Vendor: Cisco

Exam Code: 300-410

Exam Name: Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)

Version: DEMO

QUESTION 1
A CoPP policy is applied for receiving SSH traffic from the WAN interface on a Cisco ISR4321 router. However, the SSH response from the router is abnormal and stuck during the high link utilization. The problem is identified as SSH traffic does not match in the ACL.
Which action resolves the issue?

A. Rate-limit SSH traffic to ensure dedicated bandwidth.
B. Apply CoPP on the control plane interface.
C. Increase the IP precedence value of SSH traffic to 6.
D. Apply CoPP on the WAN interface inbound direction.

Answer: B
Explanation:
The problem is "SSH traffic does not match in the ACL" and "CoPP policy is applied for receiving SSH traffic from the WAN interface" so we should apply CoPP on the control plane interface instead.

QUESTION 2
Which feature minimizes DoS attacks on an IPv6 network?

A. IPv6 Binding Security Table
B. IPv6 Router Advertisement Guard
C. IPv6 Prefix Guard
D. IPv6 Destination Guard

Answer: D
Explanation:
The Destination Guard feature helps in minimizing denial-of-service (DoS) attacks. It performs address resolutions only for those addresses that are active on the link, and requires the FHS binding table to be populated with the help of the IPv6 snooping feature.The feature enables the filtering of IPv6 traffic based on the destination address, and blocks the NDP resolution for destination addresses
that are not found in the binding table. By default, the policy drops traffic coming for an unknown destination.
Reference:
https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book/IPv6_Security.pdf

QUESTION 3
A network engineer is investigating a flapping (up/down) interface issue on a core switch that is synchronized to an NTP server. Log output does not show the time of the flap.
Which command allows on the switch the time of the flap according to the clock on the device?

A. clock calendar-valid
B. service timtstamps log datetime localtime show-timezone
C. service timestamps log uptime
D. clock summer-time mst recurring 2 Sunday mar 2:00 1 sunday nov 2:00

Answer: B
Explanation:

By default, Catalyst switches add a simple uptime timestamp to logging messages. This is a cumulative counter that shows the hours, minutes, and seconds since the switch has been booted up. For example:

```
20w2d: %LINK-3-UPDOWN: Interface FastEthernet1/0/27, changed state to
down
21w3d: %SYS-5-CONFIG_I: Configured from console by vty0 (172.25.15.246)
```

At exactly what date and time did that occur? Who knows!

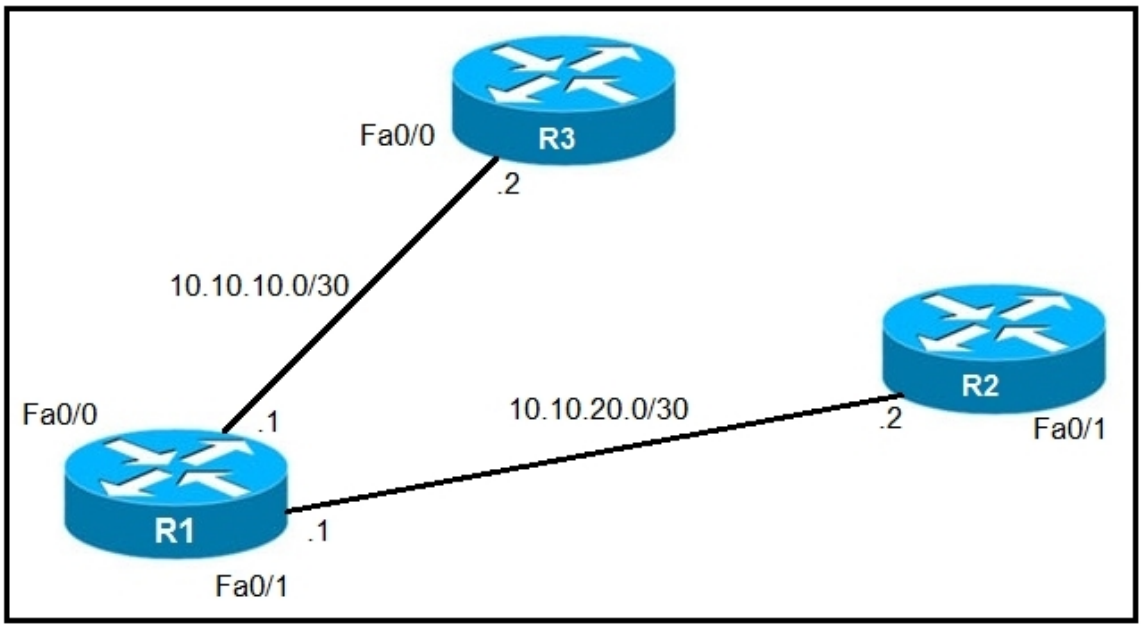
Instead, you can configure the switch to add accurate clock-like timestamps that are easily interpreted. you can use the following command to begin using the switch clock as an accurate timestamp for syslog messages:

```
Switch(config)# service timestamps log datetime [localtime] [show-
timezone] [msec] [year]
```

