Cisco 642-813

Implementing Cisco IP Switched Networks (SWITCH)

Version: Demo 12.2

QUESTION NO: 1

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

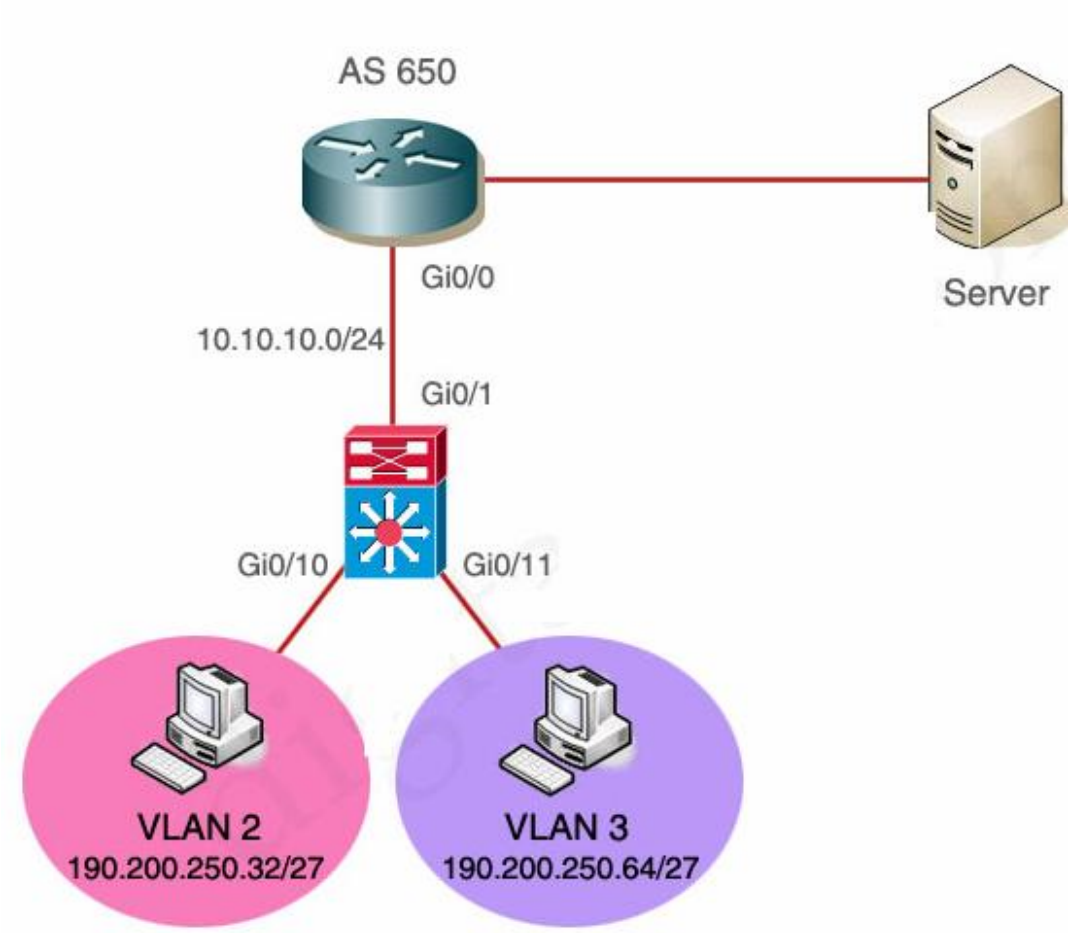
Reference:

