QUESTION 1
Refer to the exhibit. A router receiving BGP routing updates from multiple neighbors for routers in AS 690.
What is the reason that the router still sends traffic that is destined to AS 690 to a neighbor other than 10.222.10.1?

A. The local preference value in another neighbor statement is higher than 250.
B. The local preference value should be set to the same value as the weight in the route map.
C. The route map is applied in the wrong direction.
D. The weight value in another statement is higher than 200.

Answer: B

QUESTION 2
Which list defines the contents of an MPLS label?

A. 20-bit label; 3-bit traffic class; 1-bit bottom stack; 8-bit TTL.
B. 32-bit label; 3-bit flow label; 1-bit bottom stack; 8-bit hop limit.
C. 20-bit label; 3-bit flow label: 1-bit bottom stack; 8-bit hop limit
D. 32-bit label; 3-bit traffic class; 1-bit bottom stack; 8-bit TTL

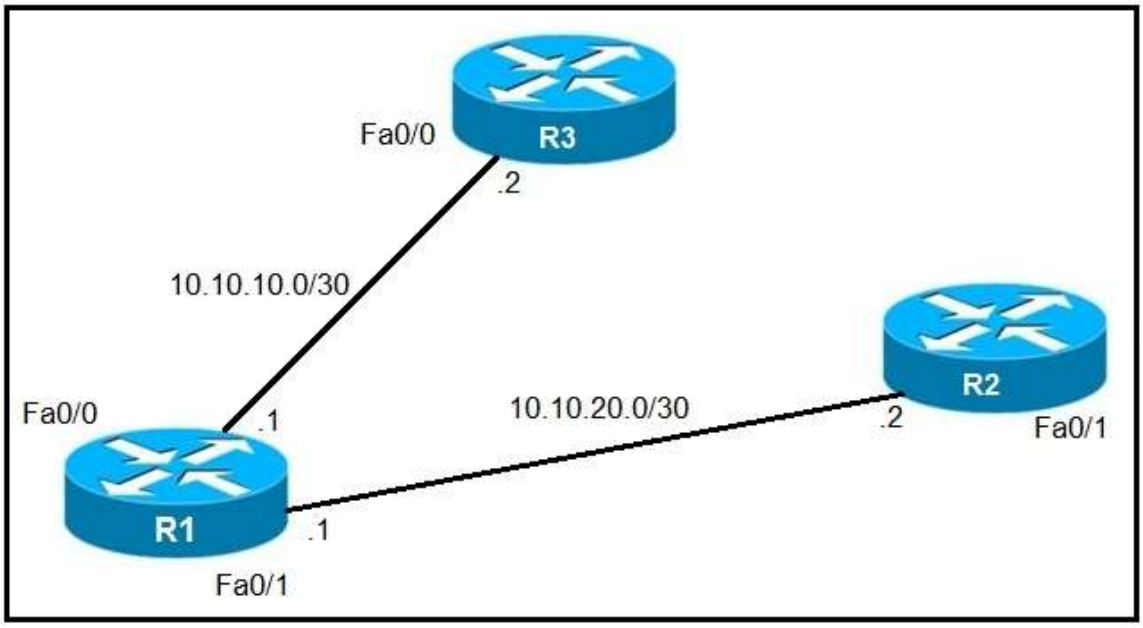
Answer: A
Explanation:
MPLS uses a 32-bit label field that contains the information that follows:
+ 20-bit label (a number)
+ 3-bit class of service (or experimental field, typically used to carry IP precedence value)
+ 1-bit bottom-of-stack indicator (indicates whether this is the last label before the IP header)
+ 8-bit TTL (equal to the TTL in the IP header)

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: A

QUESTION 6
Refer to the exhibit. During troubleshooting it was discovered that the device is not reachable using a secure web browser. What is needed to fix the problem?

```
access-list 100 deny tcp any any eq 465
access-list 100 deny tcp any eq 465 any
access-list 100 permit tcp any any eq 80
access-list 100 permit tcp any eq 80 any
access-list 100 permit udp any any eq 443
access-list 100 permit udp any eq 443 any
```

A. permit tcp port 465.
B. permit tcp port 443
C. permit udp port 465
D. permit tcp port 22

Answer: B

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?

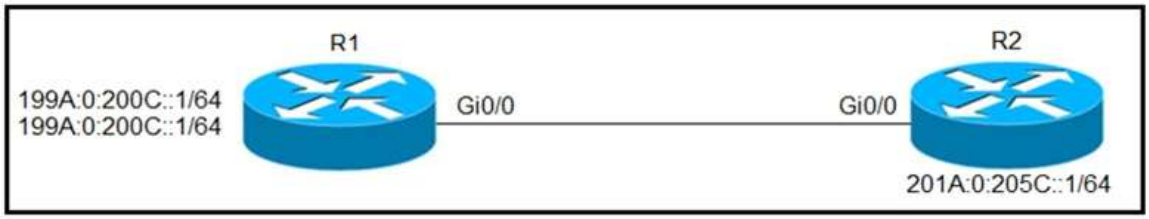
```
R1#show running-config | section dhcp
ip dhcp excluded-address 192.168.1.1 192.168.1.49
ip dhcp pool DHCP
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
   dns-server 8.8.8.8
   lease 0 12
```

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
What statement about route distinguishers in an MPLS network is true?