Below is the output if we entered the command “service timestamps log datetime localtime show-timezone” (without”msec” keyword the output would not show time in milisecond)

```
*Mar  1 00:02:24 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Loopback4, changed state to up
```

QUESTION 4
Refer to the exhibit. An IP SLA was configured on router R1 that allows the default route to be modified in the event that Fa0/0 losses reachability with the router R3 Fa0/0 interface.
The route has changed to flow through route R2.
Which debug command is used to troubleshoot this issue?



A. debug ip flow
B. debug ip sla error
C. debug ip routing
D. debug ip packet

Answer: C
Explanation:
The “debug ip routing” command enables debugging messages related to the routing table. Since the routing table is normally stable, you will only see debug messages when there are any changes in the routing table.

QUESTION 5
Refer to the exhibit. What is the result if applying this configuration?

```
R1#show policy-map control-plane
 Control Plane
        Service-policy input: CoPP-BGP
          Class-map: BGP (match all)
            2716 packets, 172071 bytes
            5 minute offered rate 0000 bps, drop rate 0000 bps
            Match: access-group name BGP
            drop

          Class-map: class-default (match-any)
            5212 packets, 655966 bytes
            5 minute offered rate 0000 bps, drop rate 0000 bps
            Match: any
```

A. The router can form BGP neighborships with any other device.
B. The router can form BGP neighborships with any device that matched by the access list named "BGP"
C. The router cannot form BGP neighborships with any other device
D. The router cannot form BGP neighborships with any device that is matched by the access list named "BGP"

Answer: D
Explanation:
https://tools.cisco.com/security/center/resources/protecting_border_gateway_protocol#13

QUESTION 6
What is a function of an end device configured with DHCPv6 guard?

A. If it is configured as a server, only prefix assignments are permitted.
B. If it is configured as a relay agent, only prefix assignments are permitted.
C. If it is configured as a client, messages are switched regardless of the assigned role.
D. If it is configured as a client, only DHCP requests are permitted.

Answer: C
Explanation:
The DHCPv6 Guard feature blocks reply and advertisement messages that come from

unauthorized DHCP servers and relay agents.
Packets are classified into one of the three DHCP type messages. All client messages are always switched regardless of device role. DHCP server messages are only processed further if the device role is set to server. Further processing of server messages includes DHCP server advertisements (for source validation and server preference) and DHCP server replies (for permitted prefixes). If the device is configured as a DHCP server, all the messages need to be switched, regardless of the device role configuration.

QUESTION 7
Refer to the exhibit. Users report that IP addresses cannot be acquired from the DHCP server. The DHCP server is configured as shown. About 300 total nonconcurrent users are using this DHCP server, but none of them are active for more than two hours per day. Which action fixes the issue within the current resources?

```
R1#show running-config | section dhcp
ip dhcp excluded-address 192.168.1.1 192.168.1.49
ip dhcp pool DHCP
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
   dns-server 8.8.8.8
   lease 0 12
```

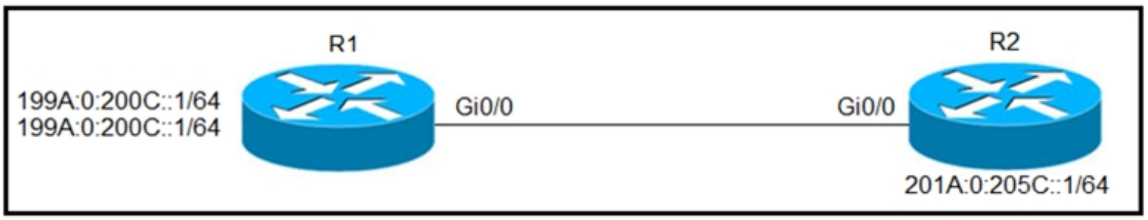
A. Configure the DHCP lease time to a bigger value
B. Add the network 192.168.2.0 255.255.255.0 command to the DHCP pool
C. Modify the subnet mask to the network 192.168.1.0 255.255.254.0 command in the DHCP pool
D. Configure the DHCP lease time to a smaller value

