

## RealTest.HP0-Y47,55.Q&A

Number: HP0-Y47  
Passing Score: 800  
Time Limit: 120 min  
File Version: 21.05



Deploying HP FlexNetwork Core Technologies

- ➡ I have corrected few questions and now score will be 95% above Guaranteed.
- ➡ Finally, I got right questions for this exam and share with you guys. Best Wishes.
- ➡ This is the best VCE I ever made. Try guys and if any suggestion please update this.
- ➡ Modified few questions, fixed few spelling mistakes and typos.
- ➡ Nicely written Questions with many corrections inside.

**Exam A****QUESTION 1**

An HP Provision switch port is implementing MAC Authentication (MAC-Auth) to a RADIUS server. A device connects to the port, and the switch submits a RADIUS Access-Request to the server. What correctly describes how the switch determines the username and password for the request?

- A. Depending on the configuration, the switch sends the device MAC address for the username or a configured username. It sends the device MAC address for the password or a configured password
- B. The switch always sends the device MAC address as the username. It always sends "provision" for the password, and this password cannot be reconfigured.
- C. The switch always sends the device MAC address as the username. Depending on the configuration, the password is the device MAC address or a configured password.
- D. The switch always sends the device MAC address as the username and the password, and this behavior cannot be reconfigured.

**Correct Answer:** D

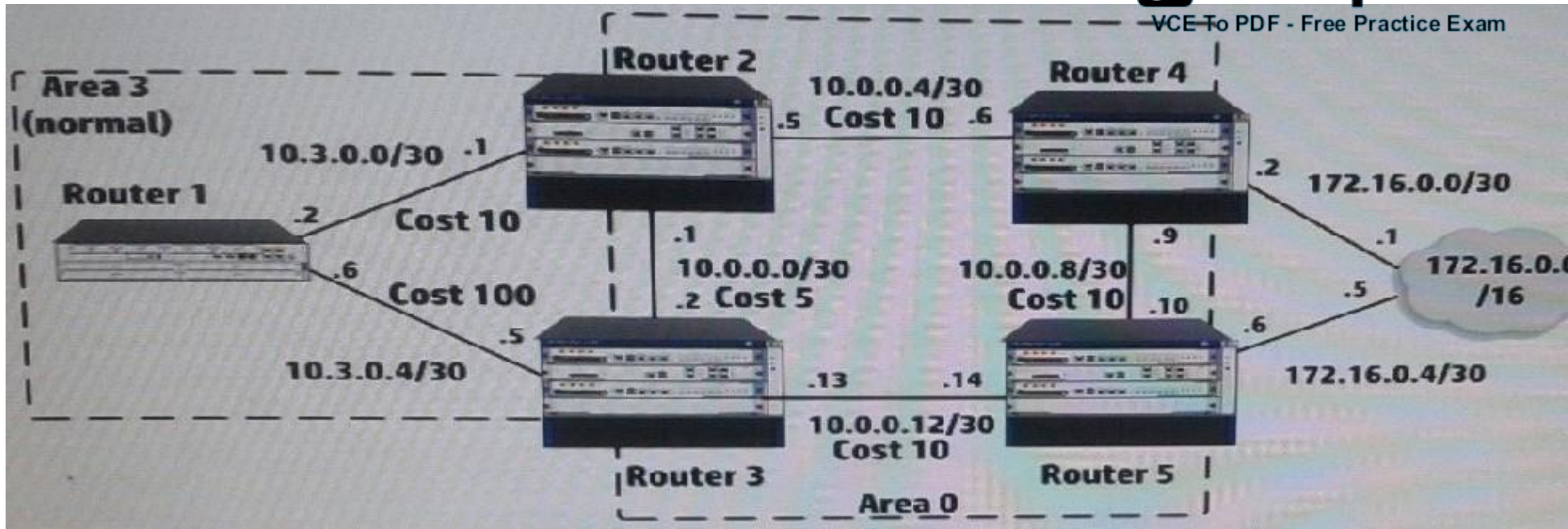
**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 2**

Refer to the exhibit.



The five routers shown in the exhibit are successfully implementing OSPF on the interface shown in the exhibit. The exhibit also shows settings for OSPF areas and interface costs.

A network administrator enters these commands on Router 4 and Router 5:

```
[Router4] ip route-static 172.16.0.0 16 172.16.0.1
[Router4] ospf 1
[Router4-ospf-1] redistribute static type 2 cost 5

[Router5] ip route-static 172.16.0.0 16 type 2 172.16.0.5
[Router5] ospf 1
[Router5-ospf-1] redistribute static type 2 cost 1
```

How can the administrator ensure that Router 2 learns the route to 172.16.0.0/16 with next hop 10.0.0.6?

A. On Router 2, enables OSPF ECMP globally

- B. On Router 4 and 5, change the metric type for redistributed static routes to type 1
- C. On Router 4, change the cost for redistributed static routes to 2
- D. On Router 2, 3, 4 and 5, change the bandwidth reference value to 100

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 3**

Refer to the exhibit.

Exhibit 1

IRF = Intelligent Resilient Framework  
 RAGG = Routed link aggregation group  
 BAGG = Bridged link aggregation group

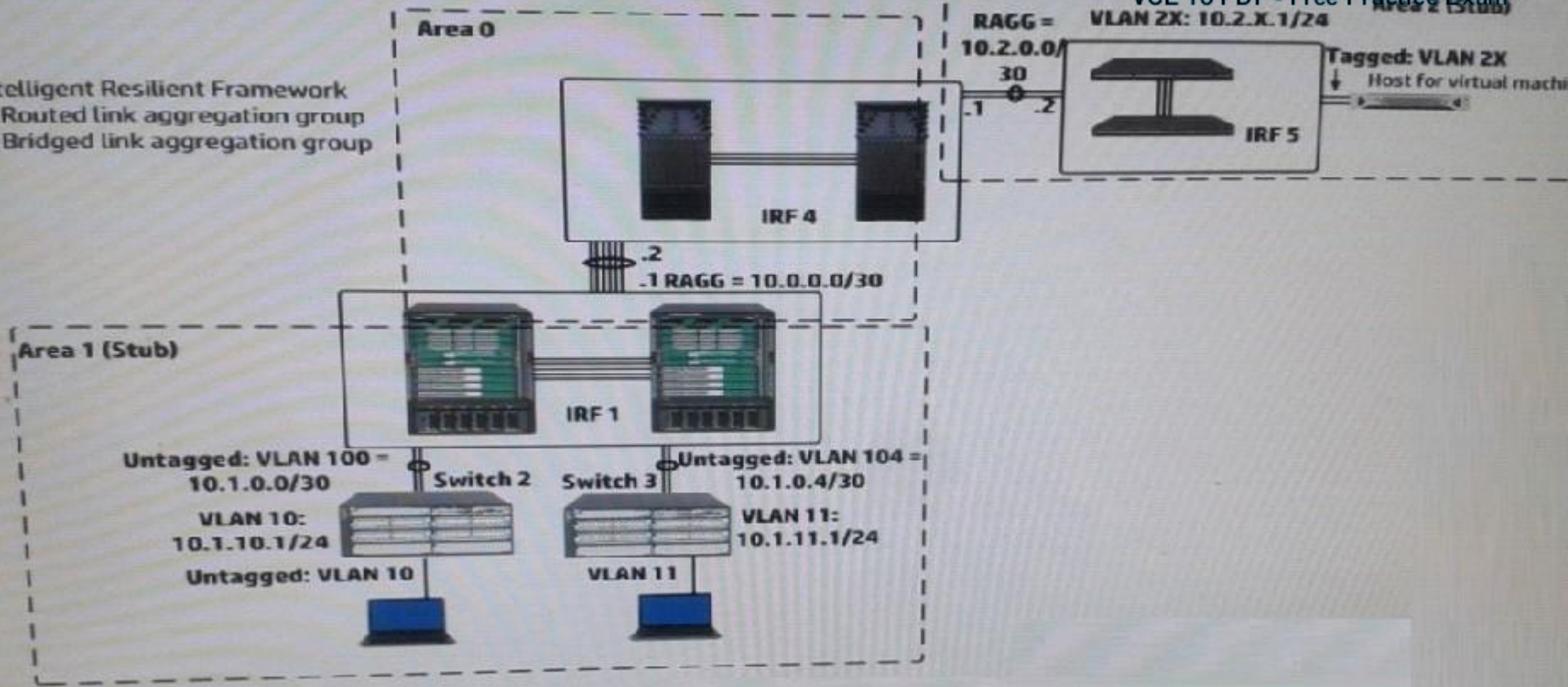


Exhibit 2

```
[IRF-1-ospf-1]display this

ospf 1
 area 0.0.0.0
  abr-summary 10.0.0.0 255.255.0.0 cost 1
  network 10.0.0.0 0.0.255.255
 area 0.0.0.1
  abr-summary 10.1.0.0 255.255.0.0 cost 1
  network 10.1.0.0 0.0.255.255
 stub
```



Exhibit 1 shows a simplified network topology. All infrastructure devices shown in the exhibit are successfully implementing OSPF on the interfaces. The exhibit also shows settings for OSPF areas. Exhibit 2 shows additional settings on IRF. The master within IRF 1 fails. Connectivity is disrupted for about one minute.

What can the network administrator do to prevent this issue occurring again?

- A. Set up OSPF Bidirectional Forwarding Detection (BFD) on the routed link aggregation groups between the IRF virtual switches
- B. Enable extended Link Access Control Detection Data Units (LACPDUs) on IRF 1 and IRF 4
- C. On IRF 1, set up Bidirectional Forwarding Detection (BFD) Multi-Access Detection (MAD) with a dedicated link.
- D. On each of the IRF virtual switches, enable opaque LSAs and set the OSPF graceful restart mode to IETF mode.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 4

A company plans to use Intelligent Management Center CMC) Network Traffic Analyzer (NTA) to monitor network utilization. How do HP switches with the solution?

- A. Provision switches use the NTA server as their sFlow collector. Comware switches use the NTA server as their NetStream server.
- B. Provision switches use the NTA server as their sFlow collector. NetStream server, or both Comware switches use the NTA server as their sFlow collector NetStream server, or both.
- C. ProVision switches use the NTA server as their sFlow collector. Comware switches as their sFlow collector, NetStream server, or both.
- D. ProVision switches use the NTA server as their sFlow collector, NetStream server, or both. Comware switches use the NTA server as their sFlow collector

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

HP Intelligent Management Center Network Traffic Analyzer Software

Product overview

HP IMC Network Traffic Analyzer (NTA) Software Module is a graphical network-monitoring tool that provides network administrators with real-time information about users and applications consuming network bandwidth. A reliable solution for enterprise and campus network traffic analysis, it defends the network against virus attacks and applies varying levels of bandwidth traffic to different services and applications. The IMC NTA software module's

network bandwidth statistics help plan, monitor, enhance, and troubleshoot networks, as well as identify bottlenecks and apply corrective measures for enhanced throughput. The software also monitors Internet egress traffic, helping administrators to analyze the bandwidth usage of specific applications and monitor the impact of non-business applications (e.g., network games) on user productivity. Granular, network-wide surveillance of complex, multilayer switched and routed environments helps rapidly identify and resolve network threats.

Real-time monitoring of database space  
Automatic generation of four types of reports  
Uses instruments embedded in switches/routers  
Support for sFlow, NetFlow, and NetStream  
Granular insight of applications, users, and ports

NetStream module -- Provides traffic analysis and statistics capture to allow network administrators to rapidly identify network anomalies and security threats as well as obtain capacity planning information; and supports NetFlow v5 and v9 (JD254A Comware v5 only)

### QUESTION 5

A company has configured two switches as an HP Intelligent Resilient Framework (IRF) virtual device. The IRF port on each switch is bound to multiple physical links. How does the switch select the link for transmitting packets on that IRF port?

- A. It uses a round-robin mechanism in which it sends each packet over a different link in turn.
- B. It uses a weighted round-robin mechanism, in which it sends each packet over a different link in turn, but can send more packets over certain links over higher weighted.
- C. It uses one of the links as an active link, the other links are in standby mode and can become active if the active link fails
- D. It uses a hash of various Layer 2, 3, or 4 information in the packet, depending on the type of traffic, the switch model, and the IRF load-sharing.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

answer is corrected.

### QUESTION 6

Refer to the exhibits.

Exhibit1

**S** System >> SNMP Template >> Add SNMP Template

**Add SNMP Template**

* Name	imc_snmpv3
* Parameter Type	SNMPv3 Priv-Aes128 Auth-Sha
* Username	imc
* Authentication Password	••••••••
* Encryption Password	••••••••
* Timeout (1-60 seconds)	4
* Retries (1-20)	3

OK Cancel

Exhibit 2



```
Provision-Switch# show snmpv3 enable
```

```
Status and Counters - SNMP v3 Global Configuration Information
SNMP v3 enabled : Yes
```

```
Provision-Switch# show snmpv3 user
```

```
Status and Counters - SNMP v3 Global Configuration Information
```

User Name	Auth. Protocol	Privacy Protocol
imc	SHA	CFB AES-128

```
Provision-Switch# show snmpv3 group
```

```
Status and Counters - SNMP v3 Global Configuration Information
```

Security Name	Security Model	Group Name
CommunityManagerReadonly	ver1	ComManagerR
CommunityManagerReadwrite	ver1	ComManagerRW
CommunityOperatorReadonly	ver1	ComOperatorR
CommunityOperatorReadwrite	ver1	ComOperatorRW
CommunityManagerReadonly	ver2c	ComManagerR
CommunityManagerReadwrite	ver2c	ComManagerRW
CommunityOperatorReadonly	ver2c	ComOperatorR
CommunityOperatorReadwrite	ver2c	ComOperatorRW

Exhibit 1 shows the SNMP template that HP Intelligent Management Center (IMC) will use when discovering an HP Provision switch. Exhibit 2 settings on the switch. IMC should have rights to read and write any parameter on the switch.

Which task must the network administrator complete to accomplish this?

- A. Create an MIB view and assign it to the "imc" user
- B. Enable the ver3 security model for the "CommunityManagerReadWrite" user
- C. Adding the "imc" user to the ManagerPriv group

D. Change the "imc" user to ver2c mode

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

<http://www.networktasks.co.uk/environments/hp/provision/snmpv3-and-imc>  
want to now create a more secure user, with SHA and AES-128

snmpv3 user imc auth sha mysecurepassword priv aes myprivpassword  
Add the user to the managerpriv group

snmpv3 group managerpriv user imc sec-model ver3

### QUESTION 7

A network administrator is configuring several HP Comware switches as an HP Intelligent Resilient Framework (IRF) virtual device. According to best practices at, which point during the IRF configuration process should the administrator activate the IRF ports?

- A. After enabling the physical interfaces that are assigned to IRF ports and saving the settings
- B. After configuring IRF ports but before assigning physical interfaces to them
- C. After enabling the physical interfaces that are assigned to IRF ports but before saving the settings
- D. Before configuring IRF ports or assigning physical interfaces to them

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Use the irf-port-configuration active command to activate configurations on all IRF ports on the device. When you physically connect members of an IRF virtual device and bind physical IRF port(s) to an IRF port whose link state is DIS or DOWN, which you can display with the display irf topology command, execution of this command is required to establish the IRF virtual device.

