Exam Questions 350-401

Implementing and Operating Cisco Enterprise Network Core Technologies

https://www.2passeasy.com/dumps/350-401/

NEW QUESTION 1
A network administrator is implementing a routing configuration change and enables routing debugs to track routing behavior during the change. The logging output on the terminal is interrupting the command typing process. Which two actions can the network administrator take to minimize the possibility of typing commands incorrectly? (Choose two.)

A. Configure the logging synchronous global configuration command
B. Configure the logging delimiter feature
C. Configure the logging synchronous command under the vty
D. Press the TAB key to reprint the command in a new line
E. increase the number of lines on the screen using the terminal length command

Answer: CD

NEW QUESTION 2
A customer requests a network design that supports these requirements:

- FHRP redundancy
- multivendor router environment
- IPv4 and IPv6 hosts

Which protocol does the design include?

A. HSRP version 2
B. VRRP version 2
C. GLBP
D. VRRP version 3

Answer: D

NEW QUESTION 3
Which devices does Cisco DNA Center configure when deploying an IP-based access control policy?

A. All devices integrating with ISE
B. selected individual devices
C. all devices in selected sites
D. all wired devices

Answer: A

Explanation:
When you click Deploy, Cisco DNA Center requests the Cisco Identity Services Engine (Cisco ISE) to send notifications about the policy changes to the network devices.

NEW QUESTION 4
What is one fact about Cisco SD-Access wireless network deployments?

A. The access point is part of the fabric underlay
B. The WLC is part of the fabric underlay
C. The access point is part the fabric overlay
D. The wireless client is part of the fabric overlay

Answer: C

NEW QUESTION 5
Which algorithms are used to secure REST API from brute attacks and minimize the impact?

A. SHA-512 and SHA-384
B. MD5 algorithm-128 and SHA-384
C. SHA-1, SHA-256, and SHA-512
D. PBKDF2, BCrypt, and SCrypt
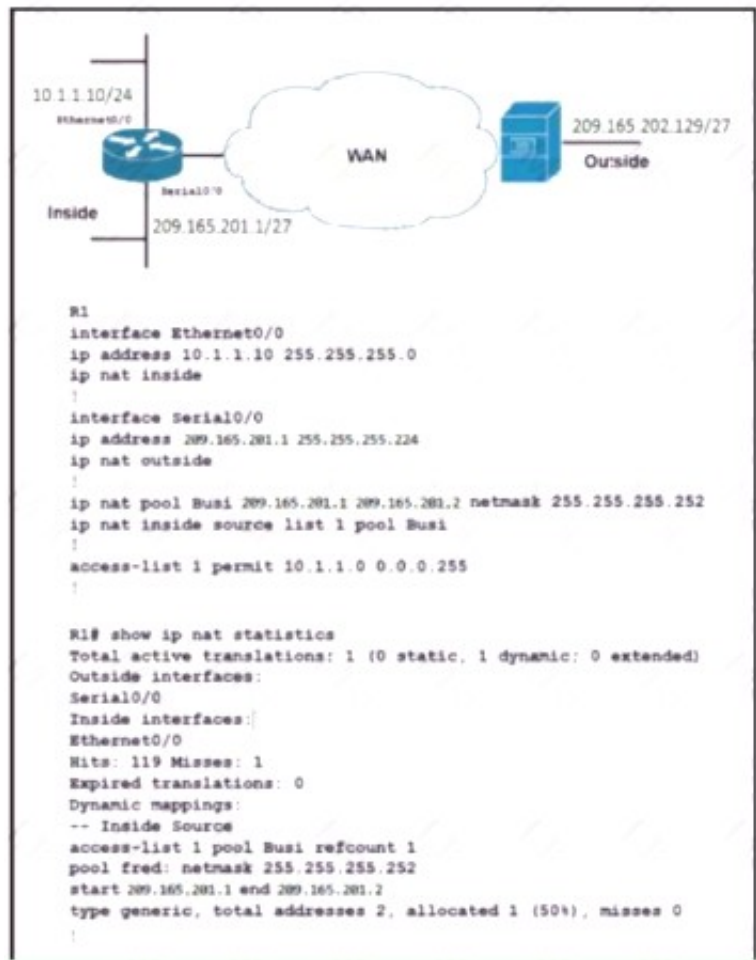
Answer: D

Explanation:
One of the best practices to secure REST APIs is using password hash. Passwords must always be hashed to protect the system (or minimize the damage) even if it is compromised in some hacking attempts. There are many such hashing algorithms which can prove really effective for password security e.g. PBKDF2, bcrypt and scrypt algorithms.
Other ways to secure REST APIs are: Always use HTTPS, Never expose information on URLs (Usernames, passwords, session tokens, and API keys should not appear in the URL),
Adding Timestamp in Request, Using OAuth, Input Parameter Validation.

NEW QUESTION 6

Refer to the exhibit.

```
10.1.1.10/24
  Ethernet0/0
                    WAN              209.165.202.129/27
                                         Outside
  Serial0/0
Inside
      209.165.201.1/27

R1
interface Ethernet0/0
ip address 10.1.1.10 255.255.255.0
ip nat inside
!
interface Serial0/0
ip address 209.165.201.1 255.255.255.224
ip nat outside
!
ip nat pool Busi 209.165.201.1 209.165.201.2 netmask 255.255.255.252
ip nat inside source list 1 pool Busi
!
access-list 1 permit 10.1.1.0 0.0.0.255
!

R1# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 0 extended)
Outside interfaces:
Serial0/0
Inside interfaces:
Ethernet0/0
Hits: 119 Misses: 1
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool Busi refcount 1
pool fred: netmask 255.255.255.252
start 209.165.201.1 end 209.165.201.2
type generic, total addresses 2, allocated 1 (50%), misses 0
```

A network engineer configures NAT on R1 and enters me show command to verity the configuration What toes the output confirm?

A. The first pocket triggered NAT to add on entry to NAT table
B. R1 is configured with NAT overload parameters
C. A Telnet from 160.1.1 1 to 10.1.1.10 has been initiated.
D. R1 to configured with PAT overload parameters

Answer: A

NEW QUESTION 7
Drag and drop the threat defense solutions from the left onto their descriptions on the right.

Umbrella		provides malware protection on endpoints
AMP4E		provides IPS/IDS capabilities
FTD		performs security analytics by collecting network flows
StealthWatch		protects against email threat vector
ESA		provides DNS protection

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Umbrella		AMP4E
AMP4E		FTD
FTD		StealthWatch
StealthWatch		ESA
ESA		Umbrella

NEW QUESTION 8
Drag and drop the characteristics from the left onto the orchestration tools they describe on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 9
Which technology provides a secure communication channel for all traffic at Layer 2 of the OSI model?

A. MACsec
B. IPsec
C. SSL
D. Cisco Trustsec

Answer: A

Explanation:
MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-ofband methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the

NEW QUESTION 10
What occurs when a high bandwidth multicast stream is sent over an MVPN using Cisco hardware?

A. The traffic uses the default MDT to transmit the data only if it isa (S,G) multicast route entry
B. A data MDT is created to if it is a (*, G) multicast route entries
C. A data and default MDT are created to flood the multicast stream out of all PIM-SM neighbors.
D. A data MDT is created to allow for the best transmission through the core for (S, G) multicast route entries.

Answer: B

NEW QUESTION 10
Which statement about TLS is accurate when using RESTCONF to write configurations on network devices?

A. It requires certificates for authentication
B. It is provided using NGINX acting as a proxy web server
C. It is used for HTTP and HTTPS requests
D. It is not supported on Cisco devices

Answer: B

NEW QUESTION 11
Which command set configures RSPAN to capture outgoing traffic from VLAN 3 on interface GigabitEthernet 0/3 while ignoring other VLAN traffic on the same interface?

monitor session 2 source interface gigabitethernet0/3 tx
monitor session 2 filter vlan 3

monitor session 2 source interface gigabitethernet0/3 tx
monitor session 2 filter vlan 1 - 2 , 4 - 4094

monitor session 2 source interface gigabitethernet0/3 rx
monitor session 2 filter vlan 3

monitor session 2 source interface gigabitethernet0/3 rx
monitor session 2 filter vlan 1 - 2 , 4 - 4094

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

Answer: D

NEW QUESTION 16
How does the RIB differ from the FIB?

A. The RIB is used to create network topologies and routing table
B. The FIB is a list of routes to particular network destinations.
C. The FIB includes many routes a single destinatio
D. The RIB is the best route to a single destination.
E. The RIB includes many routes to the same destination prefi
F. The FIB contains only the best route
G. The FIB maintains network topologies and routing table
H. The RIB is a list of routes to particular network destinations.

Answer: A

Explanation:
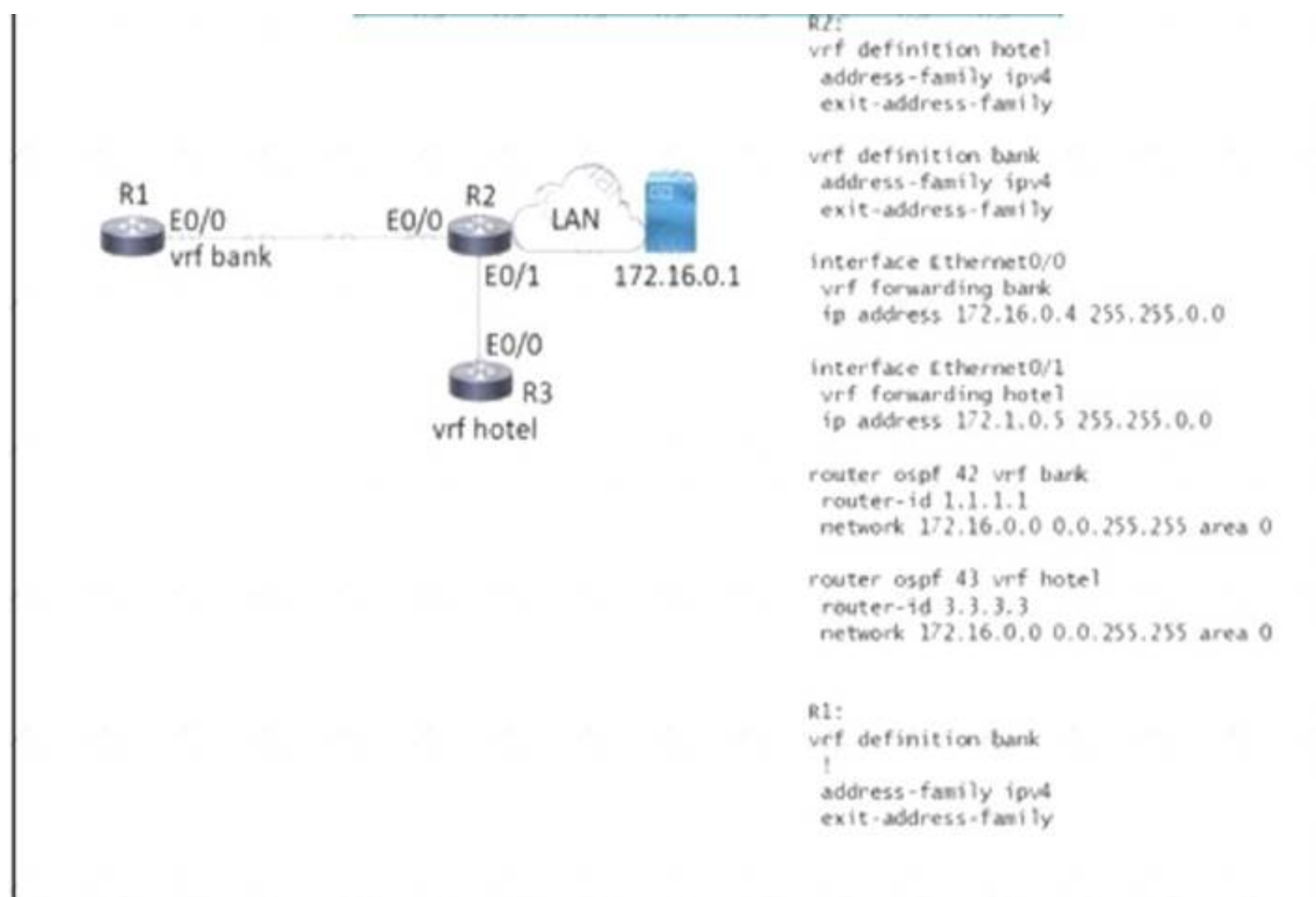RIB is derived from the control plane, FIB is used for forwarding,

NEW QUESTION 21
Which measurement is used from a post wireless survey to depict the cell edge of the access points?

A. SNR
B. Noise
C. RSSI
D. CCI

Answer: A

NEW QUESTION 22
Refer to the exhibit.

```
R2:
vrf definition hotel
 address-family ipv4
 exit-address-family

vrf definition bank
 address-family ipv4
 exit-address-family

interface Ethernet0/0
 vrf forwarding bank
 ip address 172.16.0.4 255.255.0.0

interface Ethernet0/1
 vrf forwarding hotel
 ip address 172.1.0.5 255.255.0.0

router ospf 42 vrf bank
 router-id 1.1.1.1
 network 172.16.0.0 0.0.255.255 area 0

router ospf 43 vrf hotel
 router-id 3.3.3.3
 network 172.16.0.0 0.0.255.255 area 0


R1:
vrf definition bank
 !
 address-family ipv4
 exit-address-family
```

Which configuration must be applied to R to enable R to reach the server at 172.16.0.1?

A)
```
interface Ethernet0/0
 vrf forwarding hotel
 ip address 172.16.0.7 255.255.0.0

router ospf 44 vrf Hotel
 network 172.16.0.0 0.0.255.255 area 0
```

B)
```
interface Ethernet0/0
 ip address 172.16.0.7 255.255.0.0

router ospf 44 vrf hotel
 network 172.16.0.0 255.255.0.0
```

C)
```
interface Ethernet0/0
ip address 172.16.0.7 255.255.0.0

router ospf 44 vrf bank
 network 172.16.0.0 255.255.0.0
```

D)
```
interface Ethernet0/0
 vrf forwarding bank
 ip address 172.16.0.7 255.255.0.0

router ospf 44 vrf bank
 network 172.16.0.0 0.0.255.255 area 0
```
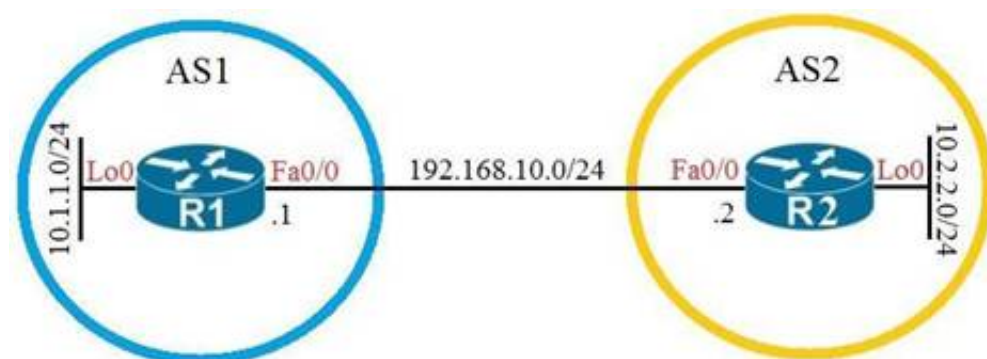
A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

NEW QUESTION 24
Refer to the exhibit.