Answer: D
Explanation:
The command “lease 0 12” set the duration of the lease (the time during which a client computer can use an assigned IP address). The syntax is “lease {days[hours] [minutes] | infinite}”. In this case the lease is (0 day) 12 hours.

We also notice that the pool of IP addresses that can issue to the clients are rather small as the network 192.168.1.0/24 only supports 253 assignable IP addresses. But the first 49 IP addresses were excluded so we only have 253 – 49 = 204 assignable IP addresses < 300 users.

Therefore the best solution is here to reduce the time of each issued IP address (to 2 hours instead of 12 hours) as they only need to use in 2 hours per day, thus increasing the chance of reuse the IP addresses for the clients.

QUESTION 8
Refer to the exhibit. Which configuration denies Telnet traffic to router 2 from 198A:0:200C::1/64?



A.
```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64 eq telnet
!
int Gi0/0
 ipv6 traffic-filter Deny_Telnet in
!
```

B.
```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64 eq telnet
!
int Gi0/0
 ipv6 access-map Deny_Telnet in
!
```

C.
```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64
!
int Gi0/0
 ipv6 access-map Deny_Telnet in
!
```

D.
```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64
!
int Gi0/0
 ipv6 traffic-filter Deny_Telnet in
!
```

Answer: A
Explanation:
When assigning an IPv4 access list to an interface you used the ip access-list ACL_NAME in|out command in interface configuration mode. To assign an IPv6 ACL to an interface you'll use the ipv6 traffic-filter ACL_NAME in|out command in interface configuration mode.

We should also specific which port (telnet in this case) we want to deny or we will drop all TCP traffic to the destination.

Note: In fact there is an error with all of the above commands as we cannot use subnet mask (/64) with keyword "host". We must remove the subnet mask before applying the ACL statement.

QUESTION 9
Which two solutions are used to overcome a flapping link that causes a frequent label binding

exchange between MPLS routers? (Choose two)

A. Create link dampening on links to protect the session.
B. Increase input queue on links to protect the session.
C. Create targeted hellos to protect the session.
D. Increase a hold-timer to protect the session.
E. Increase a session delay to protect the session.

Answer: AC
Explanation:
To avoid having to rebuild the LDP session altogether, you can protect it. When the LDP session between two directly connected LSRs is protected, a targeted LDP session is built between the two LSRs. When the directly connected link does go down between the two LSRs, the targeted LDP session is kept up as long as an alternative path exists between the two LSRs. For the protection to work, you need to enable it on both the LSRs. If this is not possible, you can enable it on one LSR, and the other LSR can accept the targeted LDP Hellos by configuring the command mpls ldp discovery targeted-hello accept.
Reference:
https://www.ccexpert.us/mpls-network/mpls-ldp-session-protection.html
https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/TECMPL-3201.pdf

Troubleshooting LDP Issues
Problem:
I. When a link flaps (for a short time),
...
Solution:
+ When LDP session supported by link hello is setup, create a targeted hello to protect the session.