Note that activating IRF port configurations may cause merge of IRF virtual devices and automatic device reboot. Therefore, to avoid configuration loss you are recommended to set the member ID for the device in the following way:

- 1) Plan the network and member IDs in advance. Determine the number of IRF ports to be created, and which physical IRF ports is used for IRF virtual device establishment.
- 2) Change member IDs. (Member ID change takes effective after device reboot, so change member IDs before executing the irf-port- configuration active command.)
- 3) Connect SFP+ cables or fibers and make sure that the physical IRF ports are well connected.
- 4) Create IRF ports.
- 5) Bind physical IRF ports to IRF ports.

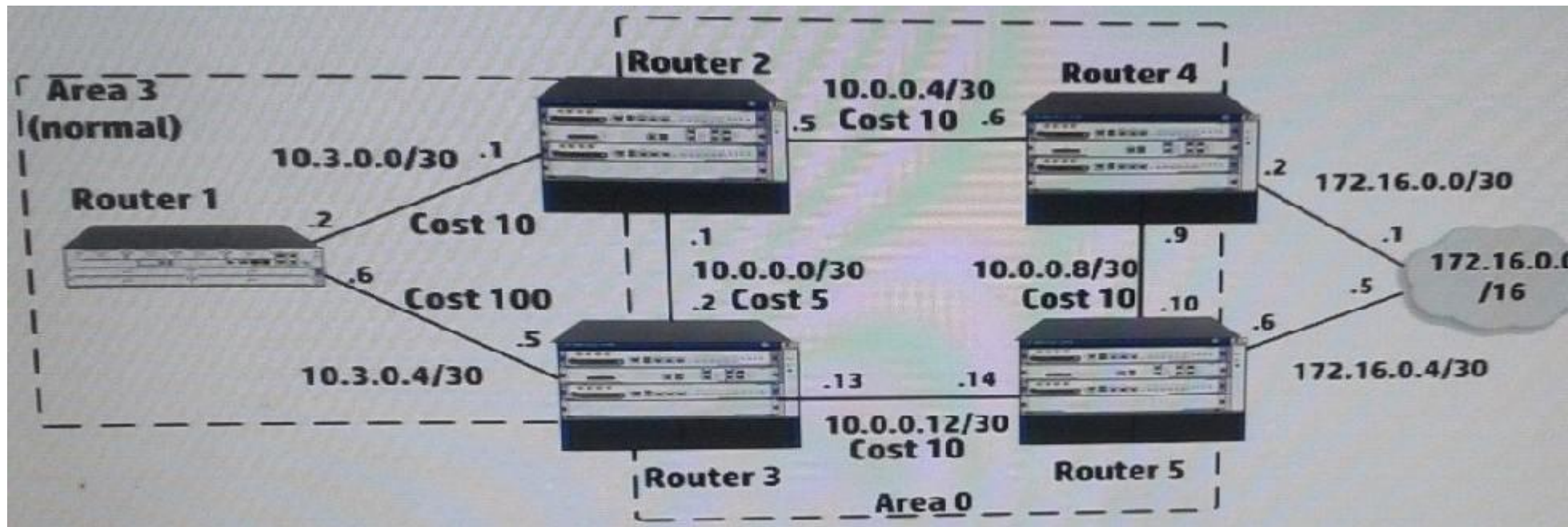
6) Save the current configurations to the configuration file to be used at the next startup.

7) Activate configurations on all IRF ports.

When the system starts up, if you bind a physical IRF port to an IRF port through the configuration file, or add a new physical port, configurations on IRF ports are automatically activated without the need to execute this command again.

#### QUESTION 8

Refer to the exhibit.



The five routers shown in the exhibit are successfully implementing OSPF on the interface shown in the exhibit. The exhibit also shows settings for OSPF areas and interface costs.

A network administrator enters these commands on Router 4 and Router 5:



```
[Router4] ip route-static 172.16.0.0 16 172.16.0.5
[Router4] ospf 1
[Router4-ospf-1] redistribute static type 2 cost 5

[Router5] ip route-static 172.16.0.0 16 172.16.0.5
[Router5] ospf 1
[Router5-ospf-1] redistribute static type 2 cost 1
```

Which statement correctly describes the OSPF routing table on Router 2?

- A. It has one next hop for 172.16.0.0/16, 10.0.0.6
- B. It has one next hop for 172.16.0.0/16, 10.0.0.2
- C. It has not learned a route to 172.16.0.0/16
- D. It has one next hop for 172.16.0.0/16, 10.0.0.6, and 10.0.0.2

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 9

The network administrator is configuring Unidirectional Link Detection (UDLD) on trk1 on an HP Provision switch. The trk1 link aggregation group has these settings:

Interfaces = 48 and 49  
Untagged VLAN = 1  
Tagged VLANs = 2-4

How should the administrator complete the setup?

- A. Enable link-keepalive on both interfaces in the trunk (48 and 49).
- B. Enable link-keepalive on interface 48, specifying the VLAN as 1.
- C. On both interfaces in the trunk (48 and 49), enable link-keepalive, specifying the VLAN as 1.
- D. Enable link-keepalive on trk1

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

[ftp://ftp.hp.com/pub/networking/software/2900yl-MCG-0207-T\\_12\\_XX-Chap10-PrtStat-BasicCfg.pdf](ftp://ftp.hp.com/pub/networking/software/2900yl-MCG-0207-T_12_XX-Chap10-PrtStat-BasicCfg.pdf)

#### **QUESTION 10**

A company wants to enforce source-specific multicasting (SSM) for several multicast streams.

This is the configuration:

Some multicast receivers support IGMPv3.

Other receivers that need to stream support IGMPv2 only.

The multicast receivers' default routers enable IGMPv3 on the interfaces associated with their subnets. The routers are correctly configured to enable the IGMPv3 receivers to receive the stream from the correct source

Which setting do the receivers' routers require to support the IGMPV2 devices?

- A. An SSM policy that selects the IGMPv2 devices and binds them to an RP address
- B. An SSM map that sets a rendezvous point (RP) for each multicast address
- C. An SSM policy that selects the appropriate multicast destinations and binds them to an RP address
- D. An SSM map that sets the correct source for each multicast address

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

[http://h20565.www2.hp.com/hpsc/doc/public/display?sp4ts.oid=6796027&docId=emr\\_na-c04412136&docLocale=en\\_US](http://h20565.www2.hp.com/hpsc/doc/public/display?sp4ts.oid=6796027&docId=emr_na-c04412136&docLocale=en_US)

IGMP SSM mapping

The IGMP SSM mapping feature provides SSM support for receiver hosts that are running IGMPv1 or IGMPv2. This feature is implemented by configuring static IGMP SSM mappings on the IGMP-enabled routers.

The SSM model assumes that the IGMP-enabled routers have identified the desired multicast sources when receivers join multicast groups. · A host running IGMPv3 can explicitly specify multicast source addresses in its reports. · A host running IGMPv1 or IGMPv2, however, cannot specify multicast source addresses in its reports. In this case, you must configure the IGMP SSM mapping feature to translate the (\*, G) information in the IGMPv1 or IGMPv2 reports into (G, INCLUDE, (S1, S2...)) information

[http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/multicast/configuration/guide/b\\_multicast/b\\_multicast\\_chapter\\_011.html#task\\_E5D313413C374821B9964D5B0E3590D8](http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/multicast/configuration/guide/b_multicast/b_multicast_chapter_011.html#task_E5D313413C374821B9964D5B0E3590D8)

#### **QUESTION 11**

Refer to the exhibit.



```
<Router1> display bgp routing
```

```
Total Number of Routes: 2
```

```
BGP Local router ID is 192.0.2.1
```

```
Status codes: * - valid, ^ - VPN best, > - best, d - damped,  
h - history, i - internal, s - suppressed, S - stale  
Origin : i - IGP, e - EGP, ? - incomplete
```

	Network	NextHop	MED	LocPrf	PrefVal	Path/O
* >	203.0.13.0	192.0.2.2			0	2,4?
*		198.5.100.1			0	3,5,4?

Which route to 203.0.13.0/24 will the switch BGP process propose to the routing table?

- A. A null route
- B. A route through 192.0.2.2
- C. A route through 198.5.100.1
- D. A route through 198.5.100.1 and 192.0.2.1

**Correct Answer:** B

**Section:** (none)

**Explanation**

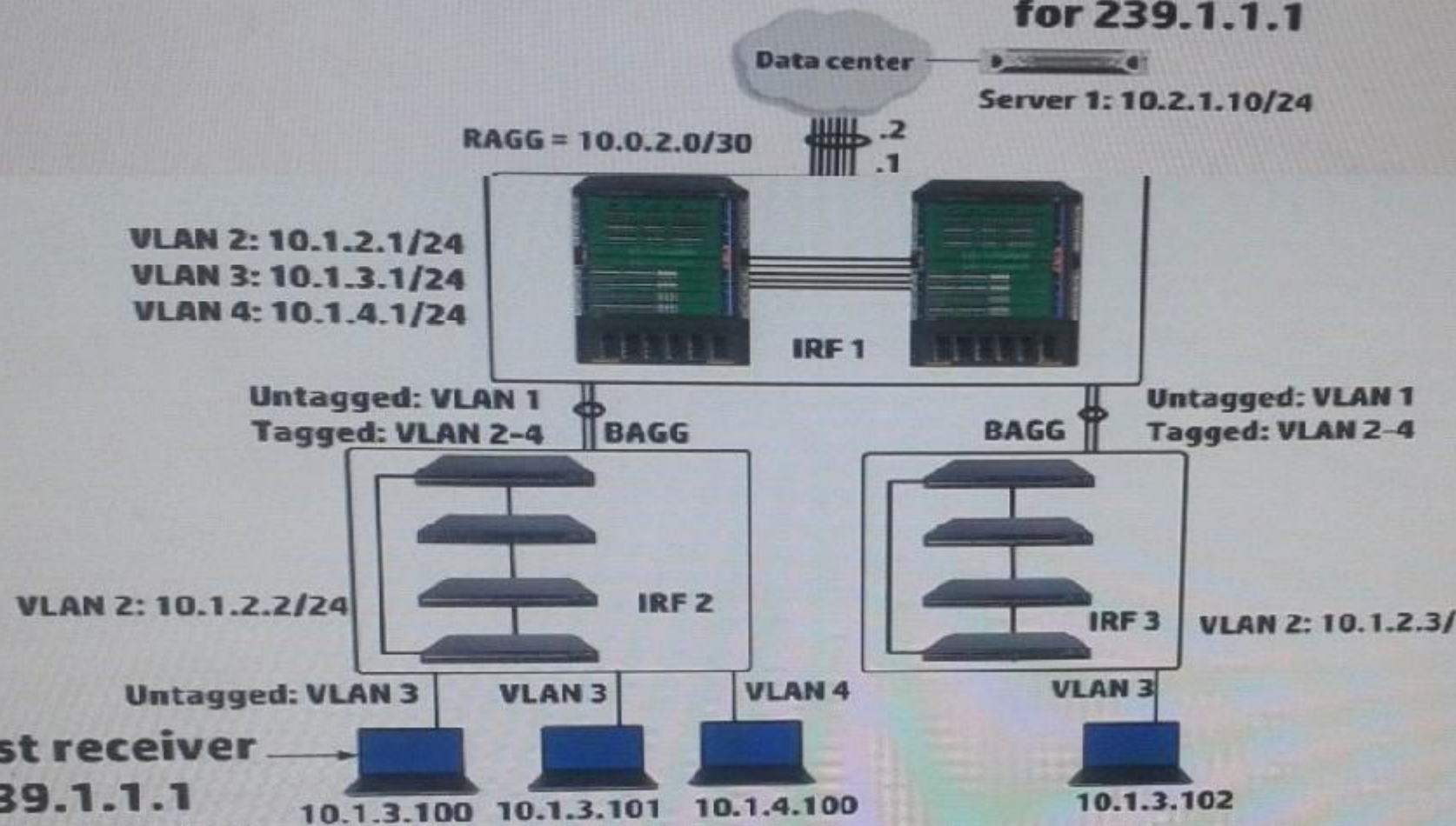
**Explanation/Reference:**

#### QUESTION 12

Refer to the exhibit.

IRF = Intelligent Resilient Framework  
RAGG = Routed link aggregation group  
BAGG = Bridged link aggregation group

**Multicast source  
for 239.1.1.1**



IRF 1, at the campus core campus core, enables Internet Group Management Protocol (IGMP) on its VLAN3 interface. IRF 1 is also part of a multicast routing solution with the data center infrastructure devices. How can a network administrator ensure that only endpoints that have registered for multicasts destined to 239.1.1.1 receive these multicasts?

- A. On every campus IRF virtual switch, set VLAN 3 as the multicast VLAN
- B. On IRF 1, enable IGMP snooping on VLAN3
- C. On each access layer IRF virtual switch, enable IGMP snooping on VLAN 3
- D. On each access layer IRF virtual switch, create a Layer 3 interface VLAN3. Enable IGMP on that interface

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

[http://www.h3c.com/portal/Technical\\_Support\\_\\_\\_Documents/Technical\\_Documents/Switches/H3C\\_S12500\\_Series\\_Switches/Configuration/Operation\\_Manual/H3C\\_S12500\\_CG-Release7128-6W710/07/201301/772657\\_1285\\_0.htm](http://www.h3c.com/portal/Technical_Support___Documents/Technical_Documents/Switches/H3C_S12500_Series_Switches/Configuration/Operation_Manual/H3C_S12500_CG-Release7128-6W710/07/201301/772657_1285_0.htm)

### QUESTION 13

Four HP 3800 Series Switches have formed a backplane stack in a ring topology. Member 1 is the commander the two stacking links on the member 1 fail. What happens?

- A. If LACP Multi-Active Detection (MAD) is enabled and the stack connects to a ProVision switch on a link aggregation, member 2, 3 and 4 and shutdown the ports Otherwise, no ports are disabled
- B. If LACP Multi-Active Detection (MAD) is enabled member 1 shuts down all of its ports. Otherwise, no ports are disabled
- C. If the split policy is one-fragment-up member 1 shuts down all of its ports
- D. If the switch policy is one-fragment-up members 2, 3, and 4 shut down all of their ports

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Results of Disconnecting a Stacking Cable

If a stacking cable becomes disconnected from one of the switches in the stack, the effect depends on the stacking topology that is being used:

Mesh--The stack topology is temporarily changed to a ring. To recover, simply reconnect the stacking cable; the mesh topology and the previous stack configuration is restored.

Ring--There is little effect. The stack topology is temporarily changed to a chain topology. To recover, simply reconnect the stacking cable; the ring topology and the previous stack configuration is restored.

Chain--The following occurs:

- The smaller section (fragment) of the stack that results from the disconnection becomes Inactive (the Stack Status value shown in the output of the show stacking command is Inactive).
- If the two resulting fragments are the same size, the fragment that contains the Commander will be Active, and the other fragment becomes Inactive.
- Both fragments will have a Commander and a Standby selected (if there is more than one switch in each fragment).



· When the stacking cable is reconnected to reform the chain:

The Commander and Standby of the Active fragment retain those roles for the resulting stack. If the original Commander was not in that fragment, then the stack will have a new Commander when the stack is reformed. The switches in the Inactive fragment reboot and assume their new roles in the reformed chain.

Stack fragment - A stack that previously had more members (that is, some of its previous members are now missing). The fragment can be Active or Inactive based on the rules described.