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: 2 CORRECT TEXT

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

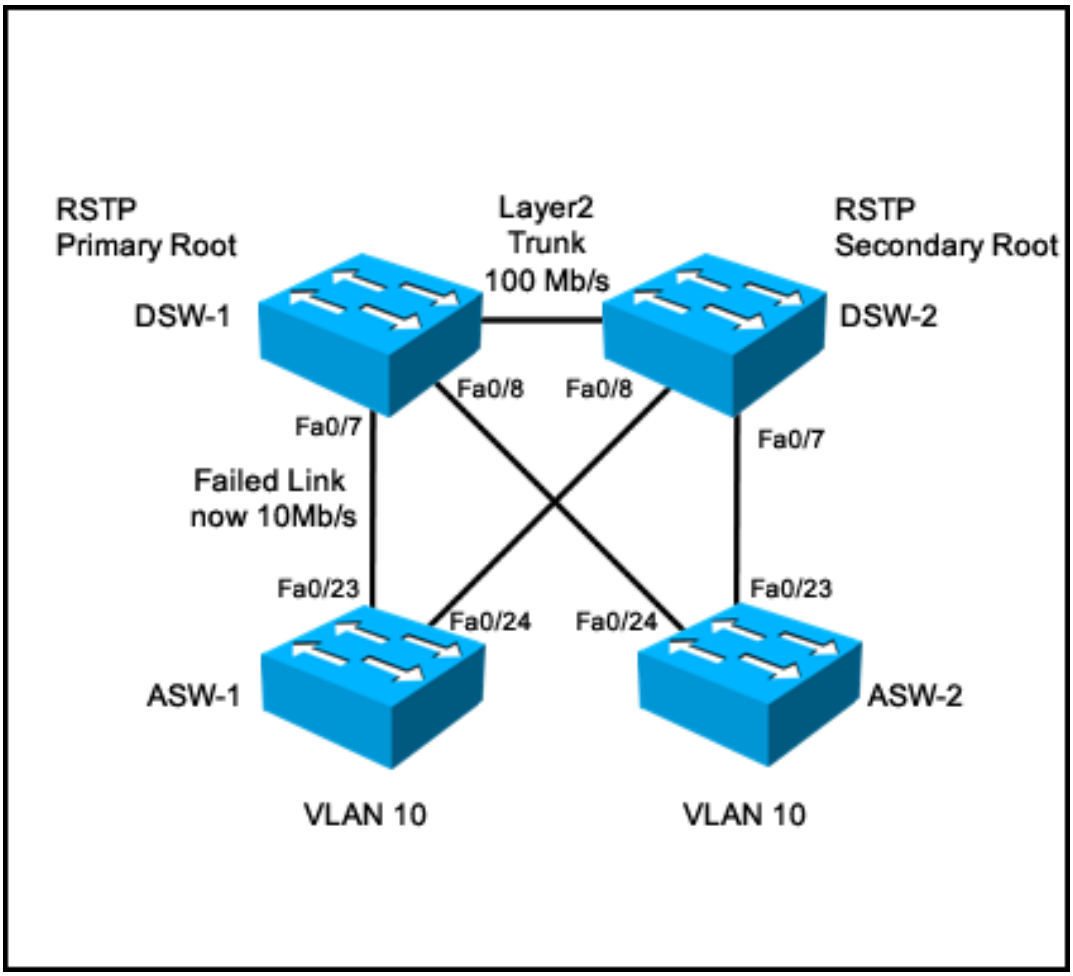


Answer: mls>enable
mls# configure terminal
mls(config)# int gi0/1
mls(config-if)#no switchport -> not sure about this command line, but you should use this command if the simulator does not let you assign IP address on Gi0/1 interface.
mls(config-if)# ip address 10.10.10.2 255.255.255.0
mls(config-if)# 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: 3

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:

QUESTION NO: 4

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: 5

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:

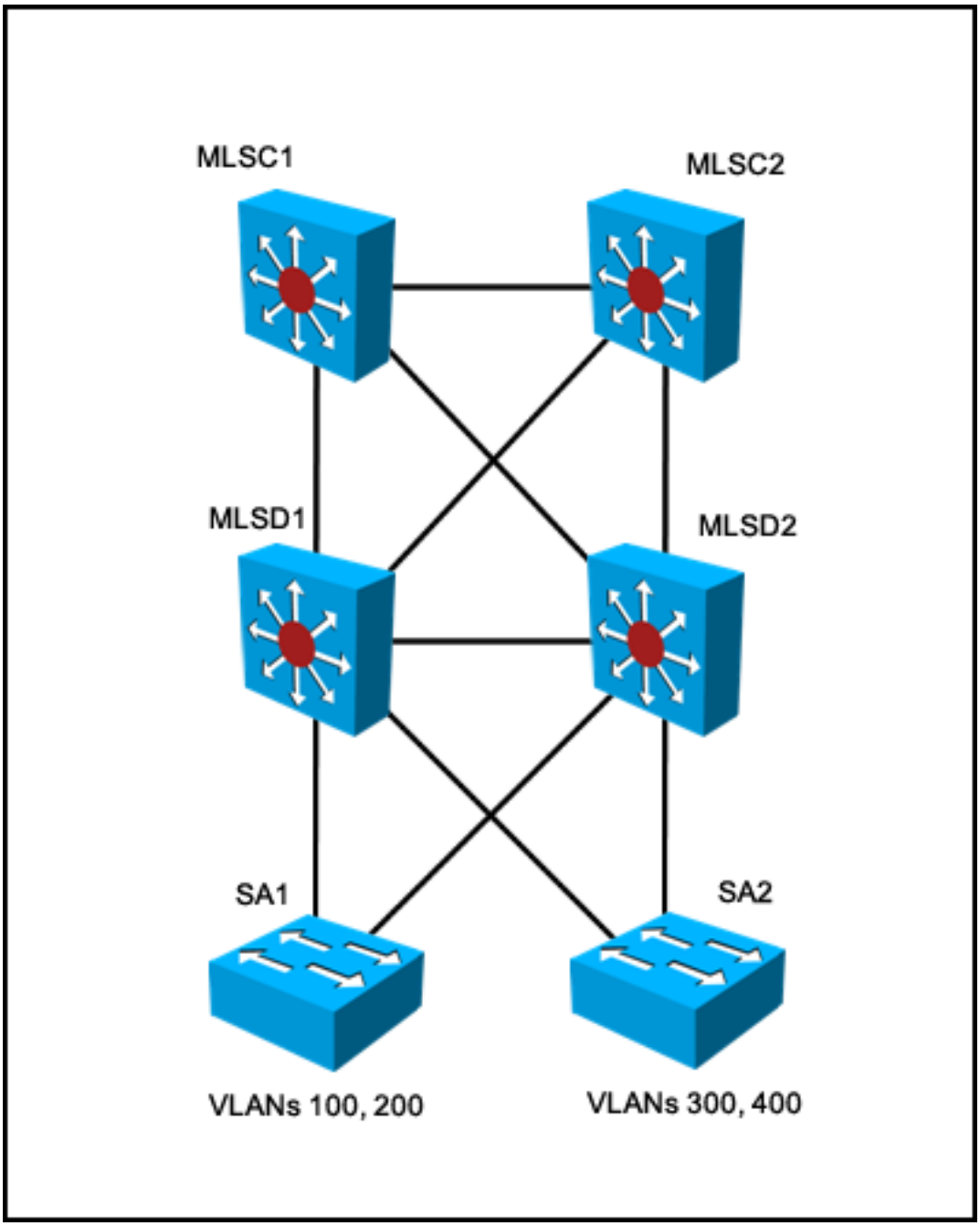
The port is operational (Port status: SecureUp) and has reached its configured maximum allowed number of MAC addresses (Maximum MAC addresses: 11, Total MAC addresses: 11).

Reference:

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

QUESTION NO: 6

Refer to the exhibit.



