

# Cisco

## Exam Questions 350-401

Implementing and Operating Cisco Enterprise Network Core Technologies



**NEW QUESTION 1**

- (Topic 4)

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

Refer to the Exhibit. Running the script causes the output in the exhibit. What should be the first line of the script?

- A. from ncclient import manager
- B. import manager
- C. from ncclient import \*
- D. ncclient manager import

**Answer: C**

**NEW QUESTION 2**

- (Topic 4)

What are two benefits of implementing a traditional WAN instead of an SD-WAN solution? (Choose two.)

- A. comprehensive configuration standardization
- B. lower control plane abstraction
- C. simplify troubleshooting
- D. faster fault detection
- E. lower data plane overhead

**Answer: BD**

**NEW QUESTION 3**

- (Topic 4)

```
FastEthernet1/0/47 - Group 1 (version 2)
  State is Standby
    7 state changes, last state change 00:00:02
  Virtual IP address is 10.1.1.1
  Active virtual MAC address is 0000.0c9f.f001
    Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.375 secs
  Authentication MD5, key-string "cisco"
  Preemption enabled, delay min 5 secs
  Active router is 10.1.1.2, priority 255 (expires in 9.396 sec)
  Standby router is local
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Fal/0/47-1" (default)
```

Refer to the exhibit. An engineer configures HSRP and enters the show standby command. Which two facts about the network environment are derived from the output? (Choose two.)

- A. The local device has a higher priority selling than the active router
- B. The virtual IP address of the HSRP group is 10.1.1.1.
- C. If the local device fails to receive a hello from the active router for more than 5 seconds, it becomes the active router.
- D. The hello and hold timers are set to custom values.
- E. If a router with a higher IP address and same HSRP priority as the active router becomes available, that router becomes the new active router 5 seconds later.

**Answer: BE**

**NEW QUESTION 4**

- (Topic 4)

A switch is attached to router R1 on its gig 0/0 interface. Fort security reasons, you want to prevent R1 from sending OSPF hellos to the switch. Which command should be enabled to accomplish this?

- A. R1(config-router)#ip ospf hello disable
- B. R1(config-router)#ip ospf hello-interval 0
- C. R1(config)#passive-interface Gig 0/0
- D. R1(config-router)#passive-interface Gig 0/0

**Answer: D**

**NEW QUESTION 5**

SIMULATION - (Topic 4)

Simulation 09

Guidelines Topology Tasks

SW01 SW02 R01

```
SW01>
SW01>
SW01>
```

Guidelines Topology Tasks

Configure the devices according to the topology to achieve these goals:

1. Configure a SPAN session on SW01 using these parameters:
  - Session Number: 20
  - Source Interface: VLAN 99
  - Traffic Direction: Transmitted Traffic
  - Destination Interface: Ethernet 0/1
2. Configure the NetFlow Top Talkers feature for outbound traffic on interface E0/2 of R01 with these parameters:
  - Number of Top Talkers: 50
  - Sort Type: Packets
  - Cache Timeout: 30 seconds
3. Configure an IP SLA operation on SW02 and start the ICMP probe with these parameters:
  - Entry Number: 10
  - Target IP: 1.1.1.1

SW01 SW02 R01

```
SW01>
SW01>
SW01>
```

2. Configure the NetFlow Top Talkers feature for outbound traffic on interface E0/2 of R01 with these parameters:
  - Number of Top Talkers: 50
  - Sort Type: Packets
  - Cache Timeout: 30 seconds
3. Configure an IP SLA operation on SW02 and start the ICMP probe with these parameters:
  - Entry Number: 10
  - Target IP: 1.1.1.1
  - Source IP: 172.16.2.2
  - Frequency: 5 seconds
  - Threshold: 250 milliseconds
  - Timeout: 3000 milliseconds
  - Lifetime: Forever