· Active Stack fragment - When a stack becomes fragmented, only one fragment remains Active; the other fragments become Inactive (all network ports are disabled). The active stack fragment inherits the MAC address and IP addressing of the stack for management. The fragment that has more switches in it will be the Active fragment. This allows more of the network ports to remain operational. If the fragments have the same number of switches in them, then the fragment that has the original Commander will be the Active fragment. · Inactive Stack fragment - The switches in this fragment do not actively switch packets. They are powered on, however, the network ceases to carry traffic. All user ports are disabled. Only the OOBM and stack ports remain active.

[http://h20565.www2.hp.com/hpsc/doc/public/display?docId=emr\\_na-c03018186](http://h20565.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c03018186)

#### QUESTION 14

Refer to the exhibit.

```
HP Stack 3800#: show stacking
Stack ID : 00031cc1-de4d48c0
MAC Address : 1cc1de-4d48c9
Stack Topology : Mesh
Stack Status : Active
Uptime : 1d 2h 35m
Software Version : KA.15.05
Mbr
```

ID	Mac Address	Model	Pri	Status
1	1cc1de-4d48c0	HP J9574A 3800-48G-PoE+-4SFP+ Switch	250	Command
2	1cc1de-4d8680	HP J9573A 3800-24G-PoE+-2SFP+ Switch	128	Standby
3	1cc1de-4e3180	HP J9574A 3800-48G-PoE+-4SFP+ Switch	240	Member
4	1cc1de-4d1820	HP J9576A 3800-24G-PoE+-2SFP+ Switch	128	Member

The HP 3800 switch with member ID 1 shown in the exhibit goes down. What happens?

- A. Switch 2 becomes the commander
- B. Switch 2 becomes the commander
- C. Switch 4 becomes the commander

D. The switch that has the longest uptime becomes master

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

When a Switch Crashes and Reboots

Commander - The standby takes over as the new Commander

- A new standby is elected
- Crashing switch writes core file to local stable storage
- Crashing switch reboots and join stack
- Core file and crash information for this switch is available from Commander Standby - A new standby is elected
- Crashing switch writes core file to local stable storage
- Crashing switch reboots and joins the stack
- Core file and crash information for this switch is available from the Commander Member - Crashing switch writes core file to local stable storage
- Crashing switch reboots and joins the stack
- Core file and crash information for this switch is available from the Commander

#### **QUESTION 15**

In which components of HP FlexNetwork solutions can Intelligent Resilient Framework (IRF) play a role?

- A. IRF can operate at any layer of both campus and data center solutions.
- B. IRF can operate at the access layer of both campus and data center solutions. It cannot operate at the core.
- C. IRF can operate within data center solutions but not in campus solutions.
- D. IRF can operate at the core of both campus and data center solutions. It cannot operate at the access layer.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

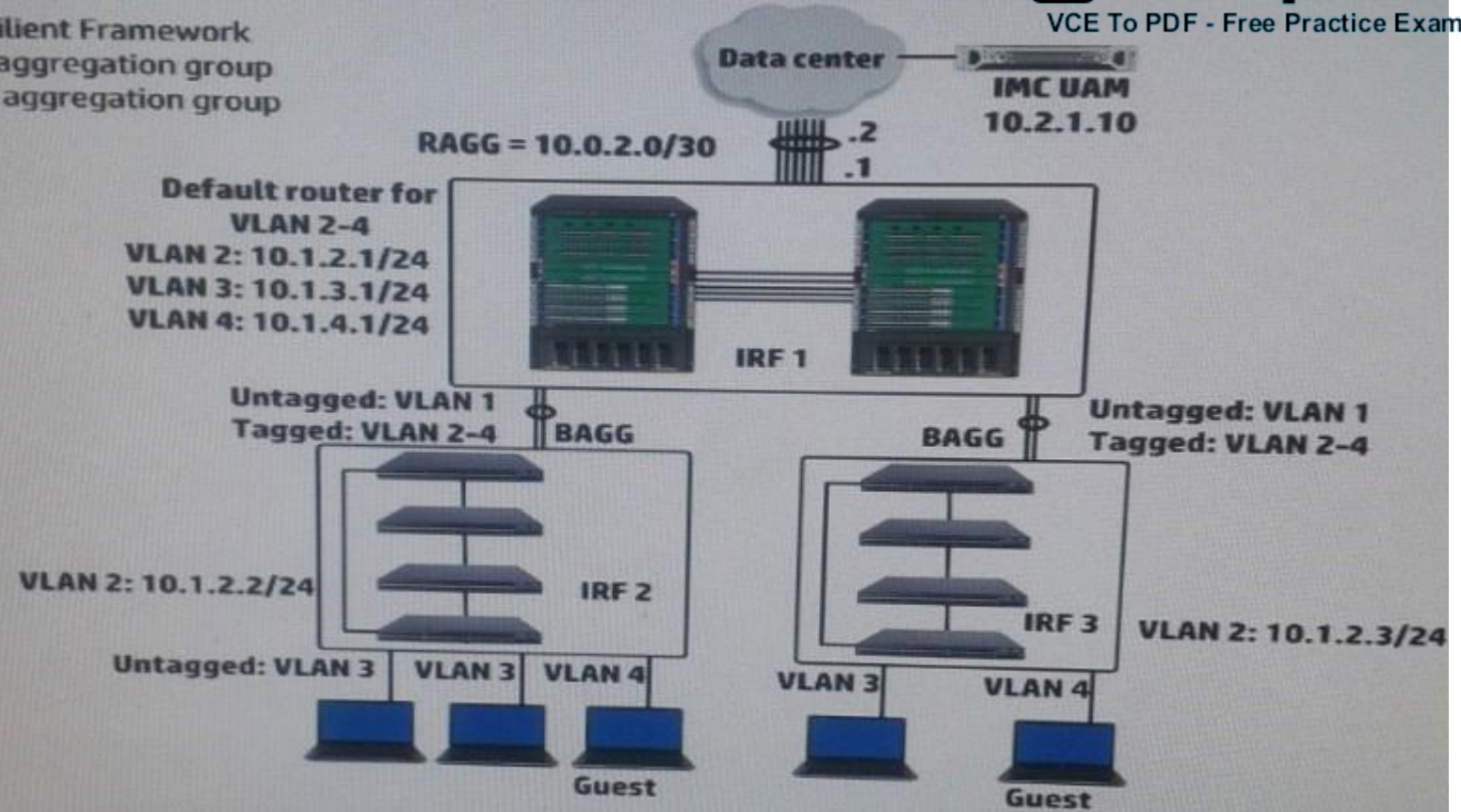
answer is modified.

#### **QUESTION 16**

Refer to the exhibit.



IRF = Intelligent Resilient Framework  
RAGG = Routed link aggregation group  
BAGG = Bridged link aggregation group



A company has a functional multicast routing solution, which routes multicasts from the data center users in VLAN3 and VLAN4. Users in VLAN 3 and VLAN 4 sometimes register for some of the same multicast. The network administrator wants to prevent duplicate multicasts on the link between the core IRF virtual switch and the access layer IRF virtual switches.

What should the administrator do to accomplish this goal?

- A. Enable IGMP snooping on VLAN 3 and VLAN4 (Layer 2) on the core switch and on the access layer switches.
- B. Create Layer 3 interfaces for VLAN 3 and VLAN 4 on the access layer switches, and enable IGMP on the interfaces.
- C. Enable Multicast VLAN and IGMP snooping on VLAN 3 on the access layer switches, and associate VLAN 4 as a sub-VLAN.
- D. Create Layer 3 interfaces for VLAN 3 and VLAN 4 on the access layer switches, and enable PIM on the interfaces.

**Correct Answer: A**

**Section: (none)**  
**Explanation**

**Explanation/Reference:**

**QUESTION 17**

An HP switch is a member of an Intelligent Resilient Framework (IRF) virtual device that has two members. What is a proper situation for issuing the mad restore command on this switch?

- A. The IRF link has failed, and MAD has caused a new member to become master. The administrator wants to restore the previous master's MAC address.
- B. The IRF link has failed, and MAD placed this member in recovery mode. The administrator wants the switch to automatically repair the failed link.
- C. The IRF link has failed, and the administrator needs to put this switch in MAD recovery mode.
- D. The IRF link has failed, and MAD placed this member in recovery mode. The active member has gone offline.

**Correct Answer: B**  
**Section: (none)**  
**Explanation**

**Explanation/Reference:**

<http://www.manualslib.com/manual/579819/Hp-6125xlg.html?page=27>

Restore the normal MAD state of the IRF fabric in Recovery state.

Use mad restore to restore the normal MAD state of the IRF fabric in Recovery state. When MAD detects that an IRF fabric has split into multiple IRF fabrics, only the one whose master has the lowest member ID among all the masters can still forward traffic. All the other fabrics are set in Recovery state and cannot forward traffic.

**QUESTION 18**

Refer to the exhibit.

```
display version comp-matrix file version2.bin
Number of Matrices in Table = 1
Matrix for HP 10504

Running version: 1104

Version Compatibility List:
1105 (Compatible)
chassis 0 slot 2: Hotfix
chassis 0 slot 3: Reboot
chassis 1 slot 2: Hotfix
chassis 1 slot 3: Reboot
```

The current software on the Intelligent Resilient Framework (IRF) virtual device shown in the exhibit is version 1104. The network administrator wants to upgrade to software version 1105.

What will happen when the administrator attempts to use In-Service Software Upgrade (ISSU) for this upgrade?

- A. The IRF virtual device will not accept the ISSU commands. It will output various error messages.
- B. When the administrator executes the switch over to the new master, a rollback will occur, causing the software to revert to the previous version.
- C. The process can complete successfully. Some links might go down, causing temporary failovers within link aggregation groups.
- D. When the administrator executes the switchover to the new master, an outage will occur while this master reboots.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

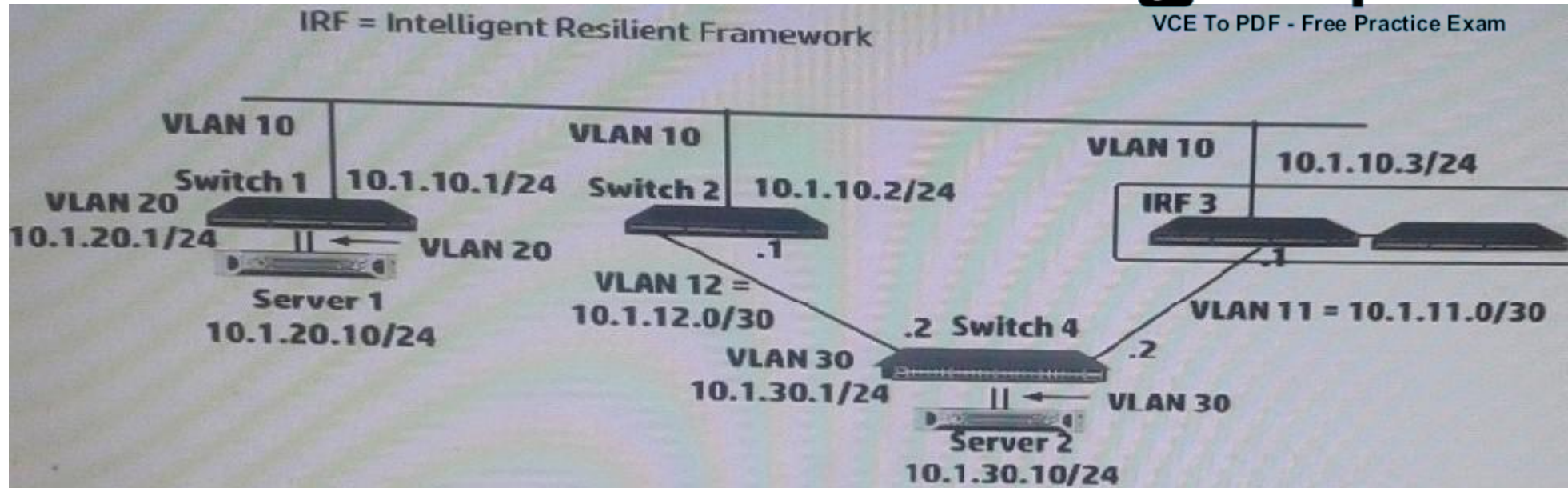
Explanation:

<http://aboutnetworking.com/2014/03/24/comware5-issu-incompatible/>

<http://aboutnetworking.com/2014/03/24/comware5-issu-compatible/>

#### **QUESTION 19**

Refer to the exhibit.



IRF 3 and Switches 1, 2 and 4 are successfully implementing OSPF on the interfaces shown in the exhibit. Then IRF 3's 10.1.10.24 link fails. Connectivity between Server 1 and Server 2 is disrupted for about 30 seconds.

What can the network administrator do to prevent this issue from occurring again?

- A. Enable opaque LSAs on each of the switches; set the OSPF graceful restart mode to IETF mode on at least IRF 3.
- B. Set the OSPF dead timer on each of the switches to equal the hello timer
- C. Set up OSPF Bidirectional Forwarding Detection (BFD) on each switch VLAN 10 interface.
- D. On IRF 3, set up Bidirectional Forwarding Detection (BFD) Multi-Active Detection (MAD) on a dedicated link between the members.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 20

Refer to the exhibit.

Exhibit 1

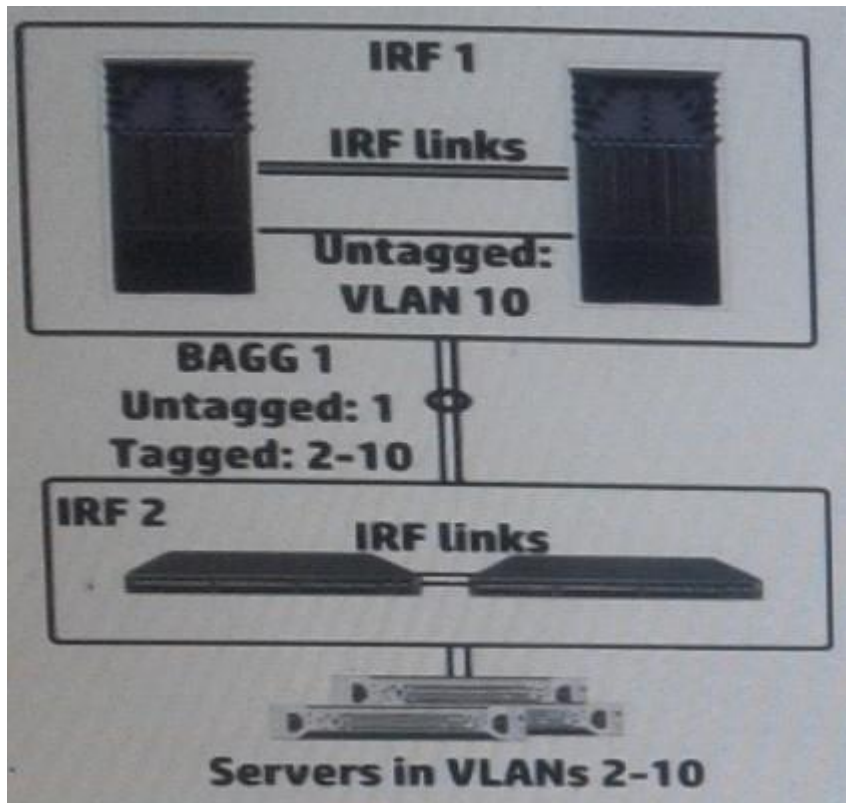


Exhibit 2



```
<IRF-1> display irf
Switch Role    Priority  CPU-Mac      Description
*+1   Master   32    00e0-fc0a-15e0  --
  2   Slave    1    00e0-fc0f-8c02  --

-----
* indicates the device is the master.
+ indicates the device through which the user logs in.
The Bridge MAC of the IRF is: 000f-e26a-58ed
Auto upgrade           : no
Mac persistent          : always
Domain ID               : 1

<IRF-1> display mad
MAD LACP enabled.
MAD BFD disabled.
MAD ARP disabled.

<IRF-1> display current-config | begin bridge-aggregation1
interface bridge-aggregation1
 link-aggregation mode dynamic
 mad enable
 port link-type trunk
 port trunk permit vlan 1 to 10

<IRF-2> display mad
MAD LACP enabled.
MAD BFD disabled.
MAD ARP disabled.

<IRF-2> display current-config | begin bridge-aggregation1
interface bridge-aggregation1
 link-aggregation mode dynamic
 mad enable
 port link-type trunk
 port trunk permit vlan 1 to 10
```

The HP Intelligent Resilient Framework (IRF) virtual devices shown in the Exhibit 1 support traffic for servers in VLAN 2-10. To enhance resiliency, the network administrator configures MAD on both IRF virtual switches. The administrator has established the settings shown in the exhibit 2. The configuration has an issue.