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

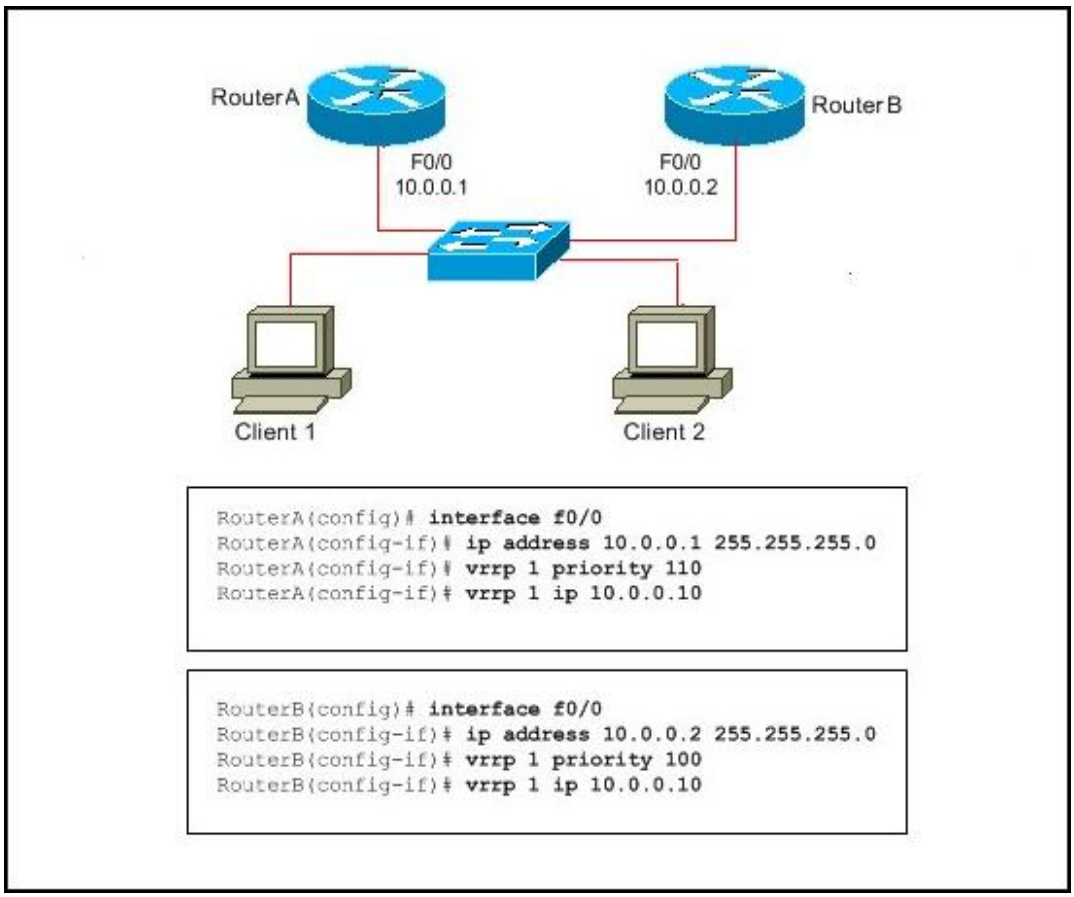
A. determine which switch is the root bridge then connect a router on a stick to it
B. configure SVIs on the core switches
C. configure SVIs on the distribution switches
D. configure SVIs on the access layer switches

Answer: C

Explanation:

QUESTION NO: 7

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 regains the master virtual router role.

Answer: B

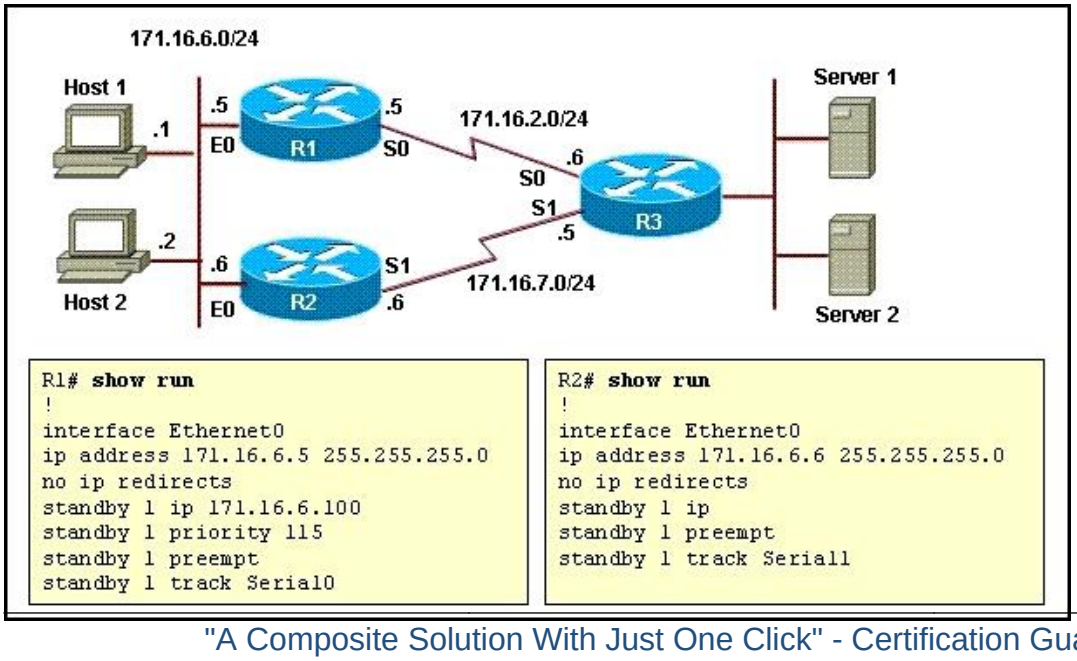
Explanation: An important aspect of the VRRP redundancy scheme is VRRP router priority. Priority determines the role that each VRRP router plays and what happens if the master virtual

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.