SW01>

SW01>

SW01>

- A. Mastered
- B. Not Mastered

**Answer:** A

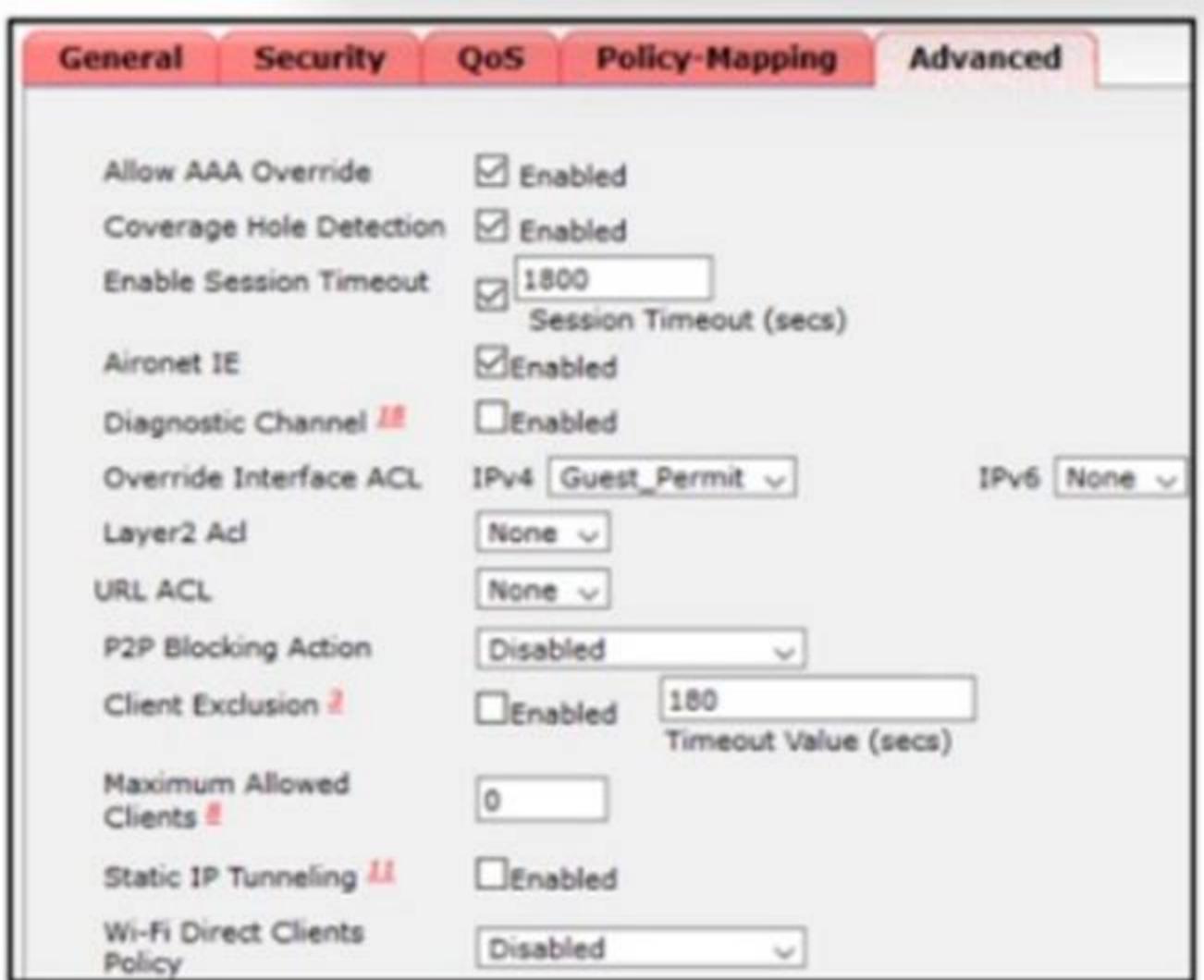
**Explanation:**

```
Sw1
Config t
Monitor session 20 source vlan 99 tx
Monitor session 20 destination interface ethernet 0/1 Copy run start
R1
Config t
Ip flow-top-talkers Top 50
Sort-by packets Cache time-out 30
Eth 0/2
Ip flow egress Copy run start Sw02
Config t
Ip sla 10
Icmp-echo 1.1.1.1 source-ip 172.16.2.2
Frequency 5
Threshold 250
```

Timeout 3000  
 Ip sla schedule 10 start-time now life forever  
 Copy run start

**NEW QUESTION 6**

- (Topic 4)  
 Refer to the exhibit.



An engineer configures a new WLAN that will be used for secure communications; however, wireless clients report that they are able to communicate with each other. Which action resolves this issue?

- A. Enable Client Exclusions.
- B. Disable Aironet IE
- C. Enable Wi-Fi Direct Client Policy
- D. Enable P2P Blocking.