How can the administrator correct the issue?

- A. Activate the Bidirectional Forwarding Detection (BFD) MAD 1 on IRF 1 and IRF 2.
- B. Exclude the ports in BAGG 1 from MAD on IRF 1 and IRF 2.
- C. Change the domain ID on IRF 2 to a unique ID.
- D. Enable extended Link Layer Control Protocol Data Units (LACPDUs) on IRF 1 and IRF 2.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

NOT ALL IMAGE CHECK for EXAMPLE THIS example there are BFD MAD

<http://www.certificationexplorer.com/Documents/HP0-Y47.pdf>

<http://aboutpnetworking.com/2014/02/01/comware7-irf-mad-lacp-new-selection-method/> <http://aboutpnetworking.com/2014/11/08/provision-support-for-irf-mad-lacp-split-brain-detection/> [http://h20565.www2.hp.com/hpsc/doc/public/display?docId=emr\\_na-c02648772](http://h20565.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c02648772)

#### **QUESTION 21**

A company has a network with HP Provision switches. The network administrator is establishing remote mirroring session between two of the switches. The remote does not use the truncation option.

What must the administrator check on any switches between the mirror source and destination?

- A. The remote probe VLAN defined for the remote mirroring session extends across the switches.
- B. All switches transmit the remote mirroring traffic as untagged traffic.
- C. All switches transmit the remote mirroring traffic on single links, rather than link aggregations (or trunks).
- D. The VLANs that carry the remote mirroring traffic support jumbo frames.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

[http://h20565.www2.hp.com/hpsc/doc/public/display?sp4ts.oid=82374&docId=emr\\_na-c02587751&docLocale=en\\_US](http://h20565.www2.hp.com/hpsc/doc/public/display?sp4ts.oid=82374&docId=emr_na-c02587751&docLocale=en_US)

#### **QUESTION 22**

Refer to the exhibit.

Exhibit 1

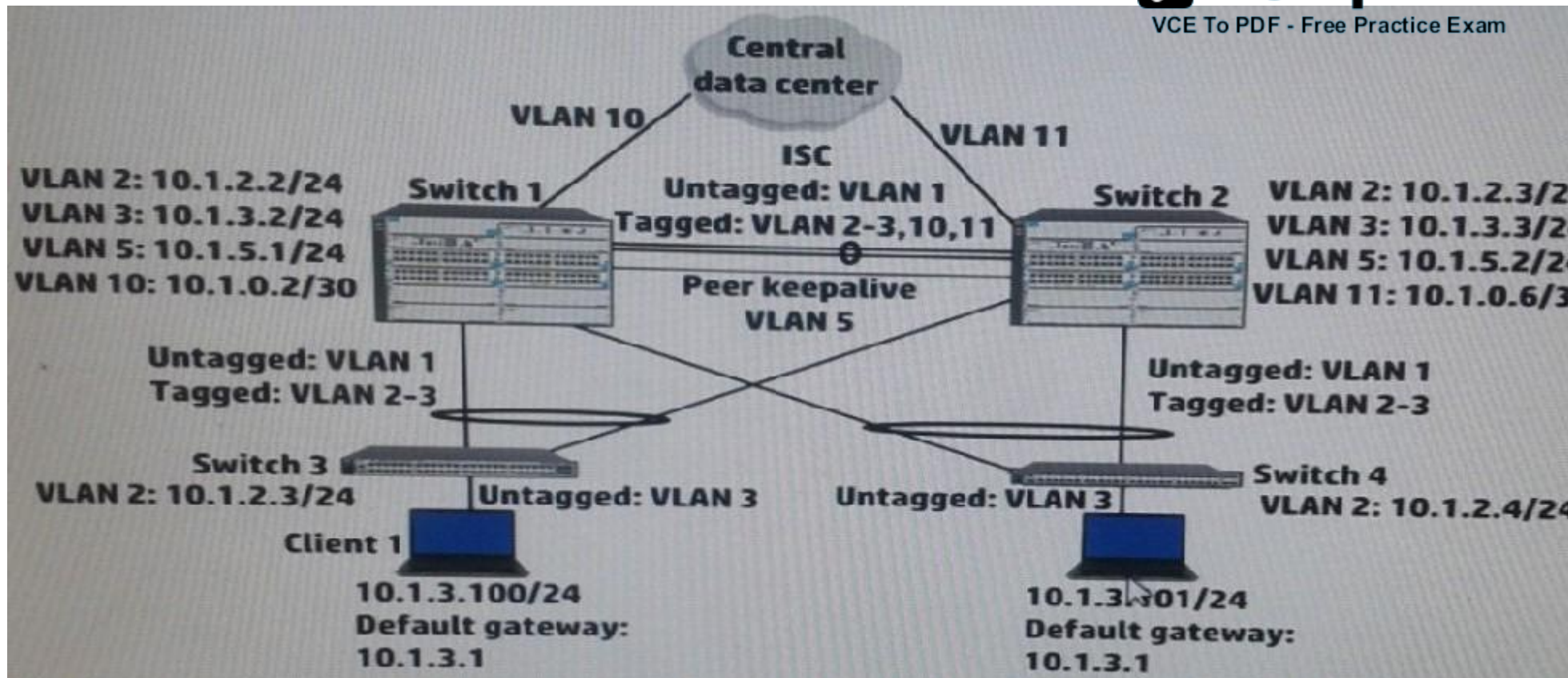


Exhibit 2

```
Switch1# show vrrp vlan 3
VRRP Virtual Router Statistics Information
```

```

Vlan ID          : 3
Virtual Router ID : 1
State            : Backup
Up Time          : 30 minutes
Virtual MAC Address : 00005e-000101
Master's IP Address : 10.1.3.3
Associated IP Addr Count : 1
Advertise Pkts RX : 451
Zero Priority RX   : 0
Bad Length Pkts   : 0
Mismatched Interval Pkts : 0
Mismatched IP TTL Pkts : 0
Near Failovers    :
Become Master     :
Zero Priority Tx   :
Bad Type Pkts     :
Mismatched Addr List Pkts :
Mismatched Auth Type Pkts :
```

Client 1 is transmitting traffic to the data center. Switch 3 transmits the traffic on the link to Switch 1. How does Switch 1 handle the traffic received from Client 1?

- A. It forwards the traffic over the ISC to Switch 2.
- B. It routes the traffic and forwards it towards the data center.
- C. It drops the traffic.
- D. It forwards the traffic over the keepalive link to Switch 2.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

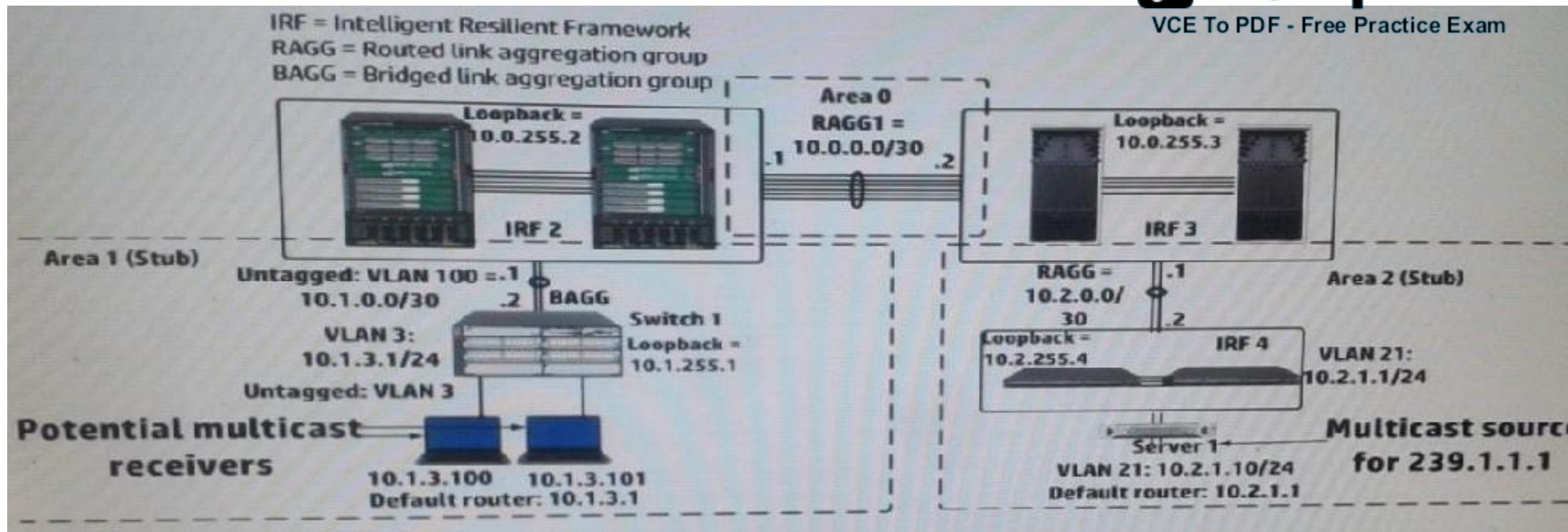
It see that destination MAC address is accessible

#### QUESTION 23

Refer to the exhibit.

.





A network administrator has begun configuring a Protocol Independent Multicast Sparse Mode (PIM-SM) solution on all of the network infrastructure devices shown in the exhibit. The administrator has selected the static method for configuring rendezvous (RPs) and wants to use 4 as RP.

Where must the administrator configure the static RP setting?

- A. On IRF 3 and IRF 4 only
- B. On switch 1, IRF 2, IRF 3, and IRF 4
- C. On IRF 2, IRF 3, and IRF 4 only
- D. On IRF 2 and IRF 3 only

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

<http://mrnciew.com/2013/01/19/pim-sm-static-rp-configurations/>

In Static-RP configuration, you need to configure "ip pim rp-address x.x.x.x" command on every multicast enable router in your network including RP itself. In this example we will make CME as RP in this network.



**QUESTION 24**

A company is implementing 802.1X authentication. These are the requirements:

Employees who pass 802.1X authentication should be placed VLAN 3.

Guests and employees who cannot authenticate, or fail authentication, should be placed in VLAN4. Different users might connect to port at different times, but only one device will connect to the port at the same time.

802.1X is enabled Globally on the switch (aaa port-access authenticator)

Which settings correctly configure the HP ProVision edge ports?

- A. `vlan 3`  
    `untagged 1-20`  
`vlan 4`  
    `tagged 1-20`  
    `aaa port-access authenticator 1-20`
- B. `vlan 3`  
    `vlan 4`  
        `untagged 1-20`  
    `aaa port-access authenticator 1-20`  
    `aaa port-access authenticator 1-20 unauth-vid 4`
- C. `vlan 3`  
    `untagged 1 - 20`  
    `vlan 4`  
        `aaa port-access authenticator 1-20`  
        `aaa port-access authenticator 1-20 unauth-vid 4`
- D. `vlan 3`  
    `tagged 1-20`  
    `vlan 4`  
        `untagged 1-20`  
        `aaa port-access authenticator 1-20`  
        `aaa port-access authenticator 1-20 max-requests 2`  
        `aaa port-access authenticator 1-20 auth-vid 3`

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Correct Answer:** D

**Section:** (none)

**Explanation**

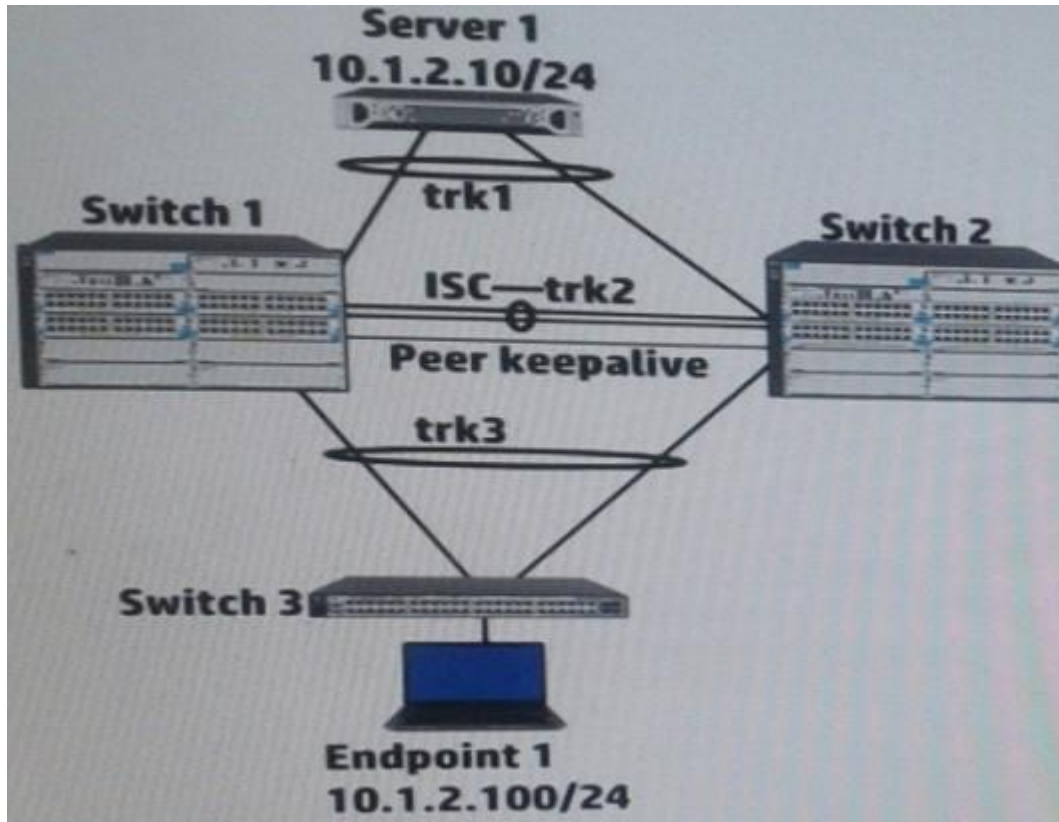
**Explanation/Reference:**

Explanation:

[ftp://ftp.hp.com/pub/networking/software/Security-Oct2005-59906024-Chap08-PortAccess\(8021x\).pdf](ftp://ftp.hp.com/pub/networking/software/Security-Oct2005-59906024-Chap08-PortAccess(8021x).pdf) Sets the period during which the port does not try to acquire a supplicant. The period begins after the last attempt authorized by the max-requests parameter fails (next page). (Default: 60 seconds)

**QUESTION 25**

Refer to the exhibit.



