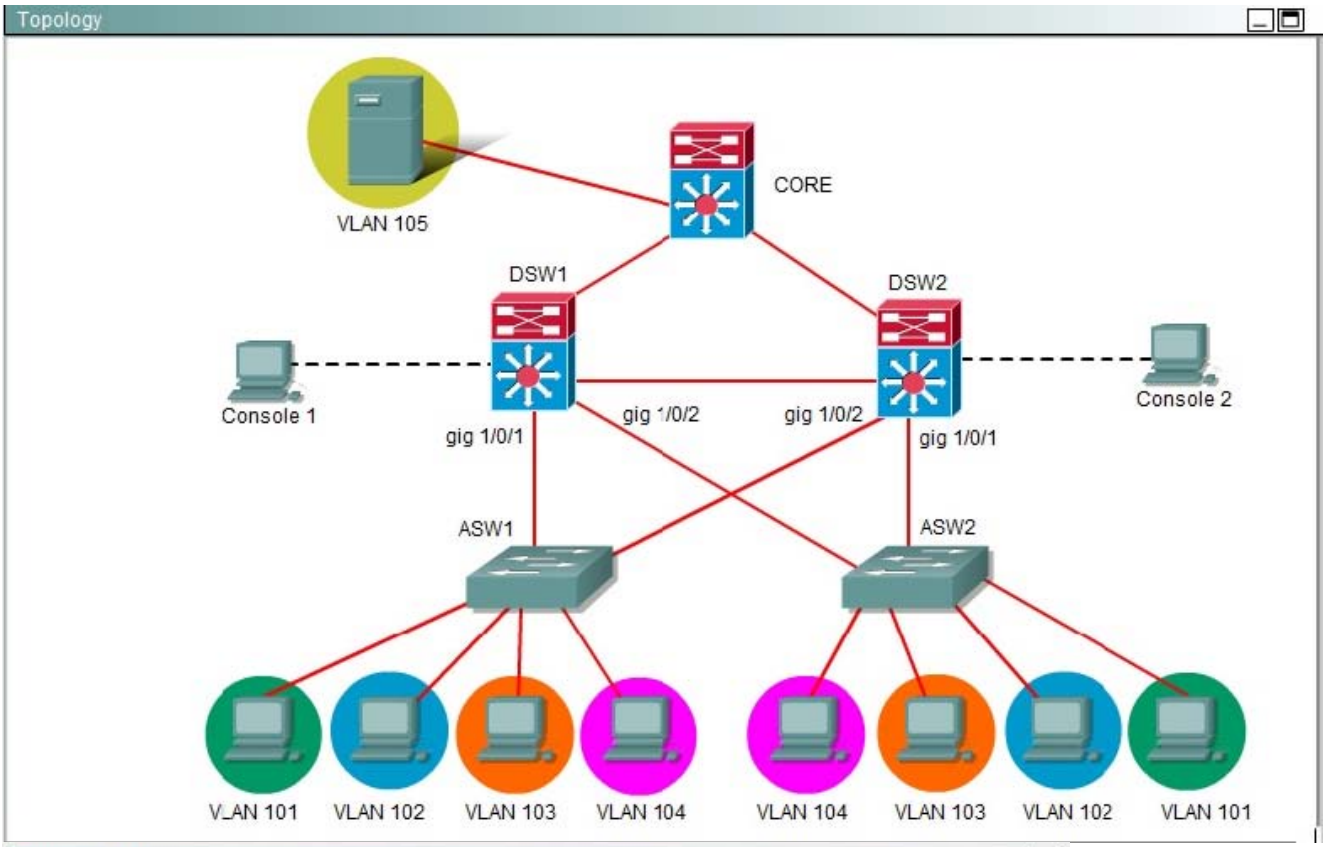
Which statement about the private VLAN configuration is true?
A. Only VLAN 503 will be the community PVLAN, because multiple community PVLANs are not allowed.
B. Users of VLANs 501 and 503 will be able to communicate.
C. VLAN 502 is a secondary VLAN.
D. VLAN 502 will be a standalone VLAN, because it 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

NO.14 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)

NO.15 HOTSPOT



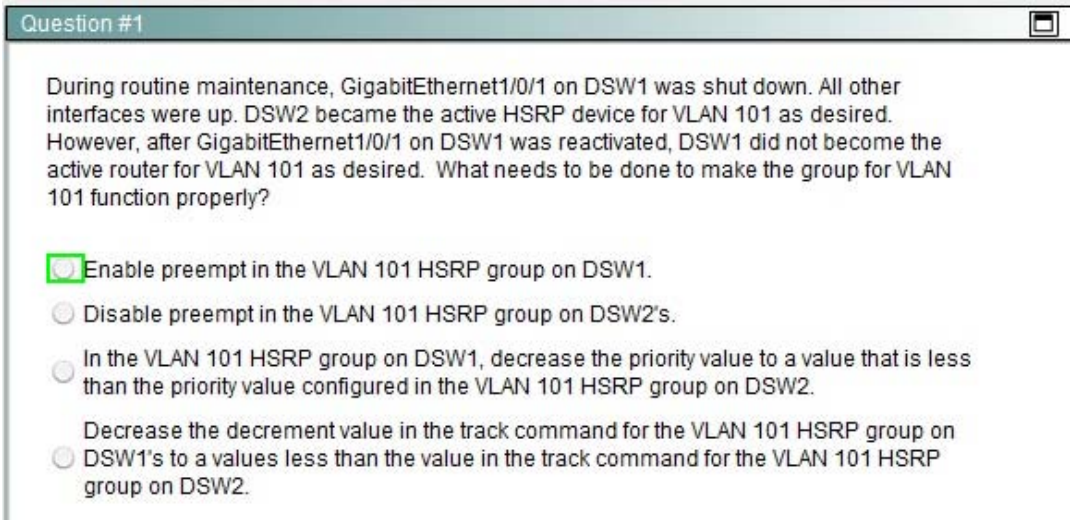


Question #1

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:



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.