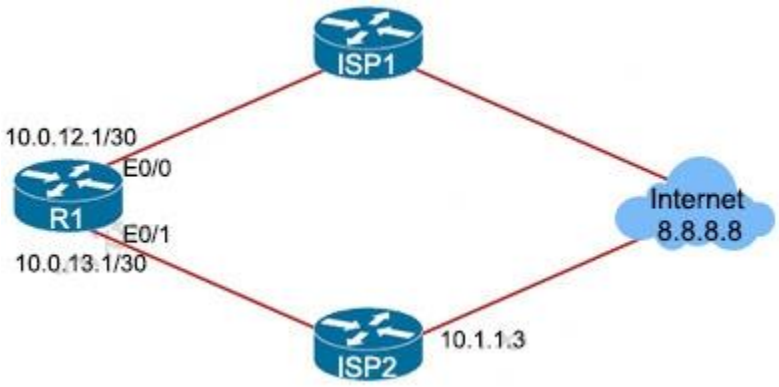
QUESTION 10
Refer to the exhibit. The administrator noticed that the connection was flapping between the two ISPs instead of switching to ISP2 when the ISP1 failed. Which action resolves the issue?

```
ip sla 1
 icmp-echo 8.8.8.8
 threshold 1000
 timeout 2000
 frequency 5
ip sla schedule 1 life forever start-time now
!
track 1 ip sla 1
!
ip route 0.0.0.0 0.0.0.0 203.0.113.1 name ISP1 track 1
ip route 0.0.0.0 0.0.0.0 198.51.100.1 2 name ISP2
```

A. Include a valid source-interface keyword in the icmp-echo statement.
B. Reference the track object 1 on the default route through ISP2 instead of ISP1.
C. Modify the static routes to refer both to the next hop and the outgoing intertace.

D. Modify the threshold to match the administrative distance of the ISP2 route.

Answer: A
Explanation:
With this configuration, when Track 1 is UP, traffic to the Internet (8.8.8.8 is the well-known DNS of Google) flows through ISP1. When Track 1 is DOWN, traffic to the Internet flows through ISP 2. But there is a problem with this configuration is we did not specify the source IP of the track. Usually, our router (R1 in the figure below) is connected to two ISPs via two different interface like this:



So if we don't specify the source IP, R1 will ping via E0/0 to ISP1. If the ping fails, R1 will remove the first default route so the backup path via ISP2 will be used and traffic will be sent via E0/1. But it also makes the track UP again (as we did not specify the source IP) and the main path is installed again to the routing table -> The connection will flap between two ISPs.
Therefore, in order to solve this issue, we must configure a source IP for the ping. In the example above, we can configure like this: "icmp-echo 8.8.8.8 source-ip 10.0.12.1".
Note: The configuration above means:
Timeout: 2000 milliseconds
frequency: 5 seconds
threshold: 1000 milliseconds

Reference: https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200785-ISP-Failover-with-default-routes-using-I.html

QUESTION 11
Refer to the exhibit. What does the imp-null tag represent in the MPLS VPN cloud?

```
Router# show tag-switching tdp bindings
(…)
tib entry: 10.10.10.1/32, rev 31
        local binding: tag: 18
        remote binding: tsr: 10.10.10.1:0, tag: imp-null
        remote binding: tsr: 10.10.10.2:0, tag: 18
        remote binding: tsr: 10.10.10.6:0, tag: 21
tib entry: 10.10.10.2/32, rev 22
        local binding: tag: 17
        remote binding: tsr: 10.10.10.2:0, tag: imp-null
        remote binding: tsr: 10.10.10.1:0, tag: 19
        remote binding: tsr: 10.10.10.6:0, tag: 22
```

A. Include the EXP bit
B. Exclude the EXP bit
C. Impose the label
D. Pop the label

Answer: D
Explanation:
The “imp-null” (implicit null) tag instructs the upstream router to pop the tag entry off the tag stack before forwarding the packet.
Note: pop means “remove the top MPLS label”

QUESTION 12
When provisioning a device in Cisco DNA Center, the engineer sees the error message "Cannot select the device. Not compatible with template.". What is the reason for the error?