Which configuration establishes EBGP neighborship between these two directly connected neighbors and exchanges the loopback network of the two routers through BGP?

A)

```
R1(config)#router bgp 1
R1(config-router)#neighbor 192.168.10.2 remote-as 2
R1(config-router)#network 10.1.1.0 mask 255.255.255.0

R2(config)#router bgp 2
R2(config-router)#neighbor 192.168.10.1 remote-as 1
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
```

B)

```
R1(config)#router bgp 1
R1(config-router)#neighbor 10.2.2.2 remote-as 2
R1(config-router)#network 10.1.1.0 mask 255.255.255.0

R2(config)#router bgp 2
R2(config-router)#neighbor 10.1.1.1 remote-as 1
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
```

C)

```
R1(config)#router bgp 1
R1(config-router)#neighbor 192.168.10.2 remote-as 2
R1(config-router)#network 10.0.0.0 mask 255.0.0.0

R2(config)#router bgp 2
R2(config-router)#neighbor 192.168.10.1 remote-as 1
R2(config-router)#network 10.0.0.0 mask 255.0.0.0
```

D)

```
R1(config)#router bgp 1
R1(config-router)#neighbor 10.2.2.2 remote-as 2
R1(config-router)#neighbor 10.2.2.2 update-source lo0
R1(config-router)#network 10.1.1.0 mask 255.255.255.0

R2(config)#router bgp 2
R2(config-router)#neighbor 10.1.1.1 remote-as 1
R2(config-router)#neighbor 10.1.1.1 update-source lo0
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
```

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

Answer: A

Explanation:
With BGP, we must advertise the correct network and subnet mask in the "network" command (in this case network 10.1.1.0/24 on R1 and network 10.2.2.0/24 on R2). BGP is very strict in the routing advertisements. In other words, BGP only advertises the network which exists exactly in the routing table. In this case, if you put the command "network x.x.0.0 mask 255.255.0.0" or "network x.0.0.0 mask 255.0.0.0" or "network x.x.x.x mask 255.255.255.255" then BGP will not advertise anything.
It is easy to establish eBGP neighborship via the direct link. But let's see what are required when we want to establish eBGP neighborship via their loopback interfaces. We will need two commands:
+ the command "neighbor 10.1.1.1 ebgp-multihop 2" on R1 and "neighbor 10.2.2.2 ebgpmultihop 2" on R1. This command increases the TTL value to 2 so that BGP updates can reach the
BGP neighbor which is two hops away.
+ Answer 'R1 (config) #router bgp 1
R1 (config-router) #neighbor 192.168.10.2 remote-as 2
R1 (config-router) #network 10.1.1.0 mask 255.255.255.0 R2 (config) #router bgp 2
R2 (config-router) #neighbor 192.168.10.1 remote-as 1
R2 (config-router) #network 10.2.2.0 mask 255.255.255.0 Quick Wireless Summary
Cisco Access Points (APs) can operate in one of two modes: autonomous or lightweight
+ Autonomous: self-sufficient and standalone. Used for small wireless networks.
+ Lightweight: A Cisco lightweight AP (LAP) has to join a Wireless LAN Controller (WLC) to function. LAP and WLC communicate with each other via a logical pair of CAPWAP tunnels.

– Control and Provisioning for Wireless Access Point (CAPWAP) is an IETF standard for control messaging for setup, authentication and operations between APs and WLCs. CAPWAP is similar to LWAPP except the following differences:

+CAPWAP uses Datagram Transport Layer Security (DTLS) for authentication and encryption to protect traffic between APs and controllers. LWAPP uses AES.

+ CAPWAP has a dynamic maximum transmission unit (MTU) discovery mechanism.

+ CAPWAP runs on UDP ports 5246 (control messages) and 5247 (data messages) An LAP operates in one of six different modes:

+ Local mode (default mode): measures noise floor and interference, and scans for intrusion detection (IDS) events every 180 seconds on unused channels

+ FlexConnect, formerly known as Hybrid Remote Edge AP (H-REAP), mode: allows data traffic to be switched locally and not go back to the controller. The FlexConnect AP can perform standalone client authentication and switch VLAN traffic locally even when it's disconnected to the WLC (Local Switched). FlexConnect AP can also tunnel (via CAPWAP) both user wireless data and control traffic to a centralized WLC (Central Switched).

+ Monitor mode: does not handle data traffic between clients and the infrastructure. It acts like a sensor for location-based services (LBS), rogue AP detection, and IDS

+ Rogue detector mode: monitor for rogue APs. It does not handle data at all.

+ Sniffer mode: run as a sniffer and captures and forwards all the packets on a particular channel to a remote machine where you can use protocol analysis tool (Wireshark, Airopeek, etc) to review the packets and diagnose issues. Strictly used for troubleshooting purposes.

+ Bridge mode: bridge together the WLAN and the wired infrastructure together.

Mobility Express is the ability to use an access point (AP) as a controller instead of a real WLAN controller. But this solution is only suitable for small to midsize, or multi-site branch locations where you might not want to invest in a dedicated WLC. A Mobility Express WLC can support up to 100 Aps
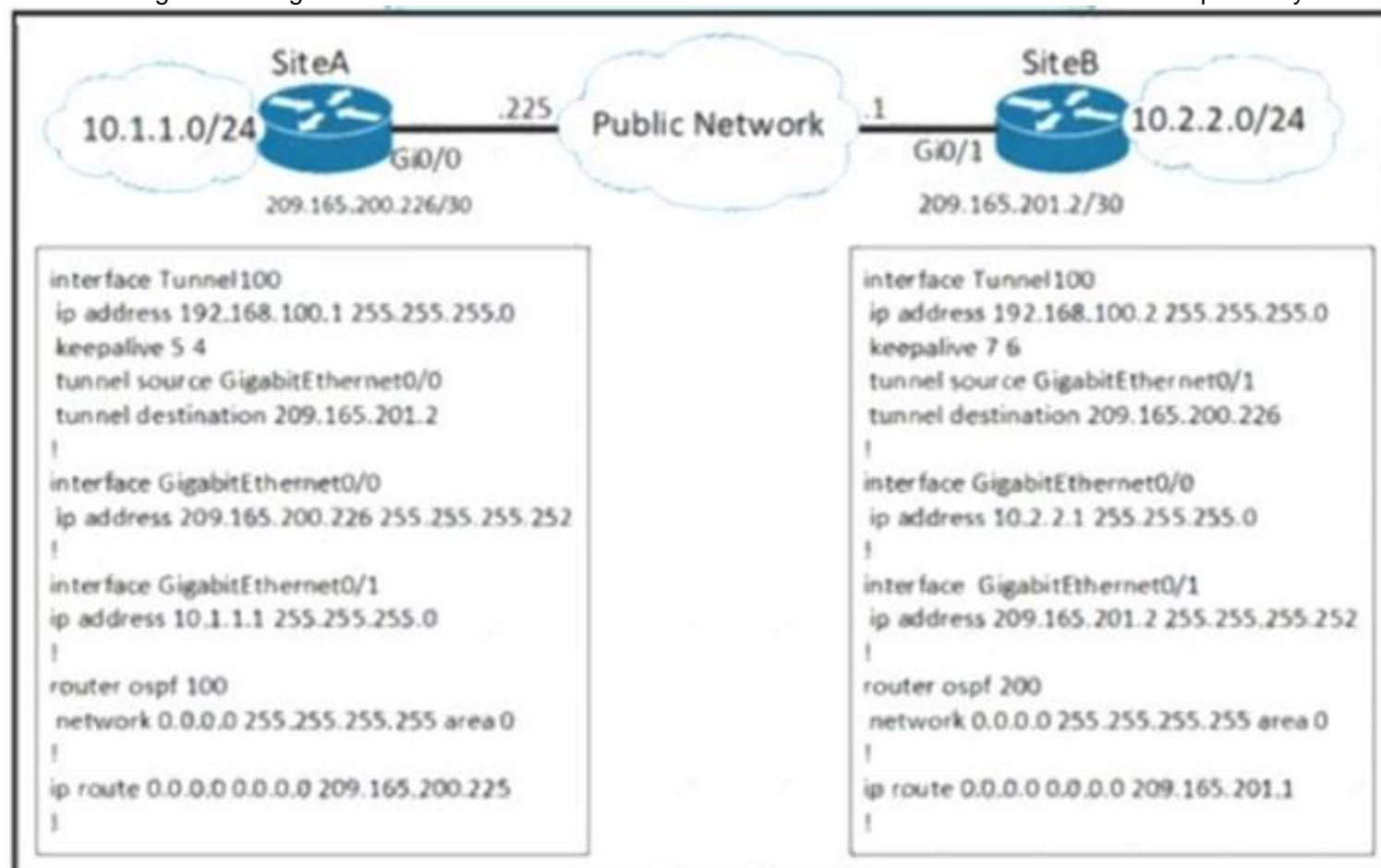
NEW QUESTION 27

An engineer is configuring a new SSID to present users with a splash page for authentication. Which WLAN Layer 3 setting must be configured to provide this functionally?

A. CCKM
B. WPA2 Policy
C. Local Policy
D. Web Policy

Answer: C

NEW QUESTION 30

A network engineer configures a new GRE tunnel and enters the show run command. What does the output verify?

A. The tunnel will be established and work as expected
B. The tunnel destination will be known via the tunnel interface
C. The tunnel keepalive is configured incorrectly because they must match on both sites
D. The default MTU of the tunnel interface is 1500 byte.

Answer: B

NEW QUESTION 33

Which benefit is offered by a cloud infrastructure deployment but is lacking in an on-premises deployment?

A. efficient scalability
B. virtualization
C. storage capacity
D. supported systems

Answer: A

NEW QUESTION 35
Refer to the exhibit.

```
Switch1#
*May 2 15:12:44:477: %SPANTREE-7-RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non trunk GigabitEthernet0/0 VLAN1.
*May 2 15:12:44:477: %SPANTREE-7-BLOCK_PORT_TYPE: Blocking GigabitEthernet0/0 on VLAN0001. Inconsistent port type.
```

```
        VLAN10                                          VLAN10
        10.0.0.1/24                                     10.0.0.2/24

    Switch1     Gi0/0                        Gi0/0    Switch2


hostname Switch1                         hostname Switch2
!                                        !
vtp domain DATACENTER1                   vtp domain DATACENTER2
!                                        !
Interface Gi0/0                          Interface Gi0/0
description TO DC2-Switch2               description TO DC1-Switch1
switchport mode trunk                    switchport mode dynamic desirable
!                                        !
Interface Vlan10                         Interface Vlan10
description LAN-10                        description LAN-10
ip address 10.0.0.1 255.255.255.0        ip address 10.0.0.2 255.255.255.0
```
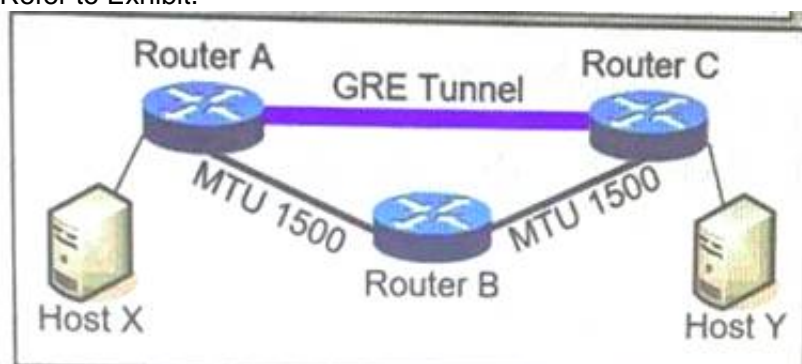
An engineer implemented several configuration changes and receives the logging message on switch1. Which action should the engineer take to resolve this issue?

A. Change the VTP domain to match on both switches
B. Change Switch2 to switch port mode dynamic auto
C. Change Switch1 to switch port mode dynamic auto
D. Change Switch1 to switch port mode dynamic desirable

Answer: A

NEW QUESTION 36
Refer to Exhibit.

```
        Router A                    Router C
              ====  GRE Tunnel  ====

         MTU 1500              MTU 1500
                    Router B

    Host X                        Host Y
```

MTU has been configured on the underlying physical topology, and no MTU command has been configured on the tunnel interfaces. What happens when a 1500-byte IPv4 packet traverses the GRE tunnel from host X to host Y, assuming the DF bit is cleared?

A. The packet arrives on router C without fragmentation.
B. The packet is discarded on router A
C. The packet is discarded on router B
D. The packet arrives on router C fragmented.

Answer: D

Explanation:
Text Description automatically generated

Like any protocol, using GRE adds a few bytes to the size of data packets. This must be factored into the MSS and MTU settings for packets. If the MTU is 1,500 bytes and the MSS is 1,460 bytes (to account for the size of the necessary IP and TCP headers), the addition of GRE 24-byte headers will cause the packets to exceed the MTU:

1,460 bytes [payload] + 20 bytes [TCP header] + 20 bytes [IP header] + 24 bytes [GRE header + IP header] = 1,524 bytes

As a result, the packets will be fragmented. Fragmentation slows down packet delivery times and increases how much compute power is used, because packets that exceed the MTU must be broken down and then reassembled.

NEW QUESTION 37

Which two operations are valid for RESTCONF? (Choose two.)

A. HEAD
B. REMOVE
C. PULL
D. PATCH
E. ADD
F. PUSH

Answer: AD

Explanation:
RESTCONF operations include OPTIONS, HEAD, GET, POST, PATCH, DELETE.