A. Route distinguishers make a unique VPNv4 address across the MPLS network.

B. Route distinguishers allow multiple instances of a routing table to coexist within the edge router.
C. Route distinguishers are used for label bindings
D. Route distinguishers define which prefixes are imported and exported on the edge router

Answer: A

QUESTION 10
Refer to the exhibit. Which control plan policy limits BGP traffic that is destined to the CPU to 1 Mbps and ignores BGP traffic that is higher rate?

```
Cat3850-Stack-2# show policy-map

Policy Map LIMIT_BGP
  Class BGP
    drop

Policy Map SHAPE_BGP
  Class BGP
    Average Rate Traffic Shaping
    cir 10000000 (bps)

Policy Map POLICE_BGP
  Class BGP
    police cir 1000k bc 1500
      conform-action transmit
      exceed-action transmit

Policy Map COPP
  Class BGP
    police cir 1000k bc 1500
      conform-action transmit
      exceed-action drop
```

A. policy-map SHAPE_BGP
B. policy-map LIMIT_BGP
C. policy-map POLICE_BGP
D. policy-map COPP

Answer: D

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

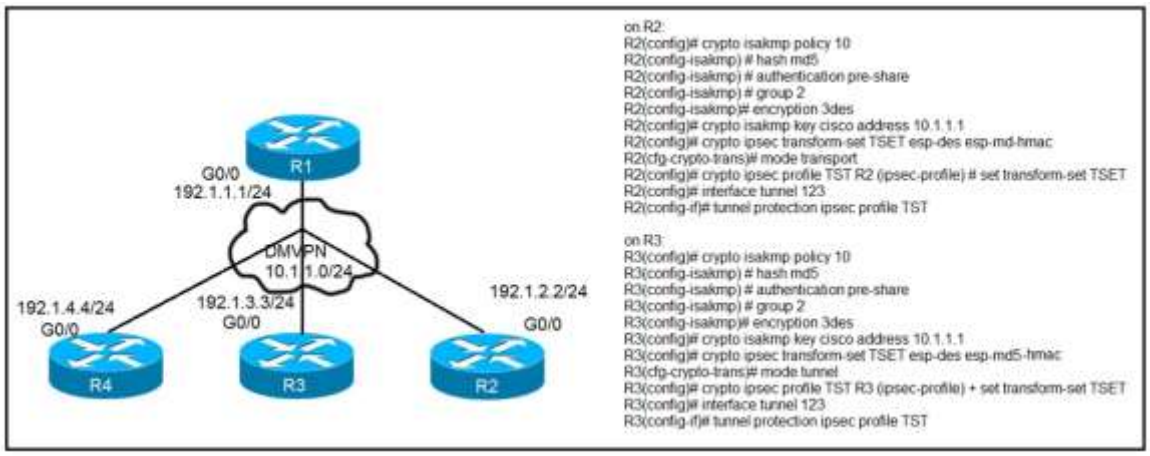
Answer: D
Explanation:
The “imp-null” (implicit null) tag instructs the upstream router to pop the tag entry off the tag stack before forwarding the packet.
Note: pop means “remove the top MPLS label”

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.)



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: AD
Explanation:
The first six commands are used to configure IPSec Phase 1 (ISAKMP Policy). Here is the details of each command used above:
+ crypto isakmp policy 10 – This command creates ISAKMP policy number 10. You can create multiple policies, for example 7, 8, 9 with different configuration. Routers participating in Phase 1 negotiation tries to match a ISAKMP policy matching against the list of policies one by one. If any policy is matched, the IPSec negotiation moves to Phase 2.
+ hash md5– MD5 algorithm will be used.
+ authentication pre-share – Authentication method is pre-shared key.
+ group 2 – Diffie-Hellman group to be used is group 2.
+ encryption 3des – 3DES encryption algorithm will be used for Phase 1.
+ crypto isakmp key cisco address 10.1.1.1 – The Phase 1 password is cisco and remote peer IP address is 10.1.1.1
The next two command lines are used to configure IPSec Phase 2 (Transform Set):
+ crypto ipsec transform-set <transform-set-name> – Creates transform-set called <transform-set-name>
+ esp-des – ESP IPSec protocol with the 56-bit Data Encryption Standard (DES) encryption algorithm will be used
+ esp-md5-hmac – ESP with the MD5 (HMAC variant) authentication algorithm will be used.
+ mode transport: only encrypts the payload and ESP trailer
or
+ mode tunnel: encrypts the IP header of the ENTIRE packet

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:
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