**Answer: D**

**NEW QUESTION 7**

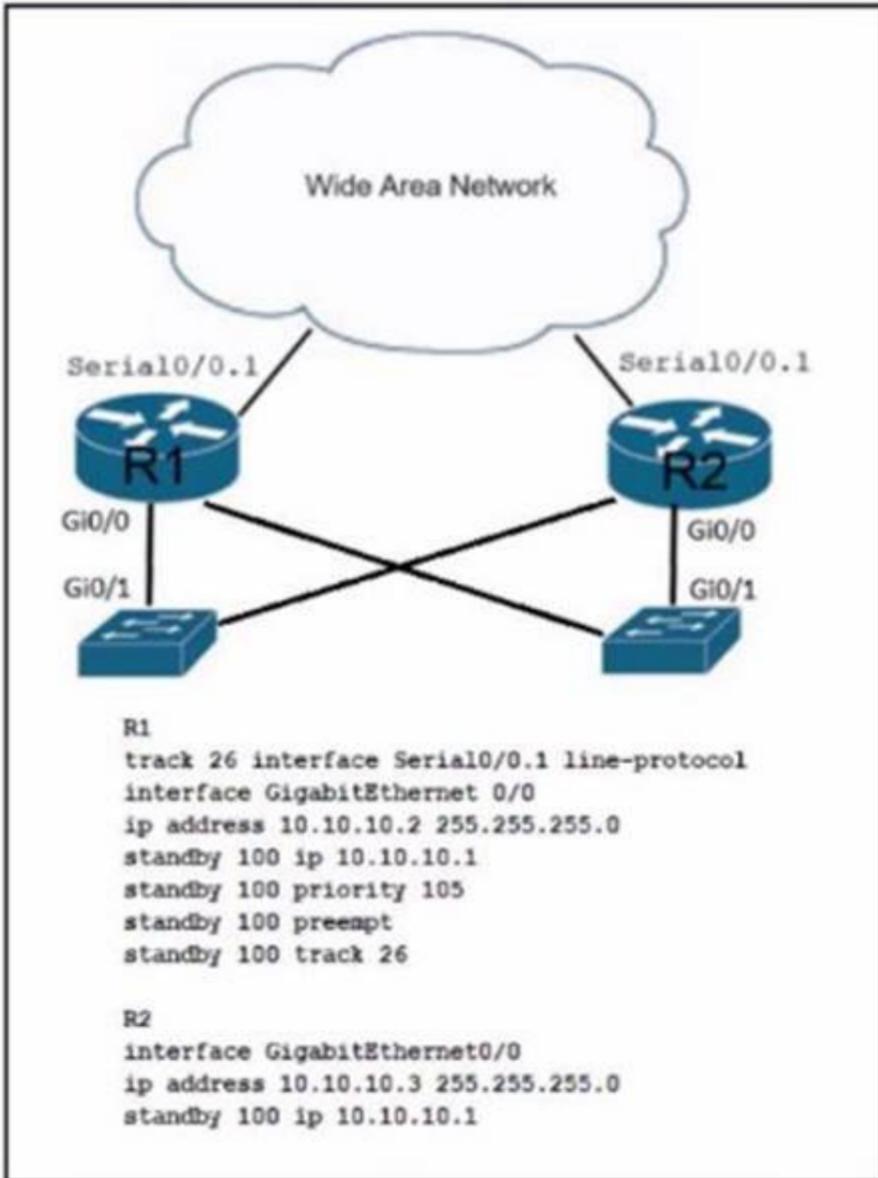
- (Topic 4)  
 Which tunnel type allows clients to perform a seamless Layer 3 roam between a Cisco AireOS WLC and a Cisco IOS XE WLC?

- A. Ethernet over IP
- B. IPsec
- C. Mobility
- D. VPN

**Answer: A**

**NEW QUESTION 8**

- (Topic 4)  
 Refer to the exhibit.



An engineer must modify the existing configuration so that R2 can take over as the primary router when serial interface 0/0.1 on R1 goes down. Which command must the engineer apply?"

- A. R2W standby 100 track 26 decrement 10
- B. R2# standby 100 preempt
- C. R2# track 26 interface SerialWO.1 line-protocol
- D. R2# standby 100 priority 100

**Answer: A**

**NEW QUESTION 9**

- (Topic 4)

Which mechanism can be used to enforce network access authentication against an AAA server if the endpoint does not support the 802.1X supplicant functionality?