NEW QUESTION 41
Refer to the exhibit.

```
interface Vlan10
 ip vrf forwarding Customer1
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan20
 ip vrf forwarding Customer2
 ip address 172.16.1.1 255.255.255.0
!
interface Vlan30
 ip vrf forwarding Customer3
 ip address 10.1.1.1 255.255.255.0
```

Which configuration allows Customer2 hosts to access the FTP server of Customer1 that has the IP address of 192.168.1.200?

A. ip route vrf Customerl 172.16.1.0 255.255.255.0 172.16.1.1 globalip route vrf Customer 192.168.1.200 255.255.255.255 192.168.1.1 globalip route 192.168.1.0 255.255.255.0 VlanlOip route 172.16.1.0 255.255.255.0 Vlan20
B. ip route vrf Customerl 172.16.1.0 255.255.255.0 172.16.1.1 Customer2ip route vrf Customer 192.168.1.200 255.255.255.255 192.168.1.1 Customerl
C. ip route vrf Customerl 172.16.1.0 255.255.255.0 172.16.1.1 Customerlip route vrf Customer 192.168.1.200 255.255.255.255 192.168.1.1 Customer2
D. ip route vrf Customerl 172.16.1.1 255.255.255.255 172.16.1.1 globalip route vrf Customer 192.168.1.200 255.255.255.0 192.168.1.1 globalip route 192.168.1.0 255.255.255.0 VlanlOip route 172.16.1.0 255.255.255.0 Vlan20

Answer: A

NEW QUESTION 42
In an SD-Access solution what is the role of a fabric edge node?

A. to connect external Layer 3- network to the SD-Access fabric
B. to connect wired endpoint to the SD-Access fabric
C. to advertise fabric IP address space to external network
D. to connect the fusion router to the SD-Access fabric

Answer: B

Explanation:
+ Fabric edge node: This fabric device (for example, access or distribution layer device) connects

NEW QUESTION 47
How cloud deployments differ from on-prem deployments?

A. Cloud deployments require longer implementation times than on-premises deployments
B. Cloud deployments are more customizable than on-premises deployments.
C. Cloud deployments require less frequent upgrades than on-premises deployments.
D. Cloud deployments have lower upfront costs than on-premises deployments.

Answer: C

NEW QUESTION 48
Refer to the exhibit.
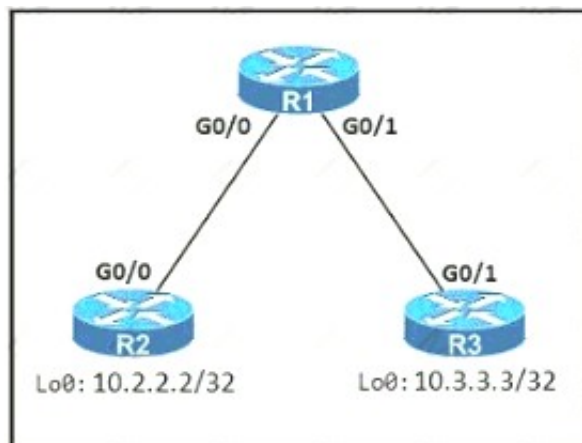
An engineer must deny Telnet traffic from the loopback interface of router R3 to the loopback interface of router R2 during the weekend hours. All other traffic between the loopback interfaces of routers R3 and R2 must be allowed at all times. Which command accomplish this task?

A)

```
R3(config)#time-range WEEKEND
R3(config-time-range)#periodic Saturday Sunday 00:00 to 23:59

R3(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R3(config)#access-list 150 permit ip any any time-range WEEKEND

R3(config)#interface G0/1
R3(config-if)#ip access-group 150 out
```

B)

```
R1(config)#time-range WEEKEND
R1(config-time-range)#periodic Friday Sunday 00:00 to 00:00

R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R1(config)#access-list 150 permit ip any any

R1(config)#interface G0/1
R1(config-if)#ip access-group 150 in
```

C)

```
R1(config)#time-range WEEKEND
R1(config-time-range)#periodic weekend 00:00 to 23:59

R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R1(config)#access-list 150 permit ip any any

R1(config)#interface G0/1
R1(config-if)#ip access-group 150 in
```

D)

```
R3(config)#time-range WEEKEND
R3(config-time-range)#periodic weekend 00:00 to 23:59

R3(config)#access-list 150 permit tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R3(config)#access-list 150 permit ip any any time-range WEEKEND

R3(config)#interface G0/1
R3(config-if)#ip access-group 150 out
```

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

Answer: C

Explanation:
We cannot filter traffic that is originated from the local router (R3 in this case) so we can only configure the ACL on R1 or R2. "Weekend hours" means from Saturday morning through Sunday night so we have to configure: "periodic weekend 00:00 to 23:59".
Note: The time is specified in 24-hour time (hh:mm), where the hours range from 0 to 23 and the minutes range from 0 to 59.
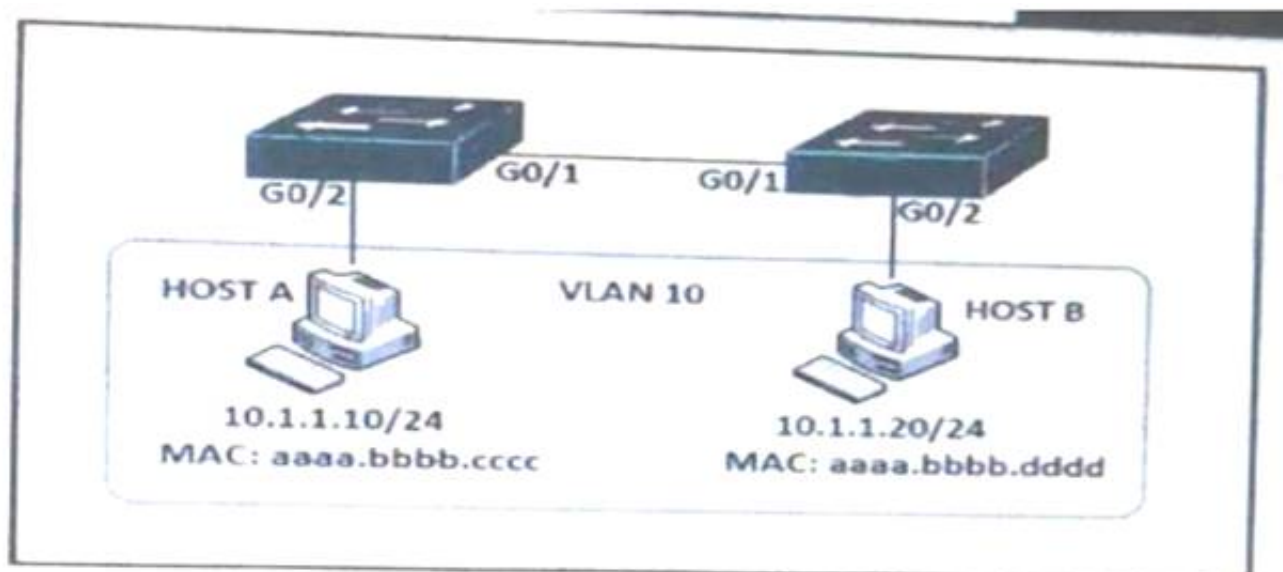
NEW QUESTION 51
A customer has several small branches and wants to deploy a WI-FI solution with local management using CAPWAP. Which deployment model meets this requirement?

A. Autonomous
B. Mobility Express
C. SD-Access wireless
D. Local mode

Answer: B

NEW QUESTION 56
Refer to the exhibit.

An engineer must deny HTTP traffic from host A to host V while allowing all other communication between the hosts, drag and drop the commands into the configuration to achieve these results. Some commands may be used more than once. Not all commands are used.

```
SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)# [          ] tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# ip access-list extended MATCH_ALL
SW1(config-ext-nacl)# [          ] ip any any

SW1(config)# vlan access-map HOST-A-B 10
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# [          ]

SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address MATCH_ALL
SW1(config-access-map)# [          ]

SW1(config)# vlan filter HOST-A-B vlan 10
```

| action drop | action forward | filter | permit | deny | match |

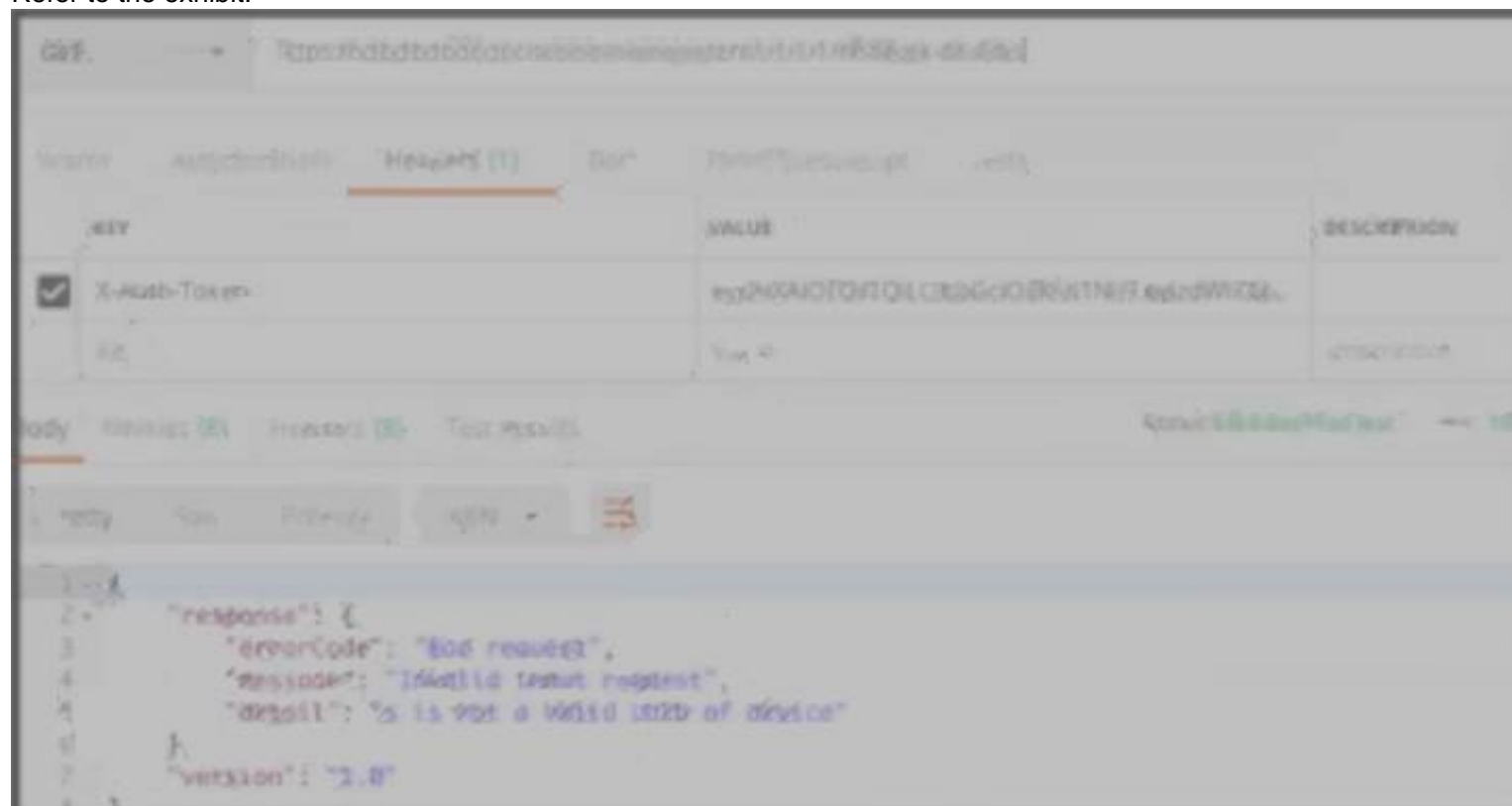A. Mastered
B. Not Mastered

Answer: A

Explanation:
Deny Permit Action drop
Action forward

NEW QUESTION 57
Refer to the exhibit.

POSTMAN is showing an attempt to retrieve network device information from Cisco DNA Center API. What is the issue?

A. The URI string is incorrect
B. The token has expired.
C. Authentication has failed
D. The JSON payload contains the incorrect UUID

Answer: D

NEW QUESTION 58
A network engineer is adding an additional 10Gps link to an exiting 2x10Gps LACP-based LAG to augment its capacity. Network standards require a bundle interface to be taken out of service if one of its member links goes down, and the new link must be added with minimal impact to the production network. Drag and drop the tasks that the engineer must perform from the left into the sequence on the right. Not all options are used.

Execute the channel-group number mode active command to add the 10Gbps link to the existing bundle.	step 1
Execute the channel-group number mode on command to add the 10Gbps link to the existing bundle.	step 2
Execute the lacp min-bundle 3 command to set the minimum number of ports threshold.	step 3
Validate the network layer of the 10Gbps link.	step 4
Execute the channel-group number mode auto command to add the 10Gbps link to the existing bundle.	
Validate the physical and data link layers of the 10Gbps link.	

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A picture containing diagram Description automatically generated

---

NEW QUESTION 63
Which protocol does REST API rely on to secure the communication channel?

A. TCP
B. HTTPS
C. SSH
D. HTTP

Answer: B

Explanation:
The REST API accepts and returns HTTP (not enabled by default) or HTTPS messages that contain JavaScript Object Notation (JSON) or Extensible Markup Language (XML) documents. You can use any programming language to generate the messages and the JSON or XML documents that contain the API methods or Managed Object (MO) descriptions.

NEW QUESTION 65
Which AP mode allows an engineer to scan configured channels for rogue access points?

A. sniffer
B. monitor
C. bridge
D. local

Answer: B

NEW QUESTION 70
Which entity is responsible for maintaining Layer 2 isolation between segments In a VXLAN environment?

A. switch fabric
B. VTEP
C. VNID
D. host switch

Answer: C

Explanation:

. The 24-bit VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments.

VXLAN uses an 8-byte VXLAN header that consists of a 24-bit VNID and a few reserved bits. The VXLAN header together with the original Ethernet frame goes in the UDP payload. The 24-bit VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments.

NEW QUESTION 75
If the noise floor is -90 dBm and wireless client is receiving a signal of -75 dBm, what is the SNR?

A. 15
B. 1.2
C. -165
D. .83

Answer: A

NEW QUESTION 79
What is the function of a fabric border node in a Cisco SD-Access environment?

A. To collect traffic flow information toward external networks
B. To connect the Cisco SD-Access fabric to another fabric or external Layer 3 networks
C. To attach and register clients to the fabric
D. To handle an ordered list of IP addresses and locations for endpoints in the fabric.