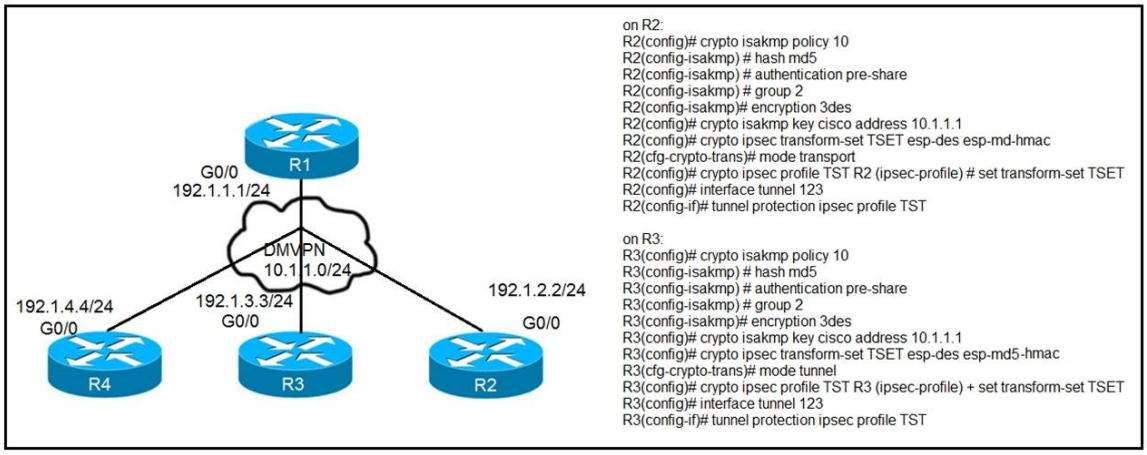
A. The software version of the template is different from the software version of the device
B. The changes to the template were not committed
C. The template has an incorrect configuration.
D. The tag that was used to filter the templates does not match the device tag.

Answer: D
Explanation:
If you use tags to filter the templates, you must apply the same tags to the device to which you want to apply the templates. Otherwise, you get the following error during provisioning: “Cannot select the device. Not compatible with template.”

Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-10/user_guide/b_cisco_dna_center_ug_1_2_10/b_dnac_ug_1_2_10_chapter_0111.html

QUESTION 13

Refer to the exhibit. After applying IPsec, the engineer observed that the DMVPN tunnel went down, and both spoke-to-spoke and hub were not establishing.
Which two actions resolve the issue? (Choose two.)



on R2:
R2(config)# crypto isakmp policy 10
R2(config-isakmp) # hash md5
R2(config-isakmp) # authentication pre-share
R2(config-isakmp) # group 2
R2(config-isakmp)# encryption 3des
R2(config)# crypto isakmp key cisco address 10.1.1.1
R2(config)# crypto ipsec transform-set TSET esp-des esp-md-hmac
R2(cfg-crypto-trans)# mode transport
R2(config)# crypto ipsec profile TST R2 (ipsec-profile) # set transform-set TSET
R2(config)# interface tunnel 123
R2(config-if)# tunnel protection ipsec profile TST

on R3:
R3(config)# crypto isakmp policy 10
R3(config-isakmp) # hash md5
R3(config-isakmp) # authentication pre-share
R3(config-isakmp) # group 2
R3(config-isakmp)# encryption 3des
R3(config)# crypto isakmp key cisco address 10.1.1.1
R3(config)# crypto ipsec transform-set TSET esp-des esp-md5-hmac
R3(cfg-crypto-trans)# mode tunnel
R3(config)# crypto ipsec profile TST R3 (ipsec-profile) + set transform-set TSET
R3(config)# interface tunnel 123
R3(config-if)# tunnel protection ipsec profile TST

A. Configure the crypto isakmp key cisco address 0.0.0.0 on R2 and R3.
B. Remove the crypto isakmp key cisco address 10.1.1.1 on R2 and R3.
C. Change the mode from mode transport to mode tunnel on R2.
D. Configure the mode from mode tunnel to mode transport on R3.
E. Configure the crypto isakmp key cisco address 192.1.1.1 on R2 and R3.

Answer: AB
Explanation:
You can't just put in the command with 0.0.0.0. If you do, you will end up with two crypto key commands and both addresses so the one to the tunnel address MUST be removed.

QUESTION 14
Which configuration enables the VRF that is labeled `'inet'' on FastEthernet0/0?

A. R1(config)# ip vrf Inet
R1(config-vrf)#ip vrf FastEthernet0/0
B. R1 (conflg)#ip vrf Inet FastEthernet0/0
C. R1(config)# ip vrf Inet
R1(config-vrf)#interface FastEthernet0/0
R1(config-if)#ip vrf forwarding Inet
D. R1 (config)#router ospf 1 vrf Inet
R1 (config-router)#ip vrf forwarding FastEthernet0/0

Answer: C
Explanation:
The first command “R1(config)# ip vrf Inet” creates vrf Inet while the two last commands associate the VRF with interface Fa0/0.

QUESTION 15
Which attribute eliminates LFAs that belong to protected paths in situations where links in a network are connected through a common fiber?