- A. private VLANs
- B. port security
- C. MAC Authentication Bypass
- D. MACsec

**Answer: C**

**NEW QUESTION 10**

- (Topic 4)

An engineer must protect the password for the VTY lines against over-the-shoulder attacks. Which configuration should be applied?

- A. service password-encryption
- B. username netadmin secret 9 \$9\$vFpMf8elb4RVV8\$seZ/bDA
- C. username netadmin secret 7\$1\$42J36k33008Pyh4QzwXyZ4
- D. line vty 0 15 p3ssword XD822j

**Answer: A**

**Explanation:**

```

cisco(config)#username test privilege 15 password test777 cisco(config)#do s running-config | include user
username test privilege 15 password 0 test777
cisco(config)#service password-encryption cisco(config)#do s running-config | include user
username test privilege 15 password 7 044F0E151B761B19 cisco(config)#
cisco(config)#do wr
Building configuration... [OK]
cisco(config)#
  
```

**NEW QUESTION 10**  
 - (Topic 4)

```

S1# 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 (SD)          -      Fa0/1 (D) Fa0/2 (D)

S1# show run | begin interface port-channel
interface Port-channel1
switchport mode trunk
|
interface FastEthernet0/1
switchport mode trunk
channel-group 1 mode on
|
interface FastEthernet0/2
switchport mode trunk
channel-group 1 mode on
|
<Output omitted>

S2# show run | begin interface port-channel
interface Port-channel1
switchport mode trunk
|
interface FastEthernet0/1
switchport mode trunk
channel-group 1 mode desirable
|
interface FastEthernet0/2
switchport mode trunk
channel-group 1 mode desirable
|
<Output omitted>
    
```

Refer to the exhibit. Traffic is not passing between SW1 and SW2. Which action fixes the issue?

- A. Configure LACP mode on S1 to passive.
- B. Configure switch port mode to ISL on S2.
- C. Configure PAgP mode on S1 to desirable.
- D. Configure LACP mode on S1 to active.

**Answer: C**

**NEW QUESTION 13**

DRAG DROP - (Topic 4)

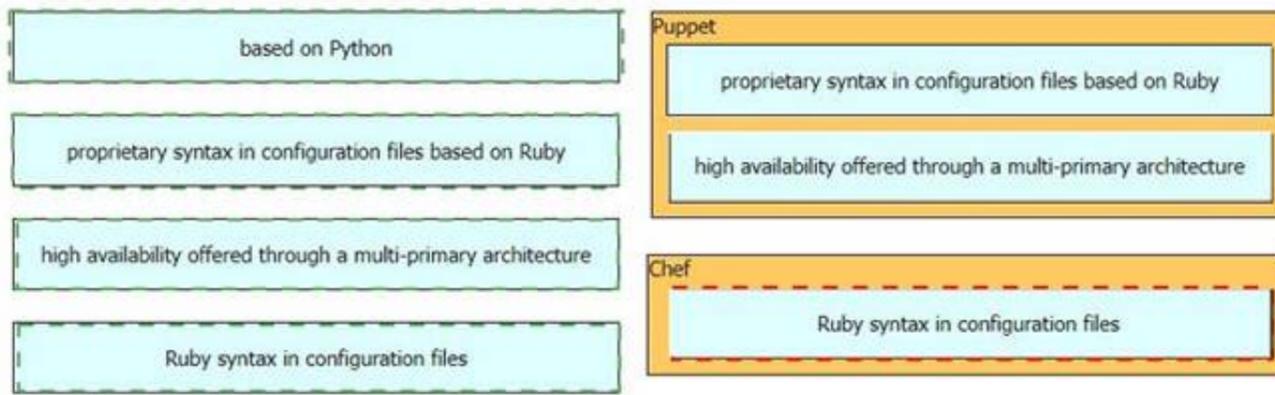
Drag and drop the automation characteristics from the left onto the corresponding tools on the right. Not all options are used.

based on Python	Puppet
proprietary syntax in configuration files based on Ruby	
high availability offered through a multi-primary architecture	Chef
Ruby syntax in configuration files	

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**



**NEW QUESTION 16**

- (Topic 4)

What is the role of the vSmart controller in a Cisco SD-WN environment?