Answer: B

NEW QUESTION 81
Refer to the exhibit.

```
Router#sh| run | b vty

line vty 0 4
  session-timeout 30
  exec-timeout 20 0
  session-limit 30
  login local
line vty 5 15
  session-timeout 30
  exec-timeout 20 0
  session-limit 30
  login local
```

Security policy requires all idle-exec sessions to be terminated in 600 seconds. Which configuration achieves this goal?

A. line vty 0 15absolute-timeout 600
B. line vty 0 15 exec-timeout
C. line vty 01 5exec-timeout 10 0
D. line vty 0 4exec-timeout 600

Answer: B

NEW QUESTION 85
What does the cisco REST response indicate?

```
{
    "response": [
        {
            "family": "Routers",
            "interfaceCount": "12",
            "lineCardCount": "9",
            "platformId": "ASR1001-X",
            "reachabilityFailureReason": "",
            "reachabilityStatus": "Reachable",
            "hostname": "RouterASR-1",
            "macAddress": "00:c8:8b:80:bb:00",
        },
        {
            "family": "Switches and Hubs",
            "interfaceCount": "41",
            "lineCardCount": "2",
            "platformId": "C9300-24UX",
            "reachabilityFailureReason": "",
            "reachabilityStatus": "Authentication Failed",
            "hostname": "cat9000-1",
            "macAddress": "18:7b:20:67:62:80",
        },
        {
            "family": "Switches and Hubs",
            "interfaceCount": "50",
            "lineCardCount": "2",
            "platformId": "WS-C3850-48U-E",
            "reachabilityFailureReason": "",
            "reachabilityStatus": "Unreachable",
            "hostname": "cat3850-1",
            "macAddress": "cc:d8:c1:15:d2:80",
        }
    ],
    "version": "1.0"
}
```

A. Cisco DNA Center has the Incorrect credentials for cat3850-1
B. Cisco DNA Center is unable to communicate with cat9000-1
C. Cisco DNA Center has the incorrect credentials for cat9000-1
D. Cisco DNA Center has the Incorrect credentials for RouterASR-1

Answer: C

NEW QUESTION 89
What is a characteristic of a next-generation firewall?

A. only required at the network perimeter
B. required in each layer of the network
C. filters traffic using Layer 3 and Layer 4 information only
D. provides intrusion prevention

Answer: D

NEW QUESTION 91
What is the output of this code?

```
def get_credentials():
    creds={'username': 'cisco', 'password': 'c3577dc8ae4e36c0bfb6fe5398614245'}
    return (creds.get('username'))

print(get_credentials())
```

A. username Cisco
B. get_credentials
C. username
D. CISCO

Answer: D

NEW QUESTION 95
Drag and drop the snippets onto the blanks within the code to construct a script that configures BGP according to the topology. Not all options are used, and some options may be used twice.

```
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
    <router>
      <ios-bgp:bgp>
        <ios-bgp:id>[        ]</ios-bgp:id>
        <ios-bgp:neighbor>
          <ios-bgp:id>[        ]</ios-bgp:id>
          <ios-bgp:remote-as>[        ]</ios-bgp:remote-as>
        </ios-bgp:neighbor>
        <ios-bgp:address-family>
          <ios-bgp:no-vrf>
            <ios-bgp:ipv4>
              <ios-bgp:af-name>unicast</ios-bgp:af-name>
              <ios-bgp:ipv4-unicast>
                <ios-bgp:neighbor>
                  <ios-bgp:id>[        ]</ios-bgp:id>
                  <ios-bgp:soft-reconfiguration>inbound</ios-bgp:soft-reconfiguration>
                </ios-bgp:neighbor>
              </ios-bgp:ipv4-unicast>
            </ios-bgp:ipv4>
          </ios-bgp:no-vrf>
        </ios-bgp:address-family>
      </ios-bgp:bgp>
    </router>
  </native>
</config>
```

Client
IP 192.168.1.2
BGP AS 65001

ISP
IP 192.168.1.1
BGP AS 65000

[192.168.1.1] [192.168.1.2] [65000] [65001] [Client] [ISP]

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated

NEW QUESTION 99
Refer to the exhibit.

```
PYTHON CODE
import requests
import json

url='http://YOURIPins'
switchuser='USERID'
switchpassword='PASSWORD'

myheaders={'content-type':'application/json'}
payload={
  "ins_api":{
    "version":"1.0",
    "type":"cli_show",
    "chunk":"0",
    "sid":"1",
    "input":"show version",
    "output_format":"json"
  }
}

response = requests.post(url,data=json.dumps(payload), headers=myheaders,auth=(switchuser,switchpassword)).json()

print(response['ins_api']['outputs']['output']['body']['kickstart_ver_str'])
```

```
HTTP JSON Response
{
  "ins_api": {
    "type": "cli_show",
    "version": "1.0",
    "sid": "eoc",
    "outputs": {
      "output": {
        "input": "show version",
        "msg": "Success",
        "code": "200",
        "body": {
          "bios_ver_str": "07.61",
          "kickstart_ver_str": "7.0(3)I7(4)",
          "bios_cmpl_time": "04/06/2017",
          "kick_file_name": "bootflash:///nxos.7.0.3.I7.4.bin",
          "kick_cmpl_time": " 6/14/1970 2:00:00",
          "kick_tmstmp": "06/14/1970 09:49:04",
          "chassis_id": "Nexus9000 93180YC-FX chassis",
          "cpu_name": "Intel(R) Xeon(R) CPU  @ 1.80GHz",
          "memory": 24633488,
          "mem_type": "kB",
          "rr_usecs": 134703,
          "rr_ctime": "Sun Mar 10 15:41:46 2019",
          "rr_reason": "Reset Requested by CLI command reload",
          "rr_sys_ver": "7.0(3)I7(4)",
          "rr_service": "",
          "manufacturer": "Cisco Systems, Inc.",
          "TABLE_package_list": {
            "ROW_package_list": {
              "package_id": {}
            }
          }
        }
      }
    }
  }
}
```

Which HTTP JSON response does the python code output give?

A. NameError: name 'json' is not defined
B. KeyError 'kickstart_ver_str'
C. 7.61
D. 7.0(3)I7(4)

Answer: D

NEW QUESTION 100
Which method creates an EEM applet policy that is registered with EEM and runs on demand or manually?

A. event manager applet ondemand event registeraction 1.0 syslog priority critical msg 'This is a message from ondemand'
B. event manager applet ondemand event manualaction 1.0 syslog priority critical msg 'This is a message from ondemand'
C. event manager applet ondemand event noneaction 1.0 syslog priority critical msg 'This is a message from ondemand'
D. event manager applet ondemandaction 1.0 syslog priority critical msg 'This is a message from ondemand'

Answer: C

Explanation:
An EEM policy is an entity that defines an event and the actions to be taken when that event occurs. There are two types of EEM policies: an applet or a script. An

applet is a simple form of policy that is defined within the CLI configuration. answer 'event manager applet ondemand event register
action 1.0 syslog priority critical msg 'This is a message from ondemand'
<="" p="" style="box-sizing: border-box;">
There are two ways to manually run an EEM policy. EEM usually schedules and runs policies on the basis of an event specification that is contained within the
policy itself. The event none command allows EEM to identify an EEM policy that can be manually triggered. To run the policy, use either the action policy
command in applet configuration mode or the event manager run command
in privileged EXEC mode.

NEW QUESTION 104
Refer to the exhibit.
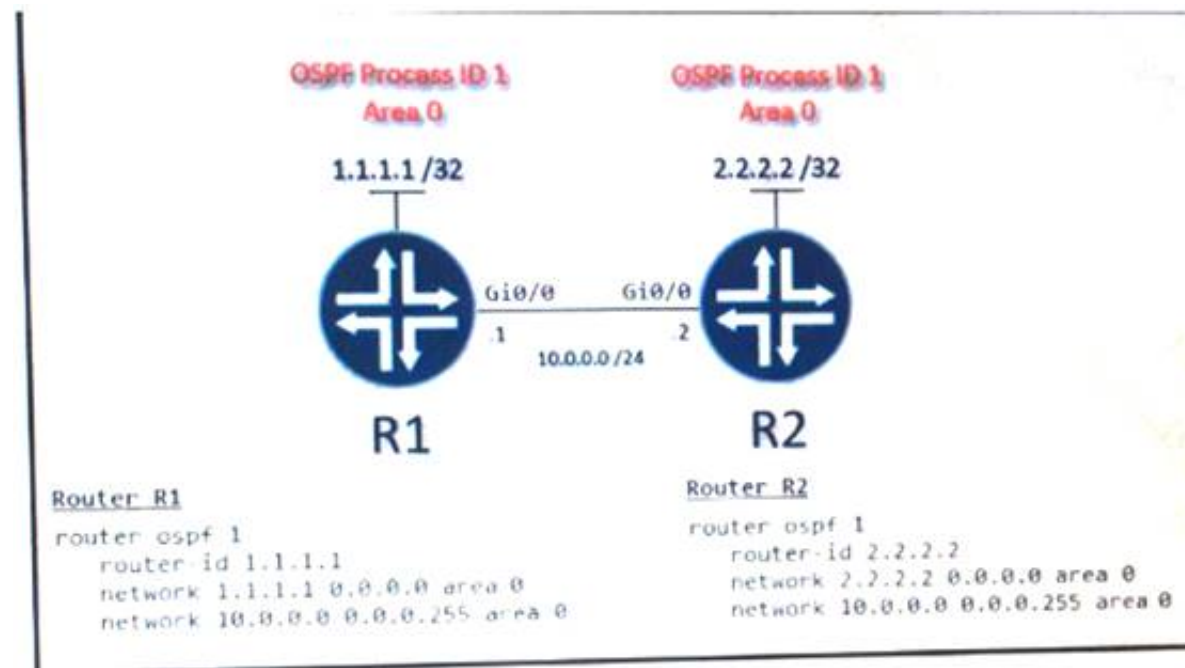
A network engineer is configuring OSPF between router R1 and router R2. The engineer must ensure that a DR/BDR election does not occur on the Gigabit
Ethernet interfaces in area 0. Which configuration set accomplishes this goal?

A)
```
R1(config-if)interface Gi0/0
R1(config-if)ip ospf network point-to-point

R2(config-if)interface Gi0/0
R2(config-if)ip ospf network point-to-point
```

B)
```
R1(config-if)interface Gi0/0
R1(config-if)ip ospf network broadcast

R2(config-if)interface Gi0/0
R2(config-if)ip ospf network broadcast
```

C)
```
R1(config-if)interface Gi0/0
R1(config-if)ip ospf database-filter all out

R2(config-if)interface Gi0/0
R2(config-if)ip ospf database-filter all out
```

D)
```
R1(config-if)interface Gi0/0
R1(config-if)ip ospf priority 1

R2(config-if)interface Gi0/0
R2(config-if)ip ospf priority 1
```

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

Answer: A

Explanation:
Broadcast and Non-Broadcast networks elect DR/BDR while Point-topoint/ multipoint do not elect DR/BDR. Therefore we have to set the two Gi0/0
interfaces to point-to-point or point-to-multipoint network to ensure that a DR/BDR election does not occur.

NEW QUESTION 106
What is a characteristic of MACsec?

A. 802.1AE provides encryption and authentication services
B. 802.1AE is bult between the host and switch using the MKA protocol, which negotiates encryption keys based on the master session key from a successful
802.1X session

C. 802.1AE is bult between the host and switch using the MKA protocol using keys generated via the Diffie-Hellman algorithm (anonymous encryption mode)
D. 802.1AE is negotiated using Cisco AnyConnect NAM and the SAP protocol

Answer: A

Explanation:
MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1x Extensible Authentication Protocol (EAP-TLS) or Pre Shared Key (PSK) framework.

NEW QUESTION 107
Which three elements determine Air Time efficiency? (Choose three)

A. evert-driven RRM
B. data rate (modulation density) or QAM
C. channel bandwidth
D. number of spatial streams and spatial reuse
E. RF group leader
F. dynamic channel assignment

Answer: ACE

NEW QUESTION 108
Which HTTP code must be returned to prevent the script form exiting?

```
def get_token () :
    device_uri = "https://192.168.1.1/dna/system/api/v1/auth/token"
    http_result = requests.post(device_uri, auth = ["test", "test398810436!"] )
    if http_result.status_code != requests.codes.ok:
        print ("Call failed! Review get_token () . ")
        sys.exit ()
    return (http_result.json () ["Token"] )
```

A. 200
B. 201
C. 300
D. 301

Answer: D

NEW QUESTION 111
In cisco SD_WAN, which protocol is used to measure link quality?

A. OMP
B. BFD
C. RSVP
D. IPsec

Answer: B

NEW QUESTION 112
Refer to the exhibit.

```
Person#1:
First Name is Johnny
Last Name is Table
Hobbies are:
• Running
• Video games

Person#2:
First Name is Billy
Last Name is Smith
Hobbies are:
• Napping
• Reading
```

Which JSON syntax is derived from this data?
A)

```
([{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': ['Running', 'Video games']}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': ['Napping', 'Reading']}])
```

B)

```
{'Person': [{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': 'Running', 'Video games'}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': 'Napping', 'Reading']}]}
```

C)

{[{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': 'Running', 'Hobbies': 'Video games'}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': 'Napping', 'Hobbies': 'Reading'}]}

D)

{'Person' [{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': ['Running', 'Video games']}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': ['Napping', 'Reading']}]}

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

Answer: D

NEW QUESTION 117
"HTTP/1.1 204 content" is returned when cur –I –x delete command is issued. Which situation has occurred?

A. The object could not be located at the URI path.
B. The command succeeded in deleting the object
C. The object was located at the URI, but it could not be deleted.
D. The URI was invalid

Answer: B

NEW QUESTION 122
Drag and drop the characteristics from the left onto the routing protocols they describe on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Diagram Description automatically generated

NEW QUESTION 123
Refer to the exhibit.

An engineer must block all traffic from a router to its directly connected subnet 209.165.200.0/24. The engineer applies access control list EGRESS in the outbound direction on the GigabitEthernet0/0 interface of the router However, the router can still ping hosts on the 209.165.200.0/24 subnet. Which explanation of this behavior is true?

A. Access control lists that are applied outbound to a router interface do not affect traffic that is sourced from the router.
B. Only standard access control lists can block traffic from a source IP address.

C. After an access control list is applied to an interface, that interface must be shut and no shut for the access control list to take effect.
D. The access control list must contain an explicit deny to block traffic from the router.