A. Interface-dispoint
B. Shared risk link group-disjoint
C. Linecard-disjoint
D. Lowest-repair-path-metric

Answer: B
Explanation:
Shared Risk Link Group (SRLG)-disjoint—Eliminates LFAs that belong to any of the protected path SRLGs. SRLGs refer to situations where links in a network share a common fiber (or a common physical attribute). If one link fails, other links in the group may also fail. Therefore, links in a group share risks.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-3s/asr1000/ire-xe-3s-asr1000/ire-ipfrr.html

QUESTION 16
White working with software images, an engineer observes that Cisco DNA Center cannot upload its software image directly from the device. Why is the image not uploading?

A. The device has lost connectivity to Cisco DNA Center.
B. The software image for the device is in bundle mode
C. The software image for the device is in install mode.
D. The device must be resynced to Cisco DNA Center

Answer: C
Explanation:
When a device is in Install Mode, Cisco DNA Center is unable to upload its software image directly from the device. When a device is in install mode, you must first manually upload the software image to the Cisco DNA Center repository before marking the image as golden.

Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3/user_guide/b_cisco_dna_center_ug_1_3/b_cisco_dna_center_ug_1_3_chapter_0100.html

QUESTION 17
Which command allows traffic to load-balance in an MPLS Layer 3 VPN configuration?

A. Multi-paths eibgp 2
B. Maximum-paths ibgp 2
C. Multi-paths 2
D. Maximum-paths 2

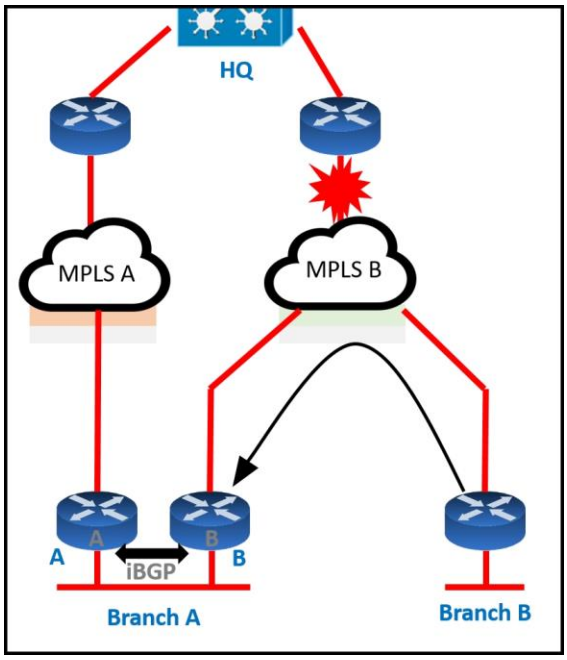
Answer: D
Explanation:
maximum-paths [ibgp] number-of-paths
Example:
switch(config-router-af)# maximum-paths 4
Configures the maximum number of multipaths allowed. Use the ibgp keyword to configure iBGP load balancing. The range is from 1 to 16.

QUESTION 18
Which mechanism provides traffic segmentation within a DMVPN network?

A. RSVP
B. BGP
C. MPLS
D. iPsec

Answer: C
Explanation:
To use the 2547oDMPVN--Traffic Segmentation Within DMVPN feature you must configure Multiprotocol Label Switching (MPLS) by using the **mpls ip** command.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-16/sec-conn-dmvpn-xe-16-book/sec-conn-dmvpn-dmvpn.html

QUESTION 19
Refer to the exhibit. the MPLS B network to reach HQ. Which action achieves this requirement?



A. Introduce an AS path filter on branch A routers so that only local prefixes are advertised into BGP
B. increase the local preference for all HQ prefixes received at branch B from the MPLS B network to be higher than the local preferences used on the MPLS A network
C. Introduce AS path prepending on the branch A MPLS B network connection so that any HQ advertisements from branch A toward the MPLS B network are prepended three times
D. Modify the weight of all HQ prefixes received at branch B from the MPLS B network to be higher than the weights used on the MPLS A network

Answer: A
Explanation:
If we modify the weight, increase local preference or use AS path prepending then we can only make MPLS B prefer over MPLS A. But when MPLS B is down then MPLS A will be used which does not meet the requirement of this question. Only with AS path filtering we can deny prefixes from certain AS and make sure branch B never uses MPLS A to reach HQ.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**