Switch 1 and Switch 2 have established an Interswitch Connection (ISC) and two distributed trunks. All of the switches have Multiple Spanning tree Protocol (MSTP) enabled. Where does Switch 1 transmit or process Bridge Protocol Data Units (BPDUs)?

- A. On trk2 and the peer keepalive
- B. On trk1 and trk3
- C. On trk1, trk2, trk3
- D. On trk2

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

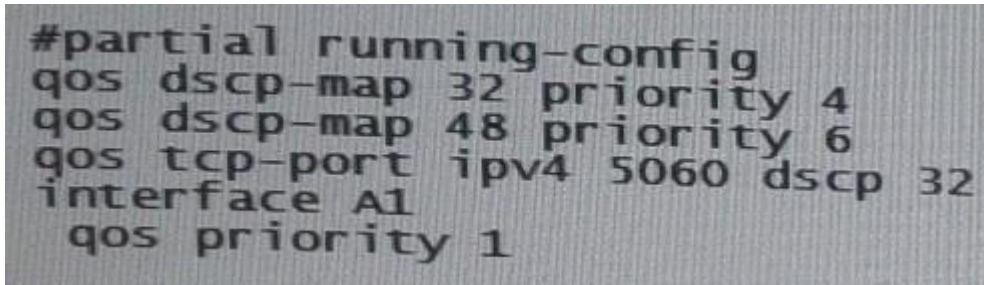
Explanation:



[http://h20628.www2.hp.com/km-ext/kmcsdirect/emr\\_na-c03015912-2.pdf](http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c03015912-2.pdf)

**QUESTION 26**

Refer to the exhibit.



```
#partial running-config
qos dscp-map 32 priority 4
qos dscp-map 48 priority 6
qos tcp-port ipv4 5060 dscp 32
interface A1
  qos priority 1
```

A network administrator is checking the Quality of Service (QoS) settings on an HP ProVision Switch.

This frame arrives on the switch:

Ingress port: A1

No 802.1Q tag

Source IP address = 10.1.2.10

Destination IP address = 10.1.4.4

DSCP = 48

Destination TCP port = 5060

To which priority queue will the switch assign this frame? (Queues are numbered 0-7)

- A. 0
- B. 1
- C. 4
- D. 6

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

If more than one global classification criteria, they are searched in the following order:

TCP / UDP port number

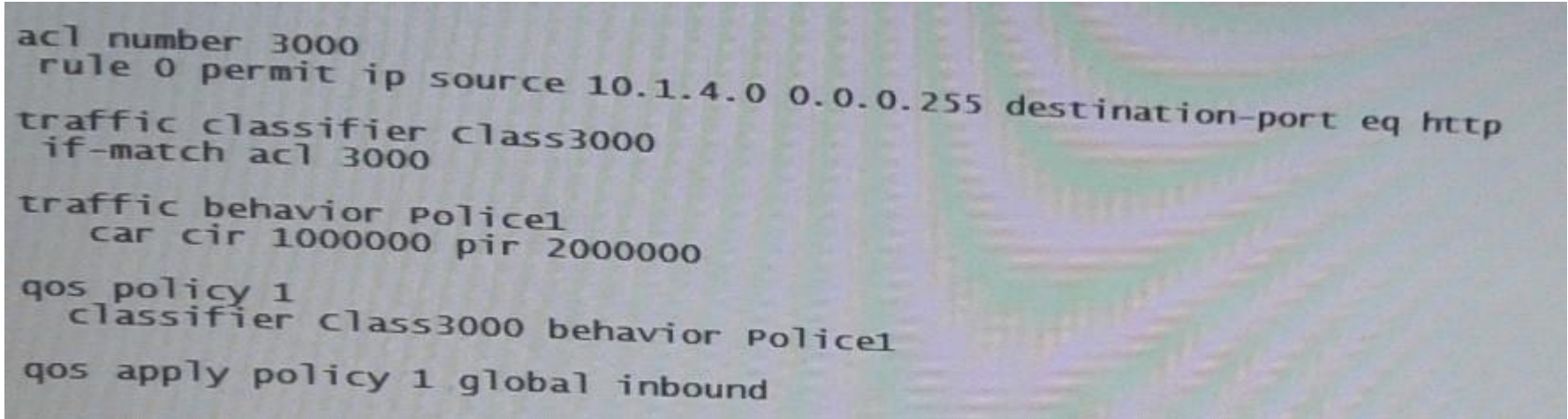
IP-address of the sender and receiver

IP precedence value

DSCP value  
Minutes of the third level  
VLAN number  
Incoming port switch  
Markings on the data link layer 802.1p  
When a packet is matched by several criteria, the marking is applied only for the first matched by the order

**QUESTION 27**

Refer to the exhibit.



```
acl number 3000
 rule 0 permit ip source 10.1.4.0 0.0.0.255 destination-port eq http
traffic classifier Class3000
 if-match acl 3000
traffic behavior Police1
 car cir 1000000 pir 2000000
qos policy 1
 classifier Class3000 behavior Police1
qos apply policy 1 global inbound
```

This HP 10500 Switch Series is receiving an average of 1 Gbps of HTTP traffic from 10.1.4.0/24. The switch starts to receive an additional 1 Gbps of HTTP traffic from 10.1.4.0/24. How does the switch handle the traffic?

- A. It drops the traffic
- B. It forwards the traffic but marks it yellow (for a higher drop precedence)
- C. It forwards the traffic without remarking it in any way
- D. It forwards the traffic but marks it for forwarding in a lower priority queue

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

## Parameters

**cir committed-information-rate:** Specifies the committed information rate (CIR) in kbps.

**cbs committed-burst-size:** Specifies the committed burst size (CBS) in bytes. The committed-burst-size argument ranges from 4000 to 16000000, the default is 4000.

**ebs excess-burst-size:** Specifies excess burst size (EBS) in bytes. The excess-burst-size argument ranges from 0 to 16000000, the default is 4000.

**pir peak-information-rate:** Specifies the peak information rate (PIR) in kbps.

**green action:** Specifies the action to be conducted for the traffic conforming to CIR. The action argument can be:

**discard:** Drops the packets.

**pass:** Forwards the packets.

**remark-dscp-pass new-dscp:** Marks the packets with a new DSCP precedence and forwards them to their destinations. The new-dscp argument is in the range 0 to 63.

By default, packets conforming to CIR are forwarded.

**red action:** Specifies the action to be conducted for the traffic conforms to neither CIR nor PIR. The action argument can be:

**discard:** Drops the packets.

**pass:** Forwards the packets.

**remark-dscp-pass new-dscp:** Marks the packets with a new DSCP precedence and forwards them to their destinations. The new-dscp argument is in the range 0 to 63.

By default, packets conforming to neither CIR nor PIR are dropped.

**yellow action:** Specifies the action to be conducted for the traffic conforms to PIR but does not conform to CIR. The action argument can be:

**discard:** Drops the packets.

**pass:** Forwards the packets.

**remark-dscp-pass new-dscp:** Marks the packets with a new DSCP precedence and forwards them to their destinations. The new-dscp argument is in the range 0 to 63.

By default, packets conforming to PIR but not conforming to CIR are forwarded.

## QUESTION 28

Refer to the exhibit.

```
interface GigabitEthernet1/0/1
  qos trust dscp

<Comware-switch> display qos map-table dscp-dot1p
#partial output

MAP-TABLE NAME: dscp-dot1p TYPE: pre-define
IMPORT : EXPORT
0 : 0
16 : 2

<Comware-switch> display qos map-table dot1p-lp
MAP-TABLE NAME: dot1p-lp TYPE: pre-define
IMPORT : EXPORT
0 : 2
1 : 0
2 : 1
3 : 3
4 : 4
5 : 5
6 : 6
7 : 7
```

A server connects to GigabitEthernet1/0/1 on an HP Comware switch. The server sends tagged traffic in VLAN2. It has an application that sets the DiffServ Code Point (DSCP) for its traffic to 16 and the 802.1p value to 2. The switch should use the DSCP to place the traffic in priority queue. The traffic belongs to the queue that is one priority level higher than the queue for best effort traffic (traffic without a QoS value)

What can the network administrator do to meet this requirement?

- A. Change GigabitEthernet1/0/1's trust setting to "dot1p" set the port priority to 3. DSCP will not be used
- B. Keep Gigabit Ethernet1/0/1's QoS trust setting to "dot1p" Set the port priority to 3.
- C. Change the dot1p-lp map to map 802.1p value 2 to lp 2 and 802.1p value 0 to lp1.
- D. Change the dscp-dot1p map to map DSCP 16 to 802.1p value 1. RECEIVE priority 0

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 29**

Refer to the exhibits.

Exhibit 1

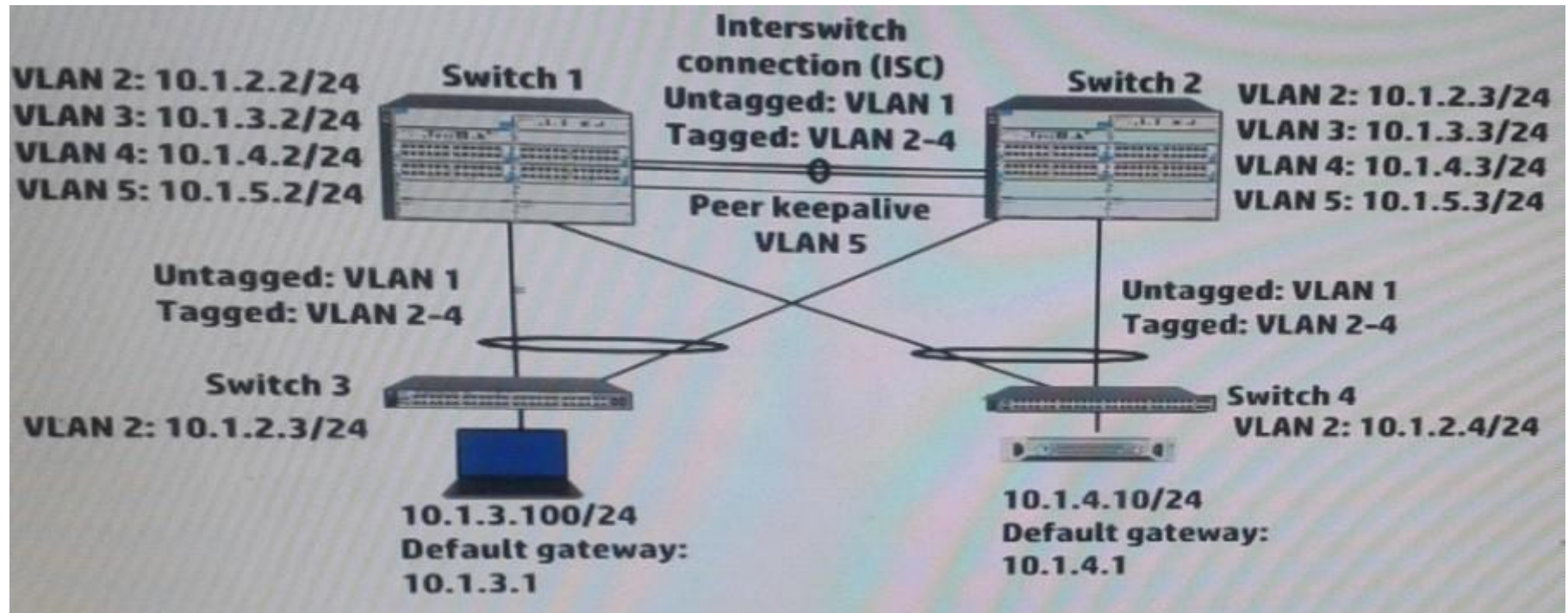


Exhibit 2

```
Switch1# show vrrp config
VRRP Global Configuration Information
VRRP Enabled : Yes
Traps Enabled : Yes
Virtual Routers Respond To Ping Requests : Yes
VRRP Nonstop Enabled : No

VRRP Virtual Router Configuration Information

VLAN ID : 3
Virtual Router ID : 1

Administrative Status [Disabled] : Enabled
Mode [Uninitialized] : Backup
Priority [100] : 254
Advertisement Interval [1] : 1
Preempt Mode [True] : True
Preempt Delay Time [0] : 120
Respond To virtual IP Ping Requests [Yes] : Yes
Primary IP Address : Lowest

IP Address      Subnet Mask
-----
10.1.3.1        255.255.255.0
```

```
Switch1# show vrrp vlan 3
VRRP Virtual Router Statistics Information

Vlan ID           : 3
Virtual Router ID : 1
State             : Master
Up Time           : 50 min
Virtual MAC Address : 00005e-000101
Master's IP Address : 10.1.3.2
Associated IP Addr Count : 1
Advertise Pkts Rx   : 0
Zero Priority Rx     : 0
Bad Length Pkts     : 0
Mismatched Interval Pkts : 0
Mismatched IP TTL Pkts : 0
Near Failovers      : 0
Become Master       : 5
Zero Priority Tx     : 3
Bad Type Pkts       : 0
Mismatched Addr List Pkts : 0
Mismatched Auth Type Pkts : 0
```

Exhibit 2 shows the Virtual Router Redundancy Protocol (VRRP) configuration and status for VLAN 3 on switch 1 during normal operation, when both Switch 1 and Switch 2 are up. Switch 1 then experiences a power failure. After a few minutes, power is restored, and the switch comes back up.



What happens to VRRP operations in VLAN 3?

- A. Switch 1 becomes Master two minutes after its VRRP processes up.
- B. Switch 2 remains Master Switch 1 receives an error and stops participating in VRRP
- C. Switch 2 remains Master, and Switch 1 becomes a Backup router.
- D. Switch 1 becomes Master as soon as its VRRP processes come up.