Reference: 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.html

QUESTION NO: 8

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

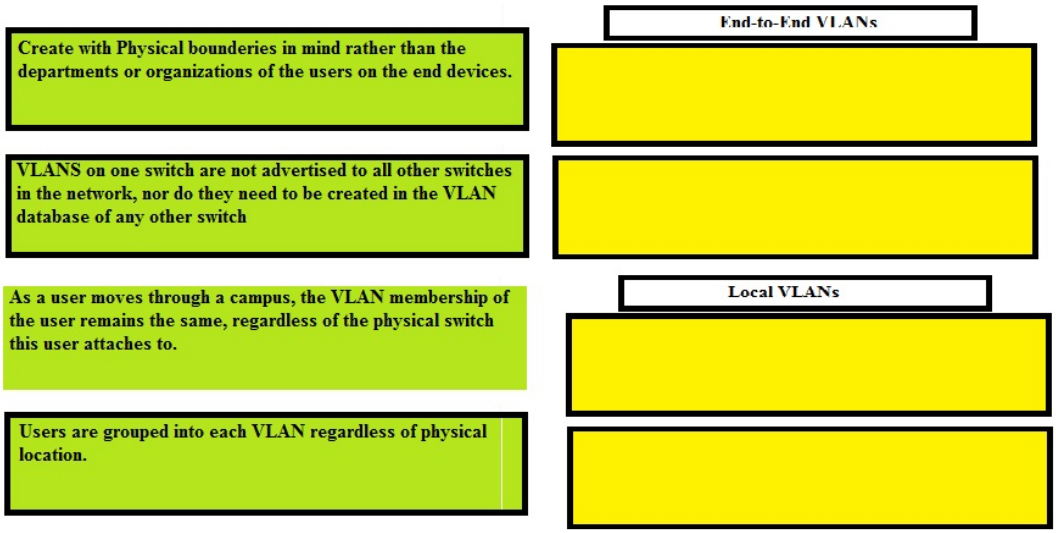
Explanation:

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.

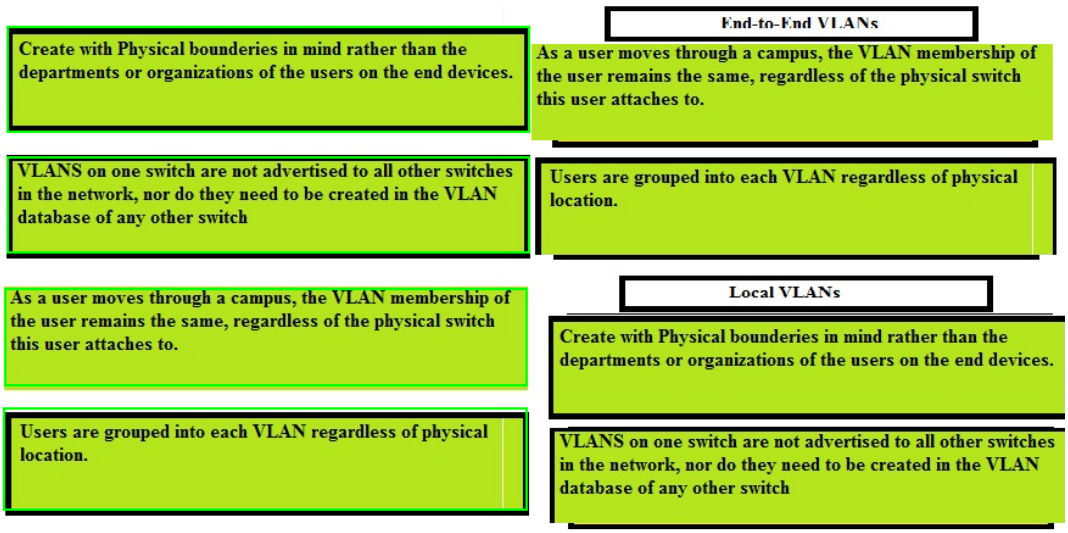
Reference: Configuring HSRP (http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_12c_ea1/configuration/guide/swhsrp.html)

QUESTION NO: 9 DRAG DROP

Match the Attributes on the left with the types of VLAN designs on the right.



Answer:



Explanation:

Local VLANs

End-to-End VLANs

QUESTION NO: 10

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 hoping 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