Answer: A

NEW QUESTION 125
Refer to the exhibit.
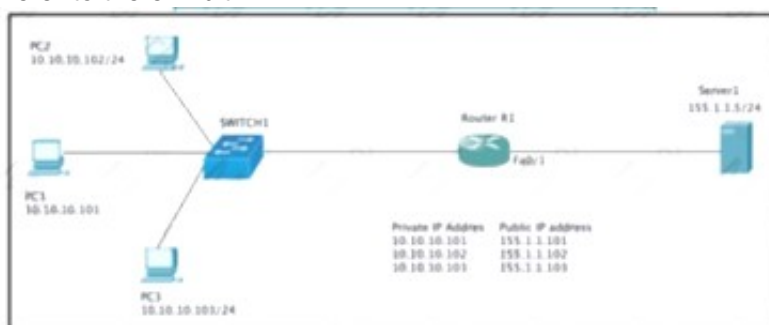
Which set of commands on router r R1 Allow deterministic translation of private hosts PC1, PC2, and PC3 to addresses in the public space?

A)
```
RouterR1(config)#int f0/0
RouterR1(config-if)#ip nat inside
RouterR1(config-if)#exit
RouterR1(config)#int f0/1
RouterR1(config-if)#ip nat outside
RouterR1(config-if)#exit
RouterR1(config)#ip nat inside source static 10.10.10.101 155.1.1.101
RouterR1(config)#ip nat inside source static 10.10.10.102 155.1.1.102
RouterR1(config)#ip nat inside source static 10.10.10.103 155.1.1.103
```

B)
```
RouterR1(config)#int f0/0
RouterR1(config-if)#ip nat inside
RouterR1(config-if)#exit
RouterR1(config)#int f0/1
RouterR1(config-if)#ip nat outside
RouterR1(config-if)#exit
RouterR1(config)#ip nat inside source static 10.10.10.101 155.1.1.101
RouterR1(config)#ip nat inside source static 10.10.10.102 155.1.1.102
RouterR1(config)#ip nat inside source static 10.10.10.103 155.1.1.103
```

C)
```
RouterR1(config)#int f0/0
RouterR1(config-if)#ip nat inside
RouterR1(config-if)#exit
RouterR1(config)#int f0/1
RouterR1(config-if)#ip nat outside
RouterR1(config-if)#exit
RouterR1(config)#access-list 1 10.10.10.0 0.0.0.255
RouterR1(config)ip nat pool POOL 155.1.1.101 155.1.1.103 netmask 255.255.255.0
RouterR1(config)ip nat inside source list 1 pool POOL
```

D)
```
RouterR1(config)#int f0/0
RouterR1(config-if)#ip nat inside
RouterR1(config-if)#exit
RouterR1(config)#int f0/1
RouterR1(config-if)#ip nat outside
RouterR1(config-if)#exit
RouterR1(config)#access-list 1 10.10.10.0 0.0.0.255
RouterR1(config)ip nat inside source list 1 interface f0/1 overload
```

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

Answer: A

NEW QUESTION 128
Refer to the exhibit.

```
Device# configure terminal
Device(config)# netconf ssh acl 1
Device(config)# netconf lock-time 100
Device(config)# netconf max-sessions 1
Device(config)# netconf max-message 10
```

A network engineer must configure NETCONF. After creating the configuration, the engineer gets output from the command show line, but not from show running-config. Which command completes the configuration?

- Device(config)# **netconf lock-time 500**
- Device(config)# **netconf max-message 1000**
- Device(config)# **no netconf ssh acl 1**
- Device(config)# **netconf max-sessions 100**

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

Answer: C

NEW QUESTION 132
What is used to perform OoS packet classification?

A. the Options field in the Layer 3 header
B. the Type field in the Layer 2 frame
C. the Flags field in the Layer 3 header
D. the TOS field in the Layer 3 header

Answer: D

NEW QUESTION 137
Refer to the exhibit.

```
<rpc-reply> [0, 1] required
    <ok> [0, 1] required
    <data> [0, 1] required
    <rpc-error> [0, 1] required
     <error-type> [0, 1] required
     <error-tag> [0, 1] required
     <error-severity> [0, 1] required
     <error-app-tag> [0, 1] required
     <error-path> [0, 1] required
     <error-message> [0, 1] required
     <error-info> [0, 1] required
      <bad-attribute> [0, 1] required
      <bad-element> [0, 1] required
      <ok-element> [0, 1] required
      <err-element> [0, 1] required
      <noop-element> [0, 1] required
      <bad-namespace> [0, 1] required
      <session-id> [0, 1] required
```

Which command is required to verify NETCONF capability reply messages?

A. show netconf | section rpc-reply
B. show netconf rpc-reply
C. show netconf xml rpc-reply
D. show netconf schema | section rpc-reply

Answer: A

NEW QUESTION 138
When using TLS for syslog, which configuration allows for secure and reliable transportation of messages to its default port?

A. logging host 10.2.3.4 vrf mgmt transport tcp port 6514
B. logging host 10.2.3.4 vrf mgmt transport udp port 6514
C. logging host 10.2.3.4 vrf mgmt transport tcp port 514
D. logging host 10.2.3.4 vrf mgmt transport udp port 514

Answer: A

Explanation:
The TCP port 6514 has been allocated as the default port for syslog over Transport Layer Security (TLS).

NEW QUESTION 140
How is MSDP used to interconnect multiple PIM-SM domains?

A. MSDP depends on BGP or multiprotocol BGP for mterdomam operation
B. MSDP SA request messages are used to request a list of active sources for a specific group
C. SDP allows a rendezvous point to dynamically discover active sources outside of its domain
D. MSDP messages are used to advertise active sources in a domain

Answer: A

NEW QUESTION 143
What is a benefit of a virtual machine when compared with a physical server?

A. Multiple virtual servers can be deployed on the same physical server without having to buy additional hardware.
B. Virtual machines increase server processing performance.
C. The CPU and RAM resources on a virtual machine cannot be affected by other virtual machines.
D. Deploying a virtual machine is technically less complex than deploying a physical server.

Answer: A

NEW QUESTION 148
Refer to the exhibit.
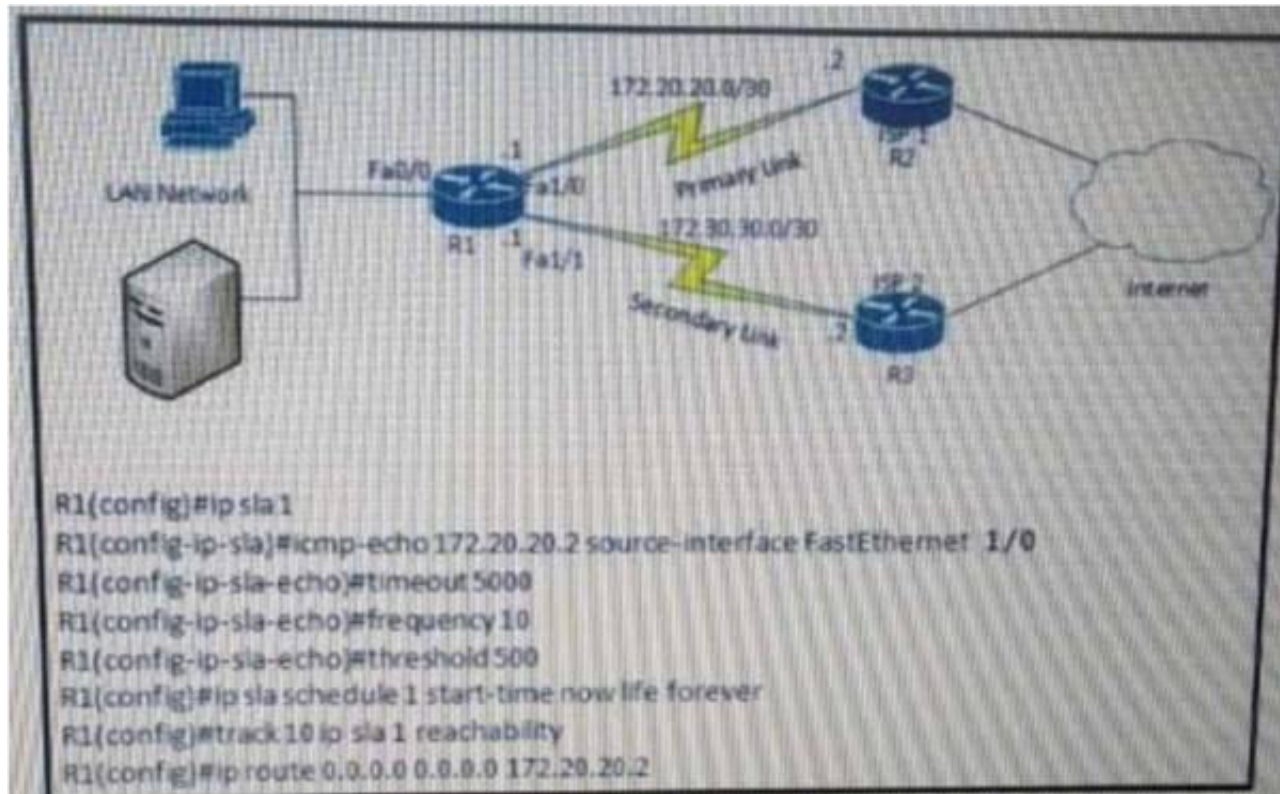
After implementing the configuration 172.20.20.2 stops replaying to ICMP echoes, but the default route fails to be removed. What is the reason for this behavior?

A. The source-interface is configured incorrectly.
B. The destination must be 172.30.30.2 for icmp-echo
C. The default route is missing the track feature
D. The threshold value is wrong.

Answer: C

Explanation:
The last command should be "R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2 track 10".

NEW QUESTION 149
An engineer must configure HSRP group 300 on a Cisco IOS router. When the router is functional, it must be the must be the active HSRP router. The peer router has been configured using the default priority value. Which command set is required?
A)

```
standby 300 priority 110
standby 300 timers 1 110
```

B)

```
standby version 2
standby 300 priority 110
standby 300 preempt
```

C)

```
standby 300 priority 90
standby 300 preempt
```

D)

```
standby version 2
standby 300 priority 90
standby 300 preempt
```

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

Answer: B

NEW QUESTION 153
Which line must be added in the Python function to return the JSON object {"cat_9k": "FXS193202SE")?

```
import json
def get_data():
    test_json = """
    {
        "response": [{
        "managementIpAddress": "10.10.2.253",
        "memorySize": "3398345152",
        "serialNumber": "FXS1932Q2SE",
        "softwareVersion": "16.3.2",
        "hostname": "cat_9k"
        }],
        "version": "1.0"
    }
    """
```

A)

```
return (json.dumps({d['hostname']: d['serialNumber'] for d in json.loads(test_json)['response']}))
```

B)

```
return (json.dumps({for d in json.loads(test_json)['response']: d['hostname']: d['serialNumber']}))
```

C)

```
return (json.loads({d['hostname']: d['serialNumber'] for d in json.dumps(test_json)['response']}))
```

D)

```
return (json.loads({for d in json.dumps(test_json)['response']: d['hostname']: d['serialNumber']}))
```

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

Answer: D

NEW QUESTION 155
An engineer runs the code against an API of Cisco DMA Center, and the platform returns this output What does the response indicate?

```
import requests
import sys
import urllib3

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

def main():
    device_uri = "https://192.168.1.1/dna/system/api/v1/auth/token"
    http_result = requests.get(device_uri, auth=("root", "test398586070!"))
    print(http_result)
    if http_result.status_code != requests.codes.ok:
        print("Call failed! Review get_token() . ")
        sys.exit()
    print(http_result.json()["Token"])

if _name_ == "_main_":
    sys.exit(main())
```
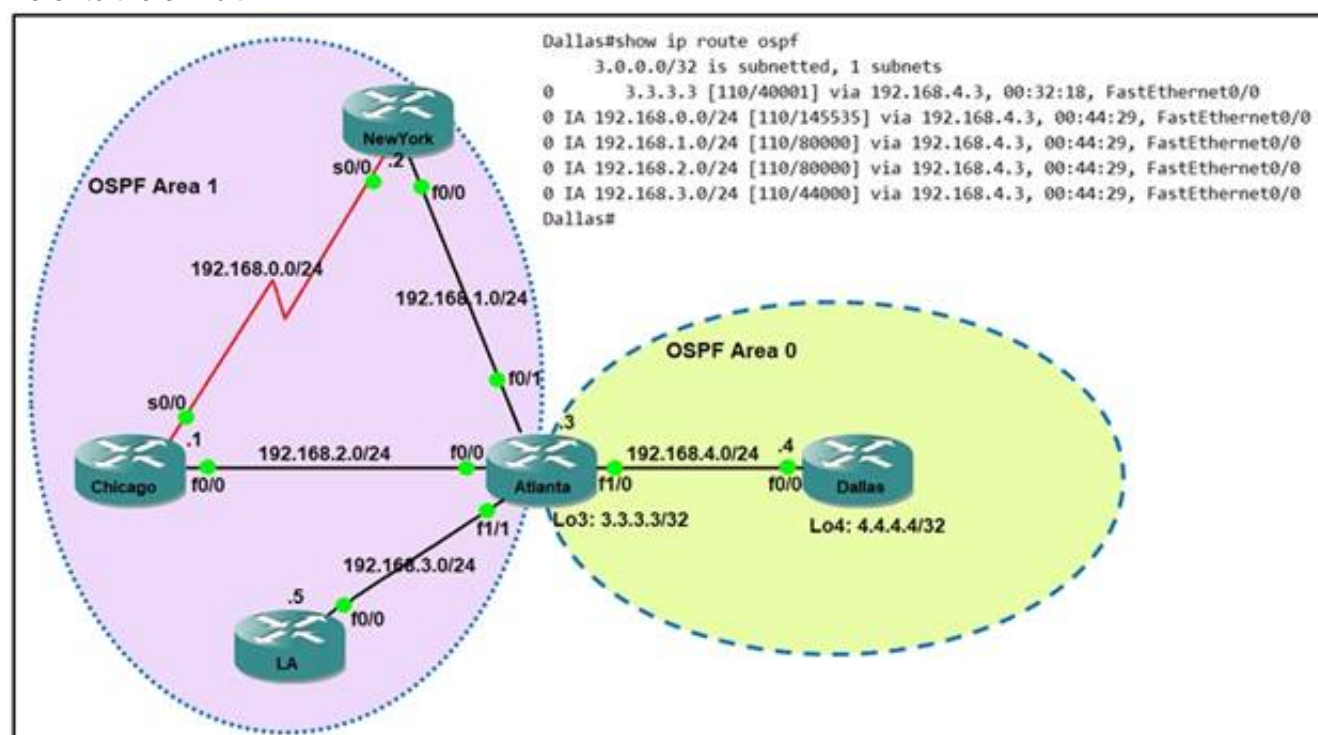
Output
```
$ python get_token.py
<Response [405]>
Call failed! Review get_token ().
```

A. The authentication credentials are incorrect
B. The URI string is incorrect.
C. The Cisco DNA Center API port is incorrect
D. The HTTP method is incorrect

Answer: A

NEW QUESTION 158
Refer to the exhibit.


```
Dallas#show ip route ospf
       3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/40001] via 192.168.4.3, 00:32:18, FastEthernet0/0
O IA 192.168.0.0/24 [110/145535] via 192.168.4.3, 00:44:29, FastEthernet0/0
O IA 192.168.1.0/24 [110/80000] via 192.168.4.3, 00:44:29, FastEthernet0/0
O IA 192.168.2.0/24 [110/80000] via 192.168.4.3, 00:44:29, FastEthernet0/0
O IA 192.168.3.0/24 [110/44000] via 192.168.4.3, 00:44:29, FastEthernet0/0
Dallas#
```

Which command when applied to the Atlanta router reduces type 3 LSA flooding into the backbone area and summarizes the inter-area routes on the Dallas router?