**Correct Answer: C**

**Section: (none)**

**Explanation**

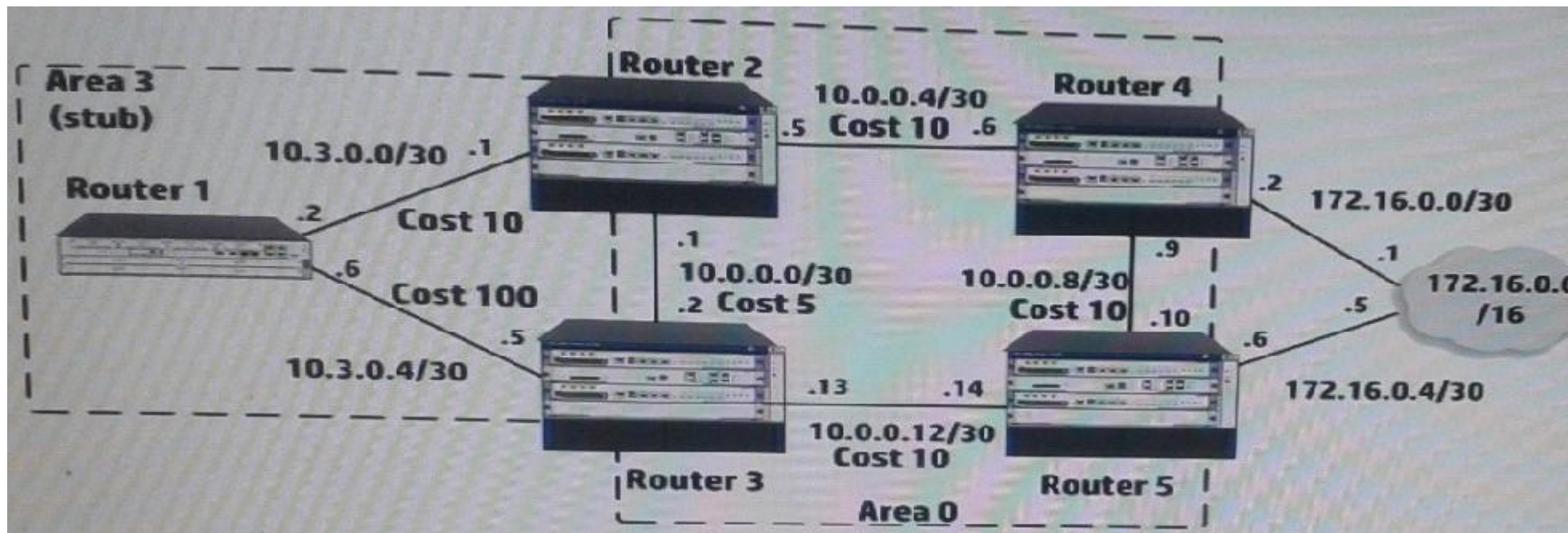
**Explanation/Reference:**

Explanation:

I think Switch2 has priority 255, because Switch2(10.1.3.2) - Master is up during 50 min, preempt is on in VRRP So Switch1 when comes online after 120min and trying to preempt still be Backup Router

### QUESTION 30

Refer to the exhibit.



Router 4, which is an HP Comware router, redistributes Routing Information Protocol (RIP) routes into Open Shortest Path First (OSPF) process 1. Router 4 has several dozen IP routes, and the network administrator wants to minimize the number of external routes throughout the entire OSPF AS. How can the administrator meet this requirement?

- A. Create an ABR summary for the RIP routes on Router 2 and Router 3.
- B. On all OSPF devices, configure all OSPF areas, including area 0, as stub areas.
- C. On all OSPF devices in area 0, set area 0 as a not-so-stubby-area (NSSA)
- D. Create an ASBR summary for the RIP routes on Router 4.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

asbr-summary command to configure a summary route.

Use the

Use the undo asbr-summary command to remove a summary route.

No ASBR route summarization is configured by default.

asbr-summary command configured, an ASBR summarizes redistributed routes that fall into the specified address With the range into a single route. If the ASBR resides in an NSSA area, it advertises the summary route in a Type-7 LSA into the area.

### **QUESTION 31**

Match each characteristic to the connect multicast routing protocol. If both protocols exhibit characteristic, you must select both.

**Hot Area:**



Require Internet Group Management Protocol (IGMP) to learn which interfaces have endpoints that need multicasts

PIM-SM only

PIM-DM only

Both PIM-SM and PIM-DM

Requires network administrator to configure at least one rendezvous (RP)

PIM-SM only

PIM-DM only

Both PIM-SM and PIM-DM

Uses a unicast routing table to determine whether incoming multicasts are arriving on the correct upstream interface

PIM-SM only

PIM-DM only

Both PIM-SM and PIM-DM

**Correct Answer:**

Require Internet Group Management Protocol (IGMP) to learn which interfaces have endpoints that need multicasts

PIM-SM only

PIM-DM only

Both PIM-SM and PIM-DM

Requires network administrator to configure at least one rendezvous (RP)

PIM-SM only

PIM-DM only

Both PIM-SM and PIM-DM

Uses a unicast routing table to determine whether incoming multicasts are arriving on the correct upstream interface

PIM-SM only

PIM-DM only

Both PIM-SM and PIM-DM

Section: (none)

Explanation

Explanation/Reference:

### QUESTION 32

Match the Comware quality of service (QoS) scheduling mechanism to its use case.

Hot Area:

Ensures that traffic in a higher priority queue is always forwarded before traffic in a lower priority queue; lower priority traffic might be starved out.

Gives more forwarding opportunities to higher priority queues. Higher priority queues receive more bandwidth, but queues with large packets might receive more bandwidth than queues with small packets.

Guarantees a specific bandwidth to traffic flows in each priority queue; divide any remaining bandwidth among queue: based on relative priority.

Correct Answer:

Strict priority (SP)

Weighted Fair Queuing (WFQ)

Weighted Round Robin (WRR) weight-based setting

Strict priority (SP)

Weighted Fair Queuing (WFQ)

Weighted Round Robin (WRR) weight-based setting

Strict priority (SP)

Weighted Fair Queuing (WFQ)

Weighted Round Robin (WRR) weight-based setting

Ensures that traffic in a higher priority queue is always forwarded before traffic in a lower priority queue; lower priority traffic might be starved out.

Strict priority (SP)

Weighted Fair Queuing (WFQ)

Weighted Round Robin (WRR) weight-based setting

Gives more forwarding opportunities to higher priority queues. Higher priority queues receive more bandwidth, but queues with large packets might receive more bandwidth than queues with small packets.

Strict priority (SP)

Weighted Fair Queuing (WFQ)

Weighted Round Robin (WRR) weight-based setting

Guarantees a specific bandwidth to traffic flows in each priority queue; divide any remaining bandwidth among queue: based on relative priority.

Strict priority (SP)

Weighted Fair Queuing (WFQ)

Weighted Round Robin (WRR) weight-based setting

Section: (none)

Explanation

Explanation/Reference:

#### QUESTION 33

Refer to the exhibit.



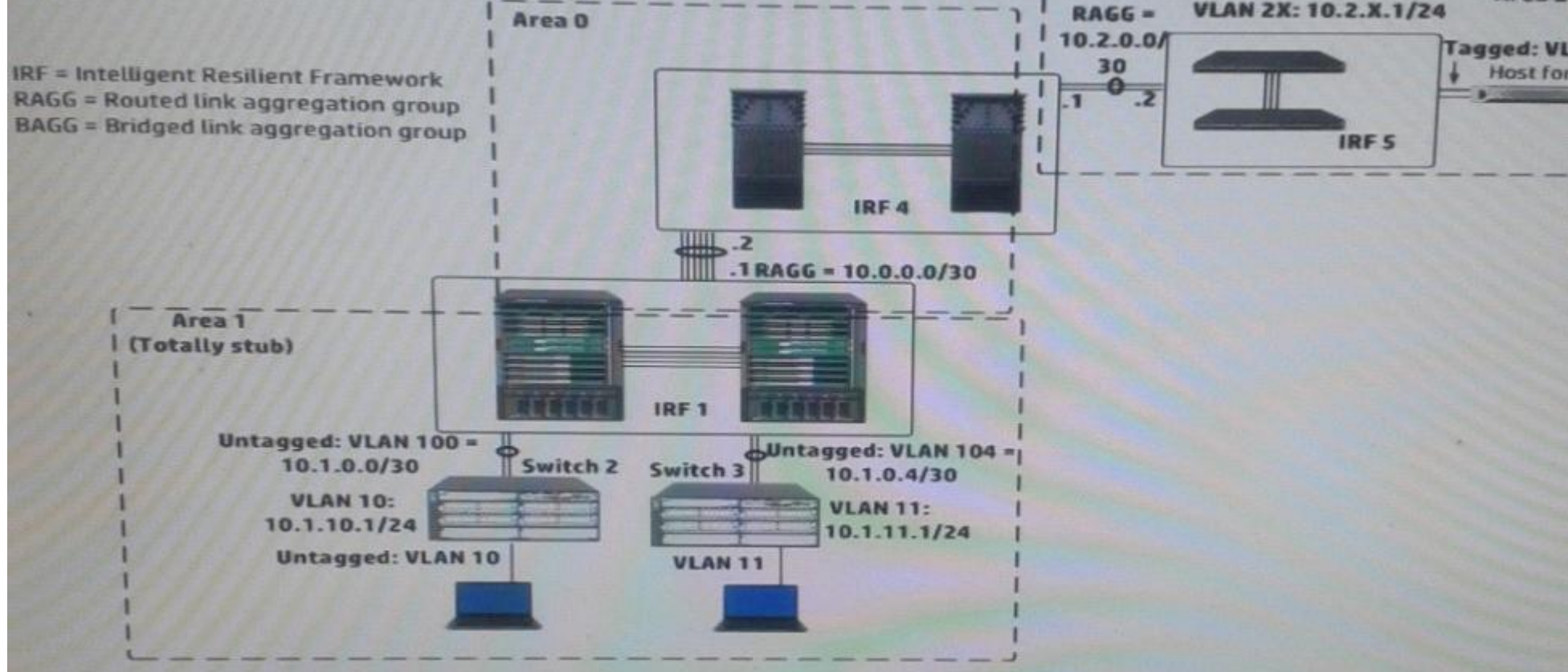


Exhibit 2

```
[IRF-1-ospf-1]display this

ospf 1
 area 0.0.0.0
  abr-summary 10.0.0.0 255.255.0.0 cost 1
  network 10.0.0.0 0.0.255.255
 area 0.0.0.1
  abr-summary 10.1.0.0 255.255.0.0 cost 1
  network 10.1.0.0 0.0.255.255
 stub no-summary
```

In exhibit 1, all infrastructure devices are implementing OSPF on the interfaces. Exhibit 1 also shows settings for OSPF areas. Exhibit 2 shows some

additional OSPF settings IRF 1.


The network administrator enters this command on IRF 4:

```
[ IRF4-ospf-1-area-0.0.0.2 ] abr-summary 10.2.0.0 16
```


The administrator verifies that the solution is functioning correctly. Indicate whether the link state database (LSDB) on a device should include an LSA for 10.2.0.0/16.

**Hot Area:**

**IRF 4 area 0 LSDB**


	
Include LSA	
Does not include LSA	

**Switch 2 area 1 LSDB**


	
Include LSA	
Does not include LSA	

**Correct Answer:**

**IRF 4 area 0 LSDB**

	
Include LSA	
Does not include LSA	

**Switch 2 area 1 LSDB**

	
Include LSA	
Does not include LSA	

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 34**

Match the HP network infrastructure product to its HP FlexNetwork component.

Hot Area:

**MultiService Router (MSR) Series**

	▼
HP FlexCampus	
HP FlexBranch	
HP FlexFabric	

**HP 5900v Switch Series**

	▼
HP FlexCampus	
HP FlexBranch	
HP FlexFabric	

**HP 10500 Switch Series**

	▼
HP FlexCampus	
HP FlexBranch	
HP FlexFabric	

**Correct Answer:**

**MultiService Router (MSR) Series**

	▼
HP FlexCampus	
HP FlexBranch	
HP FlexFabric	

**HP 5900v Switch Series**

	▼
HP FlexCampus	
HP FlexBranch	
HP FlexFabric	

**HP 10500 Switch Series**

	▼
HP FlexCampus	
HP FlexBranch	
HP FlexFabric	

**Section: (none)**

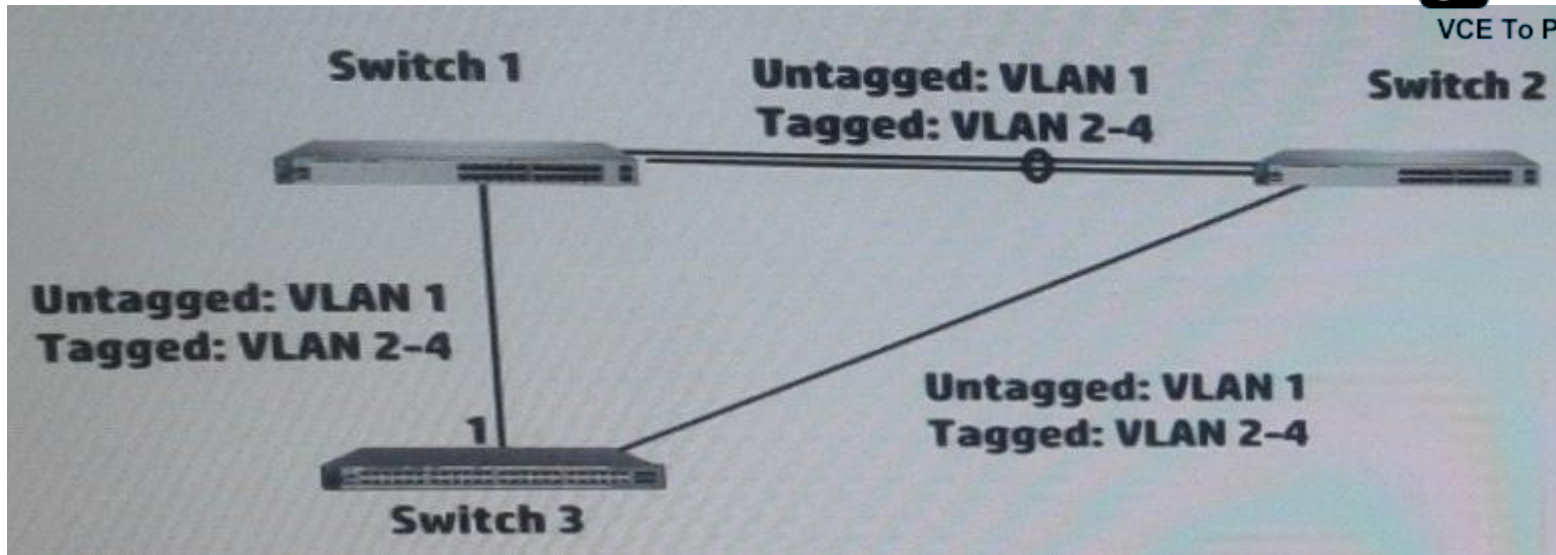
**Explanation**

**Explanation/Reference:**

**QUESTION 35**

Refer to the exhibit.







Switch 3 runs Rapid Per-VLAN Spanning Tree Plus (RPVST+), which is enabled on VLANs 1-4. Select the correct number for each of these parameters.

Hot Area:

Spanning tree instances

	
1	
2	
3	
4	

RPVST+ Bridge Protocol Data Units (BPDUs)  
transmitted on port per hello period

	
1	
2	
3	
4	

Correct Answer:

Spanning tree instances

1

2

3

4

RPVST+ Bridge Protocol Data Units (BPDUs)  
transmitted on port per hello period

1

2

3

4

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Rapid PVST+ is the IEEE 802.1w (RSTP) standard implemented per VLAN. A single instance of STP runs on each configured VLAN (if you do not manually disable STP). Each Rapid PVST+ instance on a VLAN has a single root switch. You can enable and disable STP on a per-VLAN basis when you are running Rapid PVST+.

When a switch transmits a Rapid PVST+ BPDUs frame, all switches connected to the VLAN on which the frame is transmitted receive the BPDUs. When a switch receives a BPDUs, it does not forward the frame but instead uses the information in the frame to calculate a BPDUs, and, if the topology changes, initiate a BPDUs transmission.