A. Atlanta(config-route)#area 0 range 192.168.0.0 255.255.248.0
B. Atlanta(config-route)#area 0 range 192.168.0.0 255.255.252.0
C. Atlanta(config-route)#area 1 range 192.168.0.0 255.255.252.0
D. Atlanta(config-route)#area 1 range 192.168.0.0 255.255.248.0

Answer: C

NEW QUESTION 163
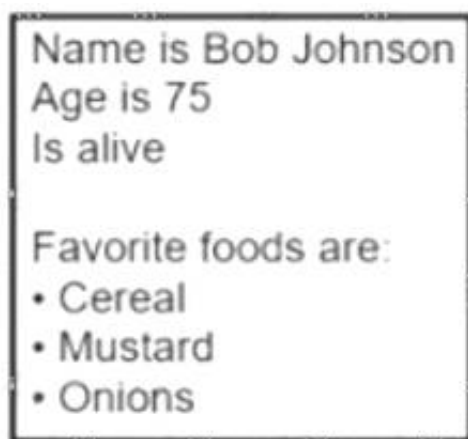Which congestion queuing method on Cisco IOS based routers uses four static queues?

A. Priority
B. custom
C. weighted fair
D. low latency

Answer: A

NEW QUESTION 167
Refer to the exhibit.

```
Name is Bob Johnson
Age is 75
Is alive

Favorite foods are:
• Cereal
• Mustard
• Onions
```

What is the Json syntax that is formed from the data?

A. Name: Bob Johnson, Age: 75, Alive': true, Favourite Foods: [Cereal, Mustard, Onions]}
B. Name: Bob Johnson, Age: 75, Alive': true, Favourite Foods: Cereal Mustard Onions
C. Name: Bob Johnson, Age: 75, Alive': true, Favourite Foods: ['Cereal'', ''Mustard'', ''Onions']}
D. Name: Bob Johnson, Age: seventy-five, Alive': true, Favourite Foods: [Cereal, Mustard, Onions]}

Answer: C

Explanation:

```
1 ▼ {
2       "Name": "Bob Johnson",
3       "Age": 75,
4       "Alive": true,
5       "Favorite Foods": ["Cereal", "Mustard", "Onions"]
6   }
```

Results

```
valid JSON
```

NEW QUESTION 169
An engineer has deployed a single Cisco 5520 WLC with a management IP address of 172.16.50.5/24. The engineer must register 50 new Cisco AIR-CAP2802I-E-K9 access points to the WLC using DHCP option 43. The access points are connected to a switch in VLAN 100 that uses the 172.16.100.0/24 subnet. The engineer has configured the DHCP scope on the switch as follows:

```
Network 172.16.100.0 255.255.255.0
Default Router 172.16.100.1
Option 43 Ascii 172.16.50.5
```

The access points are failing to join the wireless LAN controller. Which action resolves the issue?

A. configure option 43 Hex F104.AC10.3205
B. configure option 43 Hex F104.CA10.3205
C. configure dns-server 172.16.50.5
D. configure dns-server 172.16.100.1

Answer: B

NEW QUESTION 172
The login method is configured on the VTY lines of a router with these parameters

⟩ The first method for authentication it TACACS

⟩ If TACACS is unavailable login is allowed without any provided credentials
Which configuration accomplishes this task?

```
  R1#sh run | include aaa
  aaa new-model
  aaa authentication login default group tacacs+
  aaa session-id common

  R1#sh run | section vty
  line vty 0 4
    transport input none
  R1#


  R1#sh run | include aaa
  aaa new-model
  aaa authentication login default group tacacs+ none
  aaa session-id common

  R1#sh run | section vty
  line vty 0 4
    password 7 02050D480809

  R1#sh run | include username
  R1#


  R1#sh run | include aaa
  aaa new-model
  aaa authentication login telnet group tacacs+ none
  aaa session-id common

  R1#sh run | section vty
  line vty 0 4

  R1#sh run | include username
  R1#


  R1#sh run | include aaa
  aaa new-model
  aaa authentication login VTY group tacacs+ none
  aaa session-id common

  R1#sh run | section vty
  line vty 0 4
    password 7 02050D480809

  R1#sh run | include username
  R1#
```

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

Answer: B

NEW QUESTION 176
Which JSON syntax is valid?
A)

{"switch": "name": "dist1", "interfaces": ["gig1", "gig2", "gig3"]}

B)

{"switch": ("name": "dist1", "interfaces": ["gig1", "gig2", "gig3"])}

C)

{"switch". {"name". "dist1", "interfaces". ["gig1", "gig2", "gig3"]}}

D)

{/"switch/": {/"name/": "dist1", /"interfaces/": ["gig1", "gig2", "gig3"]}}

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

Answer: C

Explanation:
This JSON can be written as follows:
{
'switch': { 'name': 'dist1',
'interfaces': ['gig1', 'gig2', 'gig3']
}
}

NEW QUESTION 181
After a redundant route processor failure occurs on a Layer 3 device, which mechanism allows for packets to be forwarded from a neighboring router based on the most recent tables?

A. BFD
B. RPVST+
C. RP failover
D. NSF

Answer: D

NEW QUESTION 182
What is one benefit of implementing a VSS architecture?

A. It provides multiple points of management for redundancy and improved support
B. It uses GLBP to balance traffic between gateways.
C. It provides a single point of management for improved efficiency.
D. It uses a single database to manage configuration for multiple switches

Answer: D

NEW QUESTION 185
Which device makes the decision for a wireless client to roam?

A. wireless client
B. wireless LAN controller
C. access point
D. WCS location server

Answer: A

NEW QUESTION 186
In a Cisco SD-Access solution, what is the role of the Identity Services Engine?

A. It is leveraged for dynamic endpoint to group mapping and policy definition.
B. It provides GUI management and abstraction via apps that share context.
C. it is used to analyze endpoint to app flows and monitor fabric status.
D. It manages the LISP EID database.

Answer: A

NEW QUESTION 189
Refer to me exhibit.

```
%OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.2 on FastEthernet0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
%OSPF-6-AREACHG: 10.0.0.1/32 changed from area 0 to area 1
%OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from
backbone area must be virtual-link but not found from 10.0.0.2,
FastEthernet0/0
```

What is the cause of the log messages?

A. hello packet mismatch
B. OSPF area change
C. MTU mismatch
D. IP address mismatch

Answer: B

NEW QUESTION 193
Which TCP setting is tuned to minimize the risk of fragmentation on a GRE/IP tunnel?

A. MTU
B. Window size
C. MRU
D. MSS

Answer: D

Explanation:
The TCP Maximum Segment Size (TCP MSS) defines the maximum amount of data that a host
is willing to accept in a single TCP/IP datagram. This TCP/IP datagram might be fragmented at the IP layer. The MSS value is sent as a TCP header option only in TCP SYN segments. Each side of a TCP connection reports its MSS value to the other side. Contrary to popular belief, the MSS value is not negotiated between hosts. The sending host is required to limit the size of data in a single TCP segment to a value less than or equal to the MSS reported by the receiving host.
TCP MSS takes care of fragmentation at the two endpoints of a TCP connection, but it does not handle the case where there is a smaller MTU link in the middle between these two endpoints. PMTUD was developed in order to avoid fragmentation in the path between the endpoints. It is

NEW QUESTION 196
Refer to the exhibit.

```
access-list 100 permit gre host 209.165.201.1 host 209.165.201.6          access-list 100 permit gre host 209.165.201.6 host 209.165.201.1

crypto isakmp policy 5                                                     crypto isakmp policy 5
authentication pre-share                                                  authentication pre-share
hash sha256                                                               hash sha256
encryption aes                                                            encryption aes
group 14                                                                  group 14

crypto isakmp key D@t@c3nt3r address 209.165.201.6                         crypto isakmp key D@t@c3nt3 address 209.165.201.1

crypto ipsec transform-set My_Set esp-aes esp-sha-hmac                     crypto ipsec transform-set My_Set esp-aes esp-sha-hmac
mode transport                                                            mode transport

crypto map MAP 10 ipsec-isakmp                                            crypto map MAP 10 ipsec-isakmp
 set peer 209.165.201.6                                                    set peer 209.165.201.1
 set transform-set My_Set                                                  set transform-set My_Set
 match address 100                                                         match address 100

interface GigabitEthernet0/0                                              Interface GigabitEthernet0/1
description outside_interface                                             description outside_interface
 no switchport                                                             no switchport
 ip address 209.165.201.1 255.255.255.252                                  ip address 209.165.201.6 255.255.255.252
 crypto map MAP                                                            crypto map MAP

interface Tunnel100                                                       interface Tunnel100
ip address 192.168.100.1 255.255.255.0                                    ip address 192.168.100.2 255.255.255.0
ip mtu 1400                                                               ip mtu 1400
tunnel source GigabitEthernet0/0                                          tunnel source GigabitEthernet0/1
tunnel destination 209.165.201.6                                          tunnel destination 209.165.201.1

ip route 10.20.0.0 255.255.255.0  192.168.100.2 Tunnel100                 ip route 10.10.0.0 255.255.255.0 192.168.100.1 Tunnel100
```


A network engineer must simplify the IPsec configuration by enabling IPsec over GRE using IPsec profiles. Which two configuration changes accomplish this? (Choose two).

A. Apply the crypto map to the tunnel interface and change the tunnel mode to tunnel mode ipsec ipv4.
B. Create an IPsec profile, associate the transform-se
C. and apply the profile to the tunnel interface.
D. Remove the crypto map and modify the ACL to allow traffic between 10.10.0.0/24 to 10.20.0.0/24.
E. Remove all configuration related to crypto map from R1 and R2 and eliminate the ACL |>]
F. Create an IPsec profile, associate the transform-set AC
G. and apply the profile to the tunnel interface

Answer: AD

NEW QUESTION 197
Which two components are supported by LISP? (Choose two.)

A. Proxy ETR
B. egress tunnel router
C. route reflector
D. HMAC algorithm
E. spoke

Answer: AB

NEW QUESTION 200
Drag and drop the REST API authentication methods from the left onto their descriptions on the right.

Answer Area

HTTP basic authentication	public API resource
OAuth	username and password in an encoded string
secure vault	authorization through identity provider

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A close-up of a graph Description automatically generated with low confidence

NEW QUESTION 201
Refer to the exhibit.

```
Tunnel100 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.200.1/24
  MTU 17912 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive set (10 sec), retries 3
  Tunnel source 209.165.202.129 (GigabitEthernet0/1)
  Tunnel Subblocks:
    src-track:
      Tunnel100 source tracking subblock associated with GigabitEthernet0/1
      Set of tunnels with source GigabitEthernet0/1, 1 members (includes iterators), on interface <OK>
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
```

A network engineer configures a GRE tunnel and enters the show Interface tunnel command. What does the output confirm about the configuration?

A. The keepalive value is modified from the default value.
B. Interface tracking is configured.
C. The tunnel mode is set to the default.
D. The physical interface MTU is 1476 bytes.

Answer: C

NEW QUESTION 205
What does Call Admission Control require the client to send in order to reserve the bandwidth?

A. SIP flow information
B. Wi-Fi multimedia
C. traffic specification
D. VoIP media session awareness

Answer: D

NEW QUESTION 208
Which two mechanisms are available to secure NTP? (Choose two.)

A. IP prefix list-based
B. IPsec
C. TACACS-based authentication
D. IP access list-based
E. Encrypted authentication

Answer: DE

NEW QUESTION 210
In an SD-WAN deployment, which action in the vSmart controller responsible for?

A. handle, maintain, and gather configuration and status for nodes within the SD-WAN fabric
B. distribute policies that govern data forwarding performed within the SD-WAN fabric
C. gather telemetry data from vEdge routers
D. onboard vEdge nodes into the SD-WAN fabric

Answer: B

NEW QUESTION 213
Which component of the Cisco Cyber Threat Defense solution provides user and flow context analysis?

A. Cisco Firepower and FireSIGHT
B. Cisco Stealth watch system
C. Advanced Malware Protection
D. Cisco Web Security Appliance

Answer: B

NEW QUESTION 215
What are two differences between the RIB and the FIB? (Choose two.)

A. The FIB is derived from the data plane, and the RIB is derived from the FIB.
B. The RIB is a database of routing prefixes, and the FIB is the Information used to choose the egress interface for each packet.
C. FIB is a database of routing prefixes, and the RIB is the information used to choose the egress interface for each packet.
D. The FIB is derived from the control plane, and the RIB is derived from the FIB.
E. The RIB is derived from the control plane, and the FIB is derived from the RIB.

Answer: BE

NEW QUESTION 219
What is the differences between TCAM and the MAC address table?

A. The MAC address table is contained in CAM ACL and QoS information is stored in TCAM
B. The MAC address table supports partial match
C. TCAM requires an exact match
D. Router prefix lookups happens in CA
E. MAC address table lookups happen in TCAM.
F. TCAM is used to make Layer 2 forwarding decisions CAM is used to build routing tables

Answer: A

Explanation:
https://community.cisco.com/t5/networking-documents/cam-content-addressable-memory-vs-tcam-ternary-conte When using Ternary Content Addressable Memory (TCAM) inside routers it's used for faster address
lookup that enables fast routing.
In switches Content Addressable Memory (CAM) is used for building and lookup of mac address table that enables L2 forwarding decisions.
Besides Longest-Prefix Matching, TCAM in today's routers and multilayer Switch devices are used to store ACL, QoS and other things from upper-layer
processing.

NEW QUESTION 222
Refer to the exhibit.


```
Router# traceroute 10.10.10.1

Type escape sequence to abort.
Tracing the route to 10.10.10.1

1  10.0.0.1  5 msec  5 msec  5 msec
2  10.5.0.1  15 msec  17 msec  17 msec
3  10.10.10.1  *  *  *
```
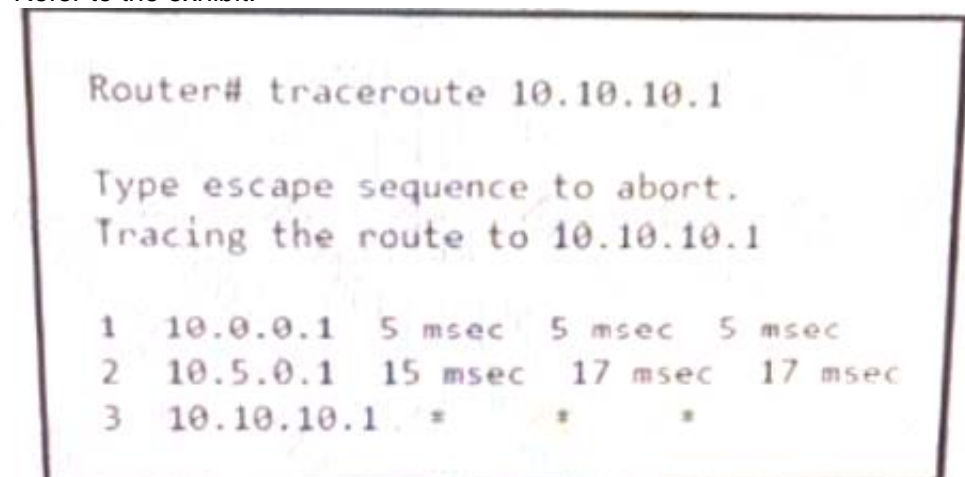
An engineer is troubleshooting a connectivity issue and executes a traceroute. What does the result confirm?

A. The destination server reported it is too busy
B. The protocol is unreachable
C. The destination port is unreachable
D. The probe timed out

Answer: B

NEW QUESTION 225
Drag and drop the solutions that comprise Cisco Cyber Threat Defense from the left onto the objectives they accomplish on the right.

StealthWatch	detects suspicious web activity
Identity Services Engine	analyzes network behavior and detects anomalies
Web Security Appliance	uses pxGrid to remediate security threats

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated with medium confidence

NEW QUESTION 230
Refer to the exhibit.

```
aaa new-model
aaa authentication login authorizationlist tacacs+
tacacs-server host 192.168.0.202
tacacs-server key ciscotestkey
line vty 0 4
login authentication authorizationlist
```

What is the effect of this configuration?

A. When users attempt to connect to vty lines 0 through 4, the device will authenticate them against TACACS+ if local authentication fails
B. The device will authenticate all users connecting to vty lines 0 through 4 against TACACS+
C. The device will allow users at 192.168.0.202 to connect to vty lines 0 through 4 using the password ciscotestkey
D. The device will allow only users at 192.166.0.202 to connect to vty lines 0 through 4

Answer: B

NEW QUESTION 235
Refer to the exhibit.
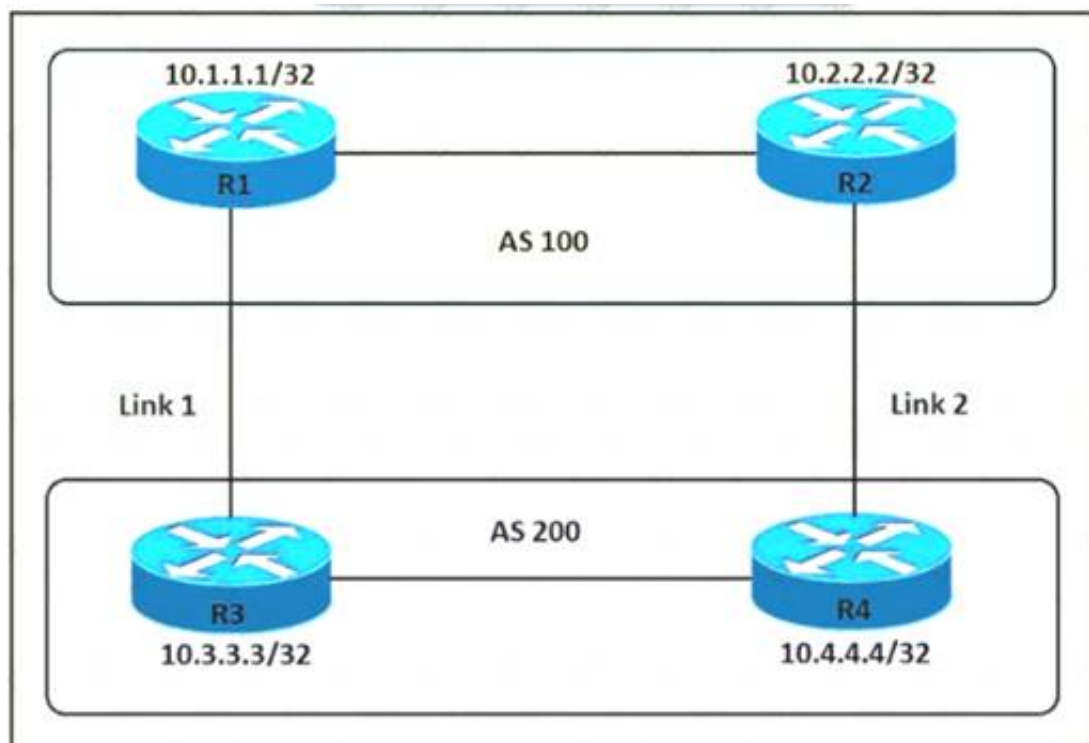
An engineer must ensure that all traffic leaving AS 200 will choose Link 2 as the exit point. Assuming that all BGP neighbor relationships have been formed and that the attributes have not been changed on any of the routers, which configuration accomplish task?

A. R4(config-router)bgp default local-preference 200
B. R3(config-router)neighbor 10.1.1.1 weight 200
C. R3(config-router)bgp default local-preference 200
D. R4(config-router)nighbor 10.2.2.2 weight 200

Answer: A

Explanation:
Local preference is an indication to the AS about which path has preference to exit the AS in order to reach a certain network. A path with a higher local preference

is preferred. The default value for local preference is 100.
Unlike the weight attribute, which is only relevant to the local router, local preference is an attribute that routers exchange in the same AS. The local preference is set with the "bgp default local-preference value" command.
In this case, both R3 & R4 have exit links but R4 has higher local-preference so R4 will be chosen as the preferred exit point from AS 200.

NEW QUESTION 238
Where is radio resource management performed in a cisco SD-access wireless solution?

A. DNA Center
B. control plane node
C. wireless controller
D. Cisco CMX

Answer: C

Explanation:
Fabric wireless controllers manage and control the fabric-mode APs using the same general model as the traditional local-mode controllers which offers the same operational advantages such as mobility control and radio resource management. A significant difference is that client traffic from wireless endpoints is not tunnelled from the APs to the wireless controller. Instead, communication from wireless clients is encapsulated in VXLAN by the fabric APs which build a tunnel to their first-hop fabric edge node. Wireless traffic it tunneled to the edge nodes as the edge nodes provide fabric services such as the Layer 3 Anycast Gateway, policy, and traffic enforcement. https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html

NEW QUESTION 242
Refer to the exhibit.
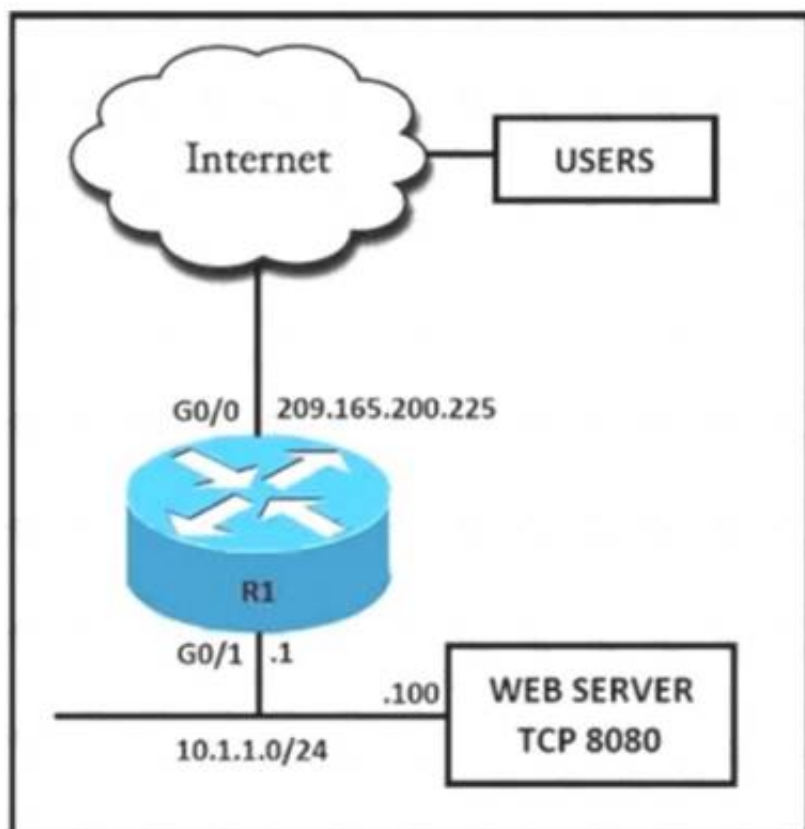
External users require HTTP connectivity to an internal company web server that is listening on TCP port 8080. Which command set accomplishes this requirement?
A)

```
interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat inside

interface G0/1
ip address 10.1.1.1 255.255.255.0
ip nat outside

ip nat inside source static tcp 10.1.1.1 8080 209.165.200.225 80
```

B)
```
interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat outside

interface G0/1
ip address 10.1.1.1 255.255.255.0
ip nat inside

ip nat inside source static tcp 10.1.1.100 8080 interface G0/0 80
```

C)

```
interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat inside
```

D)

```
interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat inside

interface G0/1
ip address 10.1.1.1 255.255.255.0
ip nat outside
```

E)

A. Option A
B. Option B
C. Option C
D. Option D
E. Option E

Answer: B

NEW QUESTION 245
Refer to the exhibit.
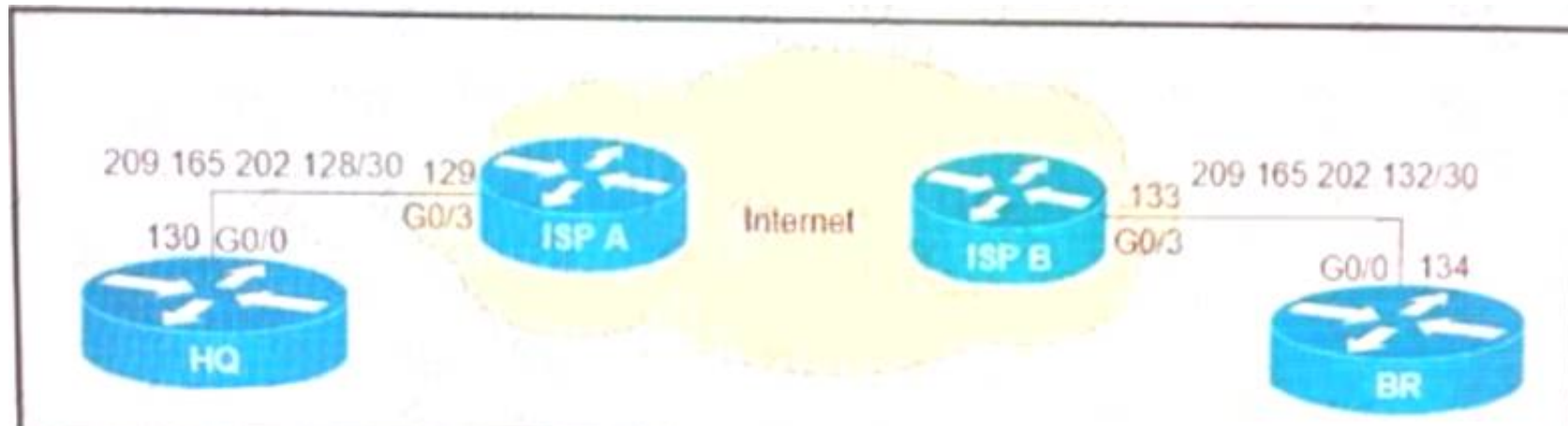
What is the effect of these commands on the BR and HQ tunnel interfaces?

```
BR(config)#interface tunnel1
BR(config-if)#keepalive 5 3

HQ(config)#interface tunnel1
HQ(config-if)#keepalive 5 3
```

A. The tunnel line protocol goes down when the keepalive counter reaches 6
B. The keepalives are sent every 5 seconds and 3 retries
C. The keepalives are sent every 3 seconds and 5 retries
D. The tunnel line protocol goes down when the keepalive counter reaches 5

Answer: B

NEW QUESTION 246
How does Cisco Trustsec enable more access controls for dynamic networking environments and data centers?

A. classifies traffic based on advanced application recognition
B. uses flexible NetFlow
C. classifies traffic based on the contextual identity of the endpoint rather than its IP address correct
D. assigns a VLAN to the endpoint

Answer: C

NEW QUESTION 249
Wireless users report frequent disconnections from the wireless network. While troubleshooting a network engineer finds that after the user a disconnect, the connection re-establishes automatically without any input required. The engineer also notices these message logs .

```
AP 'AP2' is down. Reason: Radio channel set. 6 54:04 PM
AP 'AP4' is down. Reason: Radio channel set. 6 44 49 PM
AP 'AP7' is down. Reason: Radio channel set. 6 34 32 PM
```

Which action reduces the user impact?

A. increase the AP heartbeat timeout
B. increase BandSelect

C. enable coverage hole detection
D. increase the dynamic channel assignment interval

Answer: D

Explanation:
These message logs inform that the radio channel has been reset (and the AP must be down briefly). With dynamic channel assignment (DCA), the radios can frequently switch from one channel to another but it also makes disruption. The default DCA interval is 10 minutes, which is matched with the time of the message logs. By increasing the DCA interval, we can reduce the number of times our users are disconnected for changing radio channels.