A BPDUs exchange results in the following:

- One switch is elected as the root bridge.
- The shortest distance to the root bridge is calculated for each switch based on the path cost.
- A designated bridge for each LAN segment is selected. This is the switch closest to the root bridge through which frames are forwarded to the root.
- A root port is selected. This is the port providing the best path from the bridge to the root bridge.
- Ports included in the spanning tree are selected.

See the "Rapid PVST+ BPDUs" section for a information about the fields that Rapid PVST+ adds to the BPDUs.

**QUESTION 36**

Match the characteristic to the routing protocol.

Hot Area:

**Is an Exterior Gateway Protocol (EGP)**

**Border Gateway Protocol (BGP)**  
**Open shortest Path First (OSPF)**

**Is an Interior Gateway Protocol (IGP)**

**Border Gateway Protocol (BGP)**  
**Open shortest Path First (OSPF)**

**Sends routing updates and hellos over a TCP session**

**Border Gateway Protocol (BGP)**  
**Open shortest Path First (OSPF)**

**Automatically discovers neighbors**

**Border Gateway Protocol (BGP)**  
**Open shortest Path First (OSPF)**



Correct Answer:

**Is an Exterior Gateway Protocol (EGP)**

▼

Border Gateway Protocol (BGP)

Open shortest Path First (OSPF)

**Is an Interior Gateway Protocol (IGP)**

▼

Border Gateway Protocol (BGP)

Open shortest Path First (OSPF)

**Sends routing updates and hellos over a TCP session**

▼

Border Gateway Protocol (BGP)

Open shortest Path First (OSPF)

**Automatically discovers neighbors**

▼

Border Gateway Protocol (BGP)

Open shortest Path First (OSPF)

Section: (none)  
Explanation

Explanation/Reference:

**QUESTION 37**

Refer to the exhibit.

```
Provision-Switch# show access-list vlan 4
Access Lists for VLAN 4

IPv6 Inbound           : (None)
IPv4 Inbound           : MyACL      Type: Extended
IPv6 Outbound          : (None)
IPv4 Outbound          : (None)
IPv6 VLAN              : (None)
IPv4 VLAN              : (None)
IPv4 Connection Rate Filter : (None)

Provision-Switch# show access-list MyACL
Access Control Lists

Name: MyACL
Type: Extended
Applied: Yes
```

SEQ	Entry			
10	Action: permit Src IP: 10.1.4.0 Dst IP: 10.2.1.10 Proto : UDP TOS : -	Mask: 0.0.0.255 Mask: 0.0.0.0	Port(s): Port(s): eq 53	Precedence: -
20	Action: permit Src IP: 10.1.4.0 Dst IP: 10.2.1.22 Proto : TCP TOS : -	Mask: 0.0.0.255 Mask: 0.0.0.0	Port(s): Port(s): eq 8080	Precedence: -
30	Action: deny Src IP: 10.1.4.0 Dst IP: 10.2.0.0 Proto : IP TOS : -	Mask: 0.0.0.255 Mask: 0.0.255.255	Port(s): Port(s):	Precedence: -
40	Action: permit Src IP: 10.1.4.0 Dst IP: 10.1.3.0 Proto : IP TOS : -	Mask: 0.0.0.255 Mask: 0.0.0.255	Port(s): Port(s):	Precedence: -

The switch with the ACL shown in the exhibit has IP address 10.1.4/24 on VLAN 4. It is the default router for 10.1.0/24. A client in VLAN 4 broadcast a DHCP discovery request, and the request arrives on this switch.

What happens?

- A. The ACL processes the packet, and the packet is permitted and then switched.
- B. The switch routes the packet out of VLAN 4 to the VLAN with the DHCP server.
- C. The ACL processes the packet, and the packet is dropped.
- D. The switch floods the broadcast in VLAN 4.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 38**

For which use case is a basic or standard access control list (ACL) appropriate?

- A. Controlling which devices can access other devices based on the MAC addresses
- B. Controlling which devices can access other devices based on the IP protocol number
- C. Controlling which devices can access other devices based on the IP addresses
- D. Controlling which devices can access other devices based on the source VLAN tag

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 39**

A network administrator is completing an In-Service Software Upgrade (ISSU) for an Intelligent Resilient Framework (IRF) virtual devices. The device has two members. Each member has one management module. Member1 is currently the master. The administrator has initiated a rollback time for this upgrade.

When should the administrator accept the upgrade?

- A. After upgrading both members of the IRF virtual device
- B. After checking the new software's ISSU compatibility but before upgrading either member
- C. After upgrading member 1 but before switching over to and upgrading member 2
- D. After upgrading and switching over to member 2 but before upgrading member 1

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation: Look here items 6-7

[http://www.h3c.com/portal/Technical\\_Support\\_\\_\\_Documents/Technical\\_Documents/Switches/H3C\\_S12500\\_Series\\_Switches/Configuration/Operation\\_Manual/H3C\\_S12500\\_CG-Release7128-6W710/01/201301/772597\\_1285\\_0.htm](http://www.h3c.com/portal/Technical_Support___Documents/Technical_Documents/Switches/H3C_S12500_Series_Switches/Configuration/Operation_Manual/H3C_S12500_CG-Release7128-6W710/01/201301/772597_1285_0.htm)



**QUESTION 40**

A company is determining whether HP IMC User Access manager (UAM) meets its needs for a RADIUS server. The company requires a solution for dynamic access control lists based on user identity and location (connected switch ID). Which statement correctly describes UAM support for this requirement?

- A. Administrator can use UAM service and access rules to apply identity-based ACLs. The location-based component is configured in individual switch CLIs.
- B. UAM can only meet these requirements if it is synchronized with Microsoft Active Directory (AD).
- C. UAM can meet these requirements if the company adds Endpoint Admission Defense (EAD) to the solution.
- D. Administrator can configure UAM service policies, scenarios, and access rules to meet these requirements.

**Correct Answer:** D

**Section:** (none)

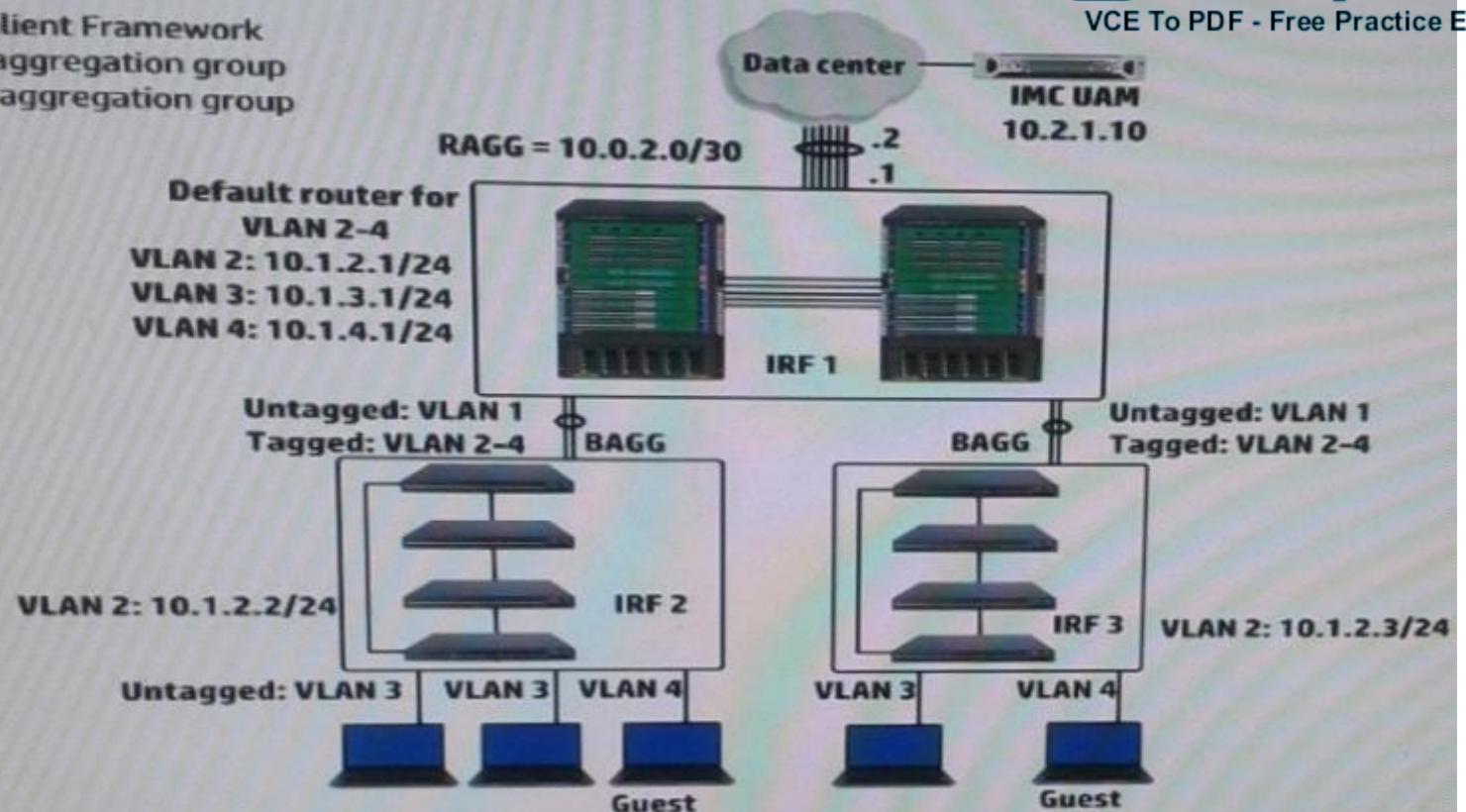
**Explanation**

**Explanation/Reference:**

**QUESTION 41**

Refer to the exhibit.

IRF = Intelligent Resilient Framework  
RAGG = Routed link aggregation group  
BAGG = Bridged link aggregation group



A company wants to implement a portal authentication solution for guests (such a solution is also called Web-Auth). Guest belong to VLAN4, as shown in the exhibit. The intelligent Management Center (IMC) User Access Manager (UAM) will provide authentication and the Web Portal.

Where should the network administrator enable portal authentication?

- A. On the VLAN 4 interface on the core IRF virtual switch
- B. On the ports with membership for VLAN 4 on the access layer IRF virtual switches
- C. On the ports with membership for VLAN 4 on the core IRF virtual switch
- D. On VLAN 4 on the core IRF virtual switch

**Correct Answer: B**

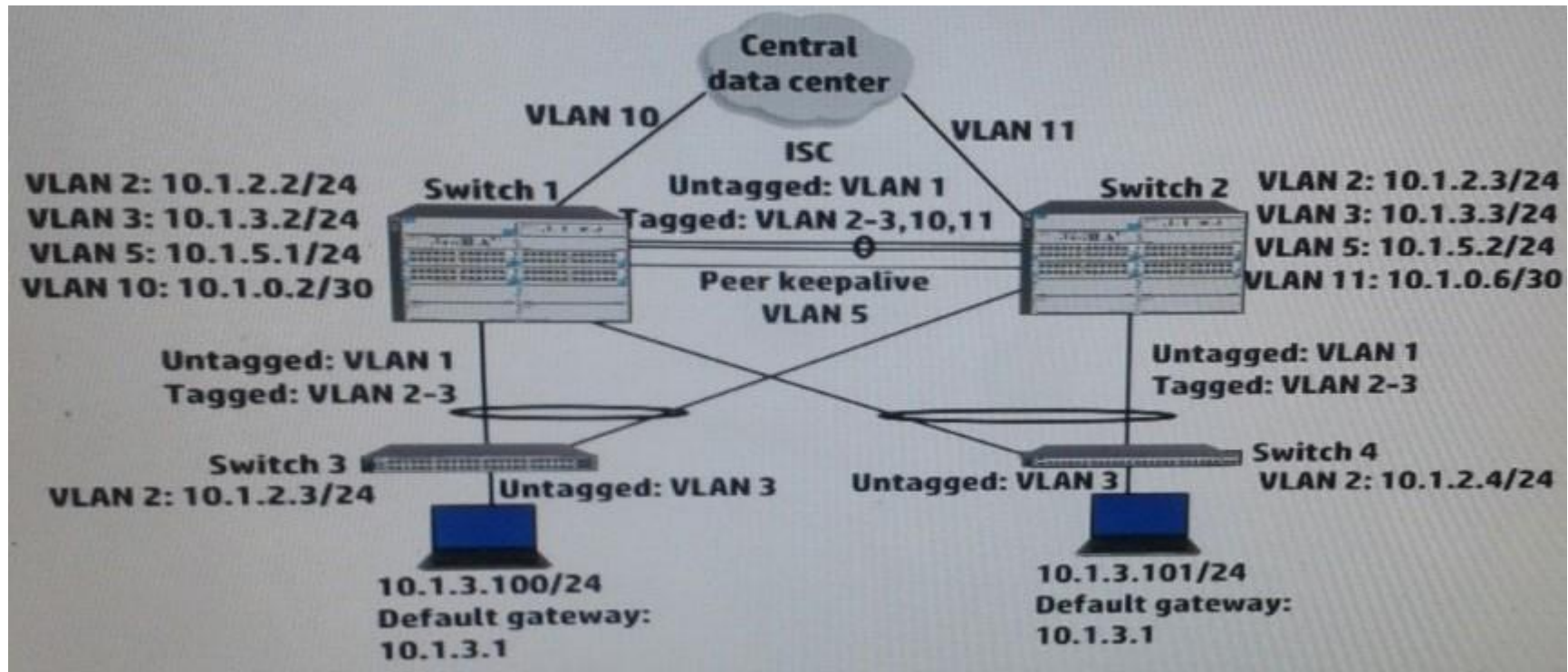
**Section: (none)**

**Explanation**

Explanation/Reference:

**QUESTION 42**

Refer to the exhibit.



Switch 1 and switch 2 run open Shortest Path First (OSPF) on all VLANs. Both switches establish an OSPF adjacency to a router at the main data center. Exhibit shows some virtual Routing Redundancy Protocol (VRRP) and OSPF settings on Switch 1 during normal operation.

How can a network administrator increase the resiliency of this solution?

- A. Implement Bidirectional Forwarding Detection (BFD) on the peer keep alive link between the core switches.
- B. Change the VLAN 10 subnet to a /24 subnet and enable VRRP on it. Place Switch 2's link to the main data center in this subnet.
- C. Make sure that, in each VRRP instance, each switch has a VRRP preempt delay of several minutes.
- D. Configure Switch 1 as an OSPF graceful restart helper in VLAN 11 and Switch 2 as a helper in VLAN 10

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 43**

A network administrator wants to configure Open Shortest Path (OSPF) MD5 authentication on VLAN 100 on an HP ProVision switch. The administrator has created a global MD5 key chain with an ID and key string that matches the neighbor's. which additional step must the administrator complete to accomplish this?

- A. Set OSPF authentication to MD5 mode in the OSPF area settings
- B. Activate MD5 key rotation globally
- C. Enable MD5 key rotation globally
- D. Assign this MD5 key to OSPF VLAN 100

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

valid and corrected.