NEW QUESTION 251
At which Layer does Cisco DNA Center support REST controls?

A. EEM applets or scripts
B. Session layer
C. YMAL output from responses to API calls
D. Northbound APIs

Answer: D

NEW QUESTION 255
How is Layer 3 roaming accomplished in a unified wireless deployment?

A. An EoIP tunnel is created between the client and the anchor controller to provide seamless connectivity as the client is associated with the new AP.
B. The client entry on the original controller is passed to the database on the new controller.
C. The new controller assigns an IP address from the new subnet to the client
D. The client database on the original controller is updated the anchor entry, and the new controller database is updated with the foreign entry.

Answer: A

NEW QUESTION 257
Drag and drop the wireless elements on the left to their definitions on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Chart, line chart Description automatically generated

NEW QUESTION 262
Which configuration restricts the amount of SSH that a router accepts 100 kbps?
A)

B)

```
class-map match-all CoPP_SSH
  match access-group name CoPP_SSH
  !
policy-map CoPP_SSH
  class CoPP_SSH
  police cir 100000
    exceed-action drop
  !
  !

Interface GigabitEthernet0/1
  ip address 209.165.200.225 255.255.255.0
  ip access-group ROBESS out
  duplex auto
  speed auto
  media-type rj4
  service-policy input CoPP_SSH

ip access-list extended CoPP_SSH
  deny tcp any any eq 22
```

C)

```
class-map match-all CoPP_SSH
  match access-group name CoPP_SSH
  !
policy-map CoPP_SSH
  class CoPP_SSH
  police cir 100000
    exceed-action drop
  !
  !

control-plane
  service-policy input CoPP_SSH

ip access-list extended CoPP_SSH
  permit tcp any any eq 22
```

D)

```
class-map match-all CoPP_SSH
  match access-group name CoPP_SSH
  !
policy-map CoPP_SSH
  class CoPP_SSH
  police cir 100000
    exceed-action drop
  !

control-plane transit
  service-policy input CoPP_SSH

ip access-list extended CoPP_SSH
  permit tcp any any eq 22
```

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

Answer: C

Explanation:
CoPP protects the route processor on network devices by treating route processor resources as a separate entity with its own ingress interface (and in some implementations, egress also). CoPP is used to police traffic that is destined to the route processor of the router such as:
+ routing protocols like OSPF, EIGRP, or BGP.
+ Gateway redundancy protocols like HSRP, VRRP, or GLBP.
+ Network management protocols like telnet, SSH, SNMP, or RADIUS.
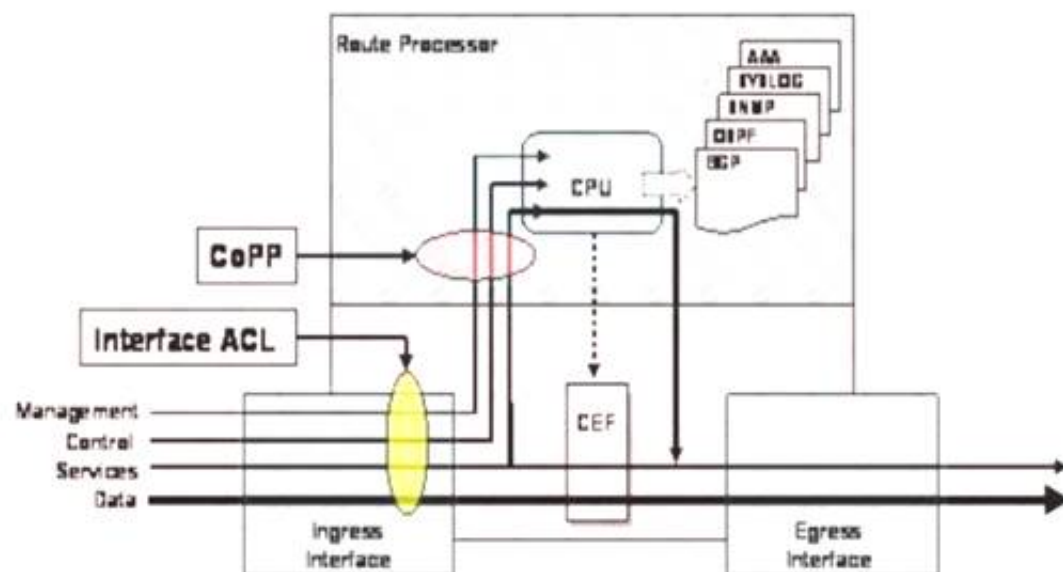
Therefore we must apply the CoPP to deal with SSH because it is in the management plane. CoPP must be put under "control-plane" command.

NEW QUESTION 265
Refer to the exhibit.

Assuming the WLC's interfaces are not in the same subnet as the RADIUS server, which interface would the WLC use as the source for all RADIUS-related traffic?

A. the interface specified on the WLAN configuration
B. any interface configured on the WLC
C. the controller management interface
D. the controller virtual interface

Answer: A

NEW QUESTION 267
Refer to the exhibit.

Based on the configuration in this WLAN security setting, Which method can a client use to authenticate to the network?

A. text string
B. username and password
C. certificate
D. RADIUS token

Answer: A

NEW QUESTION 271
A server running Linux is providing support for virtual machines along with DNS and DHCP services for a small business. Which technology does this represent?

A. container
B. Type 1 hypervisor
C. hardware pass-thru
D. Type 2 hypervisor

Answer: D

NEW QUESTION 276
How are the different versions of IGMP compatible?

A. IGMPv2 is compatible only with IGMPv1.
B. IGMPv2 is compatible only with IGMPv2.
C. IGMPv3 is compatible only with IGMPv3.
D. IGMPv3 is compatible only with IGMPv1

Answer: A

NEW QUESTION 277
Which two operational models enable an AP to scan one or more wireless channels for rouge access points and at the same time provide wireless services to clients? (Choose two.)

A. Rouge detector
B. Sniffer
C. FlexConnect
D. Local
E. Monitor

Answer: DE

NEW QUESTION 280
Refer to the exhibit.

```
Router#show ip ospf interface
GigabitEthernet0/1.40 is up, line protocol is up
  Internet Address 10.3.5.254/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID  Cost  Disabled  Shutdown  Topology Name
       0          1      no        no        Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.29, Interface address 10.3.5.254
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 172.16.30.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID  Cost  Disabled  Shutdown  Topology Name
       0          1      no        no        Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.29, Interface address 172.16.30.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 172.16.11.29/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID  Cost  Disabled  Shutdown  Topology Name
       0          1      no        no        Base
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 172.16.11.27, Interface address 172.16.11.27
  Backup Designated router (ID) 172.16.11.30, Interface address 172.16.11.30
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
```

A network engineer configures OSPF and reviews the router configuration. Which interface or interface or interface are able to establish OSPF adjacency?

A. GigabitEthemet0/1 and GigabitEthernet0/1.40
B. only GigabitEthernet0/1
C. only GigabttEthernet0/0
D. Gigabit Ethernet0/0 and GigabitEthemet0/1

Answer: C

NEW QUESTION 284
When configuration WPA2 Enterprise on a WLAN, which additional security component configuration is required?

A. NTP server
B. PKI server
C. RADIUS server
D. TACACS server

Answer: C

NEW QUESTION 288
Refer to the exhibit.

```
with manager.connect(host=192.168.0.1, port=22,
            username='admin', password='password1', hostkey_verify=True,
            device_params={'name':'nexus'}) as m:
```

What does the snippet of code achieve?

A. It creates a temporary connection to a Cisco Nexus device and retrieves a token to be used for API calls.
B. It opens a tunnel and encapsulates the login information, if the host key is correct.
C. It opens an ncclient connection to a Cisco Nexus device and maintains it for the duration of the context.
D. It creates an SSH connection using the SSH key that is stored, and the password is ignored.

Answer: C

Explanation:
ncclient is a Python library that facilitates client-side scripting and application development around the NETCONF protocol.
The above Python snippet uses the ncclient to connect and establish a NETCONF session to a Nexus device (which is also a NETCONF server).

NEW QUESTION 291
Which two network problems Indicate a need to implement QoS in a campus network? (Choose two.)

A. port flapping
B. excess jitter
C. misrouted network packets
D. duplicate IP addresses
E. bandwidth-related packet loss

Answer: BE

NEW QUESTION 295
An engineer configures HSRP group 37. The configuration does not modify the default virtual MAC address. Which virtual MAC address does the group use?

A. C0:00:00:25:00:00
B. 00:00:0c:07:ac:37
C. C0:39:83:25:258:5
D. 00:00:0c:07:ac:25

Answer: D

NEW QUESTION 297
The login method is configured on the VTY lines of a router with these parameters.
≫ The first method for authentication is TACACS
≫ If TACACS is unavailable, login is allowed without any provided credentials
Which configuration accomplishes this task?

A. R1#sh run | include aaa aaa new-modelaaa authentication login VTY group tacacs+ none aaa session-id commonR1#sh run | section vty line vty 0 4password 7 0202039485748R1#sh run | include username R1#
B. R1#sh run | include aaa aaa new-modelaaa authentication login telnet group tacacs+ none aaa session-id commonR1#sh run | section vty line vty 0 4R1#sh run | include username R1#
C. R1#sh run | include aaa aaa new-modelaaa authentication login default group tacacs+ none aaa session-id commonR1#sh run | section vty line vty 0 4password 7 0202039485748
D. R1#sh run | include aaa aaa new-modelaaa authentication login default group tacacs+ aaa session-id commonR1#sh run | section vty line vty 0 4transport input none R1#

Answer: C

Explanation:
According to the requirements (first use TACACS+, then allow login with no authentication), we have to use "aaa authentication login … group tacacs+ none" for AAA command.
The next thing to check is the if the "aaa authentication login default" or "aaa authentication login list-name" is used. The 'default' keyword means we want to apply for all login connections
(such as tty, vty, console and aux). If we use this keyword, we don't need to configure anything else under tty, vty and aux lines. If we don't use this keyword then we have to specify which line(s) we want to apply the authentication feature.
From above information, we can find out answer 'R1#sh run | include aaa aaa new-model
aaa authentication login default group tacacs+ none aaa session-id common
R1#sh run | section vty line vty 0 4
password 7 0202039485748
If you want to learn more about AAA configuration, please read our AAA TACACS+ and RADIUS Tutorial – Part 2.
For your information, answer 'R1#sh run | include aaa aaa new-model
aaa authentication login telnet group tacacs+ none aaa session-id common
R1#sh run | section vty line vty 0 4
R1#sh run | include username
R1#' would be correct if we add the following command under vty line ("line vty 0 4"): "login
authentication telnet" ("telnet" is the name of the AAA list above)

NEW QUESTION 302
Refer to the exhibit.

```
ip sla 10

icmp-echo 192.168.10.20

timeout 500

frequency 3

ip sla schedule 10 life forever start-time now
track 10 ip sla 10 reachability
```

The IP SLA is configured in a router. An engineer must configure an EEM applet to shut down the interface and bring it back up when there is a problem with the IP SLA. Which configuration should the engineer use?

A. event manager applet EEM_IP_SLA event track 10 state down
B. event manager applet EEM_IP_SLA event track 10 state unreachable
C. event manager applet EEM_IP_SLA event sla 10 state unreachable
D. event manager applet EEM_IP_SLA event sla 10 state down

Answer: A

Explanation:
The ip sla 10 will ping the IP 192.168.10.20 every 3 seconds to make sure the connection is still up. We can configure an EEM applet if there is any problem with this IP SLA via the command event track 10 state down.

NEW QUESTION 307
How is 802.11 traffic handled in a fabric-enabled SSID?

A. centrally switched back to WLC where the user traffic is mapped to a VXLAN on the WLC
B. converted by the AP into 802.3 and encapsulated into VXLAN
C. centrally switched back to WLC where the user traffic is mapped to a VLAN on the WLC
D. converted by the AP into 802.3 and encapsulated into a VLAN

Answer: B

NEW QUESTION 309
Refer to the exhibit.

```
    M - Hot-standby (LACP only)
    R - Layer3  S - Layer2
    U - in use f - failed to allocate aggregator
    M - not in use, minimum links not met
    u - unsuitable for bundling
    w - waiting to be aggregated
    d - default port
    Number of channel-groups in use: 1
    Number of aggregators: 1
    Group Port-channel Protocol Ports
    ------+-------------+-----------+-----------------
    ------
    1 Po1(S D ) PAgP Gi0/0(I) Gi0/1(I)


    SW3# show etherchannel summary
    Flags: D - down P - bundled in port-channel
    I - stand-alone s - suspended
    H - Hot-standby (LACP only)
    R - Layer3  S - Layer2
    U - in use f - failed to allocate aggregator
    M - not in use, minimum links not met
    u - unsuitable for bundling
    w - waiting to be aggregated
    d - default port
    Number of channel-groups in use: 1
    Number of aggregators: 1
    Group Port-channel Protocol Ports
    ------+-------------+-----------+-----------------
    ------
    1 Po1(S D ) LACP Gi0/0(I) Gi0/1(I)
```

Which action resolves the EtherChannel issue between SW2 and SW3?

A. Configure switchport mode trunk on SW2.
B. Configure switchport nonegotiate on SW3
C. Configure channel-group 1 mode desirable on both interfaces.
D. Configure channel-group 1 mode active on both interfaces.

Answer: D

NEW QUESTION 314

Which measure is used by an NTP server to indicate its closeness to the authoritative time source?

A. latency
B. hop count
C. time zone
D. stratum

Answer: D

NEW QUESTION 317
Which technology is used as the basis for the cisco sd-access data plane?

A. IPsec
B. LISP
C. VXLAN
D. 802.1Q

Answer: C

NEW QUESTION 319
What is a benefit of data modeling languages like YANG?

A. They enable programmers to change or write their own application within the device operating system.
B. They create more secure and efficient SNMP OIDs.
C. They make the CLI simpler and more efficient.
D. They provide a standardized data structure, which results in configuration scalability and consistency.

Answer: D

Explanation:
Yet Another Next Generation (YANG) is a language which is only used to describe data models (structure). It is not XML or JSON.

NEW QUESTION 323
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 350-401 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 350-401 Product From:

https://www.2passeasy.com/dumps/350-401/

Money Back Guarantee

350-401 Practice Exam Features:

* 350-401 Questions and Answers Updated Frequently

* 350-401 Practice Questions Verified by Expert Senior Certified Staff

* 350-401 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 350-401 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year