**QUESTION 44**

Refer to the exhibit.

```
[Switch-interface GigabitEthernet1/0/1] display this
port link-mode bridge
port access vlan 2
dot1x guest-vlan 4
dot1x auth-fail vlan 3
dot1x port-method portbased
dot1x

#Global dot1x settings:
dot1x
dot1x timer supp-timeout 30
dot1x retry 1
dot1x authentication-method eap
```

A user connects a device to GigabitEthernet 1/0/1 on switch. The device does not have an 802.1X supplicant. One minute passes. How does the switch port handle the client?

- A. It blocks the client
- B. It assigns the client to VLAN2
- C. It assigns the client to VLAN3
- D. It assigns the client to VLAN4

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 45

A company uses 802.1X authentication to force users to connect to the network. The company uses access layer switches to enforce the 802.1X authentication and HP IMC User Access manager (UAM) as the RADIUS server.

The customer requires switches to apply a specific settings to contractor use connections. The network administrator checks the switch documentation and determines that this settings uses a vendor-specific attribute (VSA). The administrator check UAN and verifies that it has this VSA defined on it.

How does administrator configure UAM to apply the correct setting?



- A. Define IP port groups on the access devices that need to receive the settings. Configure the VSA and its settings within these groups.
- B. Add the settings to the VSA definition and then activate the VSA globally
- C. Create a scenario with the VSA and its settings; apply this scenario to the access devices that need to receive the settings
- D. Create a proprietary attribute policy with the VSA and its settings; apply this policy in the service policy for the contractor users

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 46**

How does virtual output queuing (VoQ) help switches avoid head-of-line blocking and enhance throughput?

- A. It divides each port ingress queue into different queues based on the priority and egress port of each packet
- B. It establishes a matrix of connections to multiple cross-bar switches within the switch backplane
- C. It considers traffic congestion, queues traffic, and informs the ingress port when it can use the crossbar
- D. It allows the ingress port to fragment packets and send the fragments in multiple queues over different crossbars

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 47**

A company uses 802.1X authentication to force users to authenticate to connect to the network. The company uses HP IMC User Access manager (UAM) as the RADIUS server. The company wants to assign users to VLANs based on their identity. For example, contractor should be assigned in VLAN 20. Assume that VLANs are extended correctly across the network infrastructure.

Where does a network administrator configure the VLAN policy?

- A. In the access device configuration UAM
- B. In local-user accounts for contractors, which are configured on access layer switches
- C. In an authorized VLAN list, which is applied to access layer switches edge ports
- D. In an access rule on UAM, which will be selected in the contractor service policy

**Correct Answer:** D

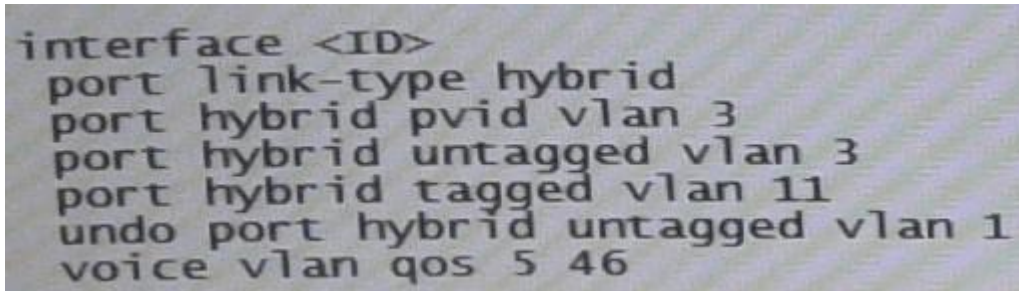
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 48**

Refer to the exhibit.



```
interface <ID>
port link-type hybrid
port hybrid pvid vlan 3
port hybrid untagged vlan 3
port hybrid tagged vlan 11
undo port hybrid untagged vlan 1
voice vlan qos 5 46
```

An HP Comware Switch connects to Voice over (VoIP) phones. The phones connect to user's computers, so each switch port connects a computer and a phone.

These are the specifications:

The VLAN for data traffic is VLAN3

The VLAN for traffic VoIP is VLAN11

The phones support Link Layer Discovery Protocol (LLDP) Media Endpoint Detection (MED).

The network administrator wants to use LLDP-MED to advertise the voice VLAN ID and priority settings to the phones. The phones will then send tagged traffic in that VLAN. The switch should not check the incoming traffic's MAC address against its voice OID list. The exhibit shows the applicable switch port configuration.

Which additional step must the administrator complete to accomplish this?

- A. Enable voice VLAN 11 (voice vlan 11 enable)
- B. Change the port to trunk mode (port link-type trunk)
- C. Enable LLDP compatibility with Cisco Discovery Protocol (CDP) (lldp compliance admin-status cdp txrx)
- D. Enable the port to advertise voice VLAN 11 with LLDP (lldp voice-vlan 11)

**Correct Answer: D**

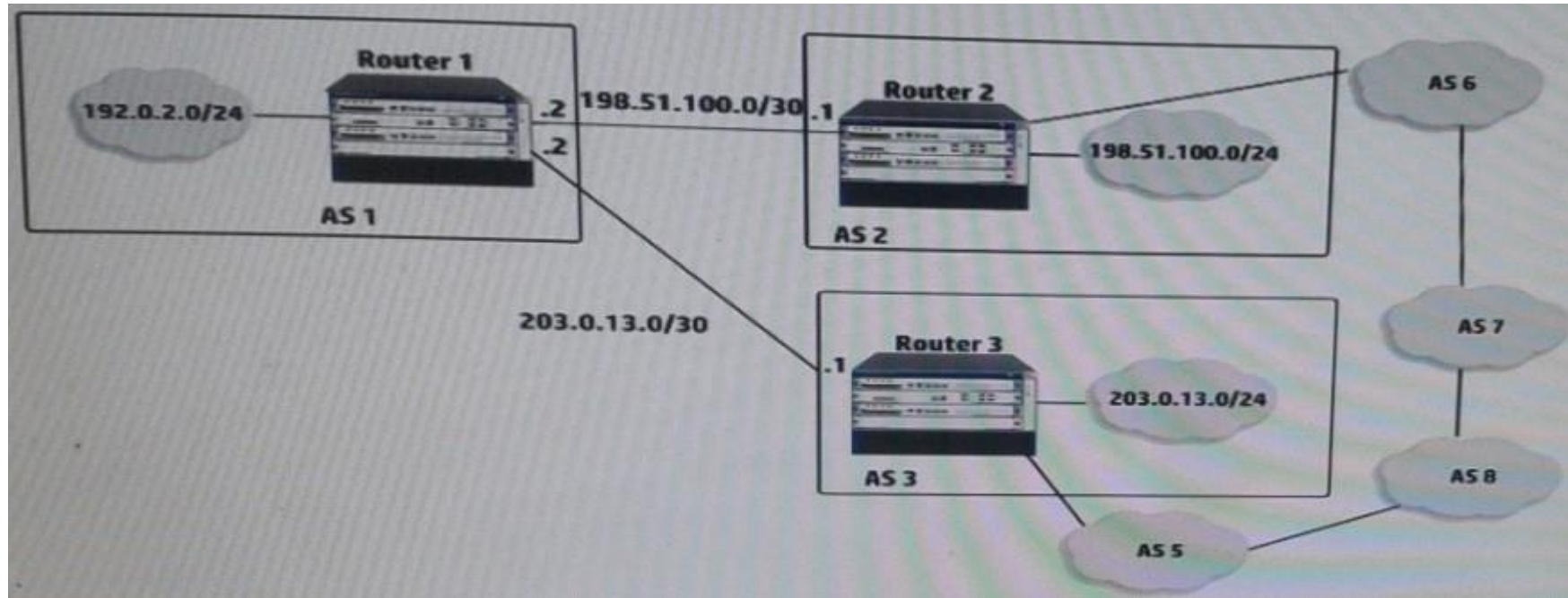
**Section: (none)**

**Explanation**

Explanation/Reference:

**QUESTION 49**

Refer to the exhibit.



These three routers are currently configured for BGP. They do not apply any routing policy in terms of BGP on routes or attributes advertised to an received from peers. How can the network administrator for Router 1 cause Router 1 to advertise 192.0.2.0/24 to Router 2 and Router 3?

- A. Enable BGP routing on RAGG1
- B. Add a null route to 192.0.2.0/24
- C. Apply route policy 1 as an inbound policy for both peers
- D. Apply route policy 1 as an outbound policy for both peers

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 50**

A company needs a simple authenticate solution for guests. The HP Comware access layer switches will implement portal authentication (or Web-Auth). The network administrator wants the switch to host the login web page on an IP address that not used for any other purpose.

What should the administrator do to accomplish this goal?

- A. Set the IP address when defining the local portal server, and create a loopback interface for the address
- B. Create RADIUS scheme that specifies this IP address for the authentication server. Select this scheme for portal authentication in the default domain
- C. Create a layer 3 interface for the guest VLAN and assign the desired IP address. Activate local portal authentication on this interface.
- D. Set the IP address when defining the local portal server, and the switch automatically begins using that address.

**Correct Answer:** C

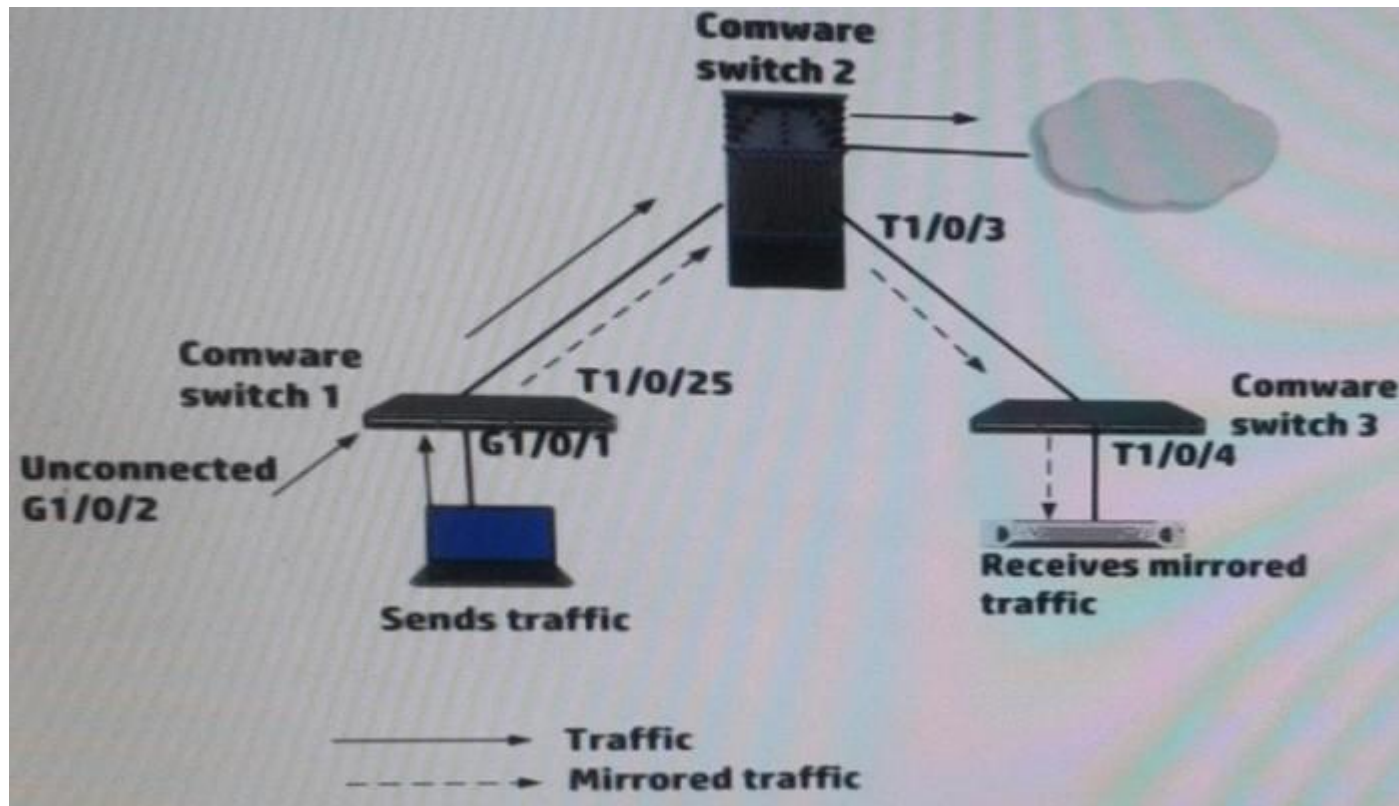
**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 51**

Refer to the exhibit.



A network administrator set up a remote mirroring on the HP Comware switches in the exhibit. The administrator must define several ports while entering mirroring-group commands on these switches. Which port should be the reflector port (sometimes called monitor-egress port)?

- A. Switch 1, G1/0/2
- B. Switch3, T1/0/4
- C. Switch 1, T1/0/25
- D. Switch 1, G1/0/1

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 52**

Two HP 10500 Series Switches connect on a 10G fiber link. One of the two fibers in the link breaks, and a broadcast storm occurs. How could a network administrator prevent a problem like this from happening again?

- A. Configure Device Link Detection Protocol (DLDP) on both sides of the link.
- B. Use Rapid Per VLAN Spanning Tree Plus (RPVST+) instead of Multiple Spanning Tree Protocol (MSTP).
- C. Implement sFlow or NetStream on both sides of the link, setting the collector to an Intelligent Management Center (IMC) server.
- D. Add another 10G link and create a link aggregation group on each switch that includes both links.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 53**

HP Comware Switch 1 connects to switch 2 on GigabitEthernet 1/0/1. Switch 2 implements an inbound rate limit of 600 Mbps. The network administrator wants switch 1 to buffer traffic that exceeds the Switch 2 rate limit of 600 Mbps and send the traffic at 600 Mbps. All traffic has the same 802.1p priority and is forwarded in priority queue 2. What should the administrator apply to the Switch 1 interface GigabitEthernet 1/0/1?

- A. A line rate limit of 600 Mbps on queue 2
- B. A QoS policy with a classifier that matches all traffic and a CAR behavior that sets a CIR of 600 Mbps
- C. A weighted random early discard (WRED) table with a limit of 600 for queue 2
- D. A traffic shaping rate limit of 600 Mbps on queue 2

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 54**

What distinguishes an HP switch with a CLOS fabric from an HP switch with a crossbar fabric?

- A. The CLOS fabric can integrate with a virtual switch, which is deployed in a virtualized server.
- B. The CLOS fabric is a requirement for an Intelligent Resilient Framework (IRF) virtual switch with more than two members.
- C. The CLOS fabric can dynamically shut down power to unused switch ports, proving better energy efficiency.

D. The CLOS fabric can dynamically load-balance internal traffic over many paths, helping the switch support 40G/100G. **VCE To PDF - Free Practice Exam**

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 55**

A company needs a simple guest access solution. On each HP Provision access layer switch, the network administrator (Web-Auth) to an external Web server. Which guidelines must the administrator follow while setting up the Web server?

- A. The Web server must be able to ping IP addresses in the Web-Auth subnet on each switch.
- B. The server must have a certificate that is signed by a CA certificate loaded on the access layer switches.
- C. The login pages must exactly match template pages provided by HP. with the exception of the logo image.
- D. The login pages must use specific names, which are documented in switch manuals.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

modified.