- A. it performs authentication and authorization
- B. it manages the control plane.
- C. it is the centralized network management system
- D. it manages the data plane

**Answer: B**

**NEW QUESTION 17**

- (Topic 4)

```

line con 0
 password cisco
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 !
end

router#sh run | i username|aaa
no aaa new-model
username user password 0 user
router#
    
```

Refer to the exhibit Which configuration enables password checking on the console line, using only a password?

A)

```

router(config)# line con 0
router(config-line)# exec-timeout 0 0
    
```

B)

```

router(config)# line con 0
router(config-line)# login
    
```

C)

```

router(config)# line con 0
router(config-line)# login local
    
```

D)

```

router(config)# line vty 0 4
router(config-line)# login
    
```

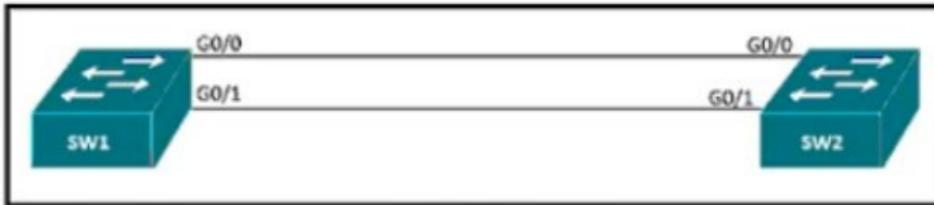
- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: B**

**NEW QUESTION 20**

- (Topic 2)

Refer to the exhibit.



An engineer reconfigures the port-channel between SW1 and SW2 from an access port to a trunk and immediately notices this error in SW1's log. Which command set resolves this error?

A)

```
SW1(config-if)#interface G0/0
SW1(config-if)#spanning-tree bpduguard enable
SW1(config-if)#shut
SW1(config-if)#no shut
```

B)

```
SW1(config-if)#interface G0/0
SW1(config-if)#no spanning-tree bpduguard enable
SW1(config-if)#shut
SW1(config-if)#no shut
```

C)

```
SW1(config-if)#interface G0/1
SW1(config-if)#spanning-tree bpduguard enable
SW1(config-if)#shut
SW1(config-if)#no shut
```

D)

```
SW1(config-if)#interface G0/0
SW1(config-if)#no spanning-tree bpdudfilter
SW1(config-if)#shut
SW1(config-if)#no shut
```

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

**Answer: B**

**NEW QUESTION 23**

- (Topic 2)

Refer to the exhibit.

```
DSW1#sh spanning-tree vlan 20

VLAN0020
Spanning tree enabled protocol ieee
Root ID    Priority    24596
Address    0018.7363.4300
Cost       2
Port       13 (FastEthernet1/0/11)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    28692 (priority 28672 sys-id-ext 20)
Address    001b.0d8e.e080
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa1/0/7        Desg FWD 2        128.9    P2p
Fa1/0/10       Desg FWD 2        128.12   P2p
Fa1/0/11       Root FWD 2        128.13   P2p
Fa1/0/12       Altn BLK 2        128.14   P2p
```

What does the output confirm about the switch's spanning tree configuration?

- A. The spanning-tree mode stp ieee command was entered on this switch
- B. The spanning-tree operation mode for this switch is IEEE.
- C. The spanning-tree operation mode for this switch is PVST+.
- D. The spanning-tree operation mode for this switch is PVST

**Answer: C**

**NEW QUESTION 28**

DRAG DROP - (Topic 2)

Drag and drop the snippets onto the blanks within the code to construct a script that shows all logging that occurred on the appliance from Sunday until 9:00 p.m Thursday Not all options are used.

```
event manager applet Logging
event timer cron name Logging cron-entry " [ ] "
action 2.0 cli command "enable"
action [ ] cli command "show logging | [ ] "
```

1.0

3.0

redirect  
ftp://cisco:cisco@192.168.1.1

0 21 \* \* 0-4

0 21 \* \* 1-5

ftp://cisco:cisco@192.168.1.1

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Graphical user interface, text, application Description automatically generated

**NEW QUESTION 32**

- (Topic 2)

In a Cisco SD-WAN solution, which two functions are performed by OMP? (Choose two.)

- A. advertisement of network prefixes and their attributes
- B. configuration of control and data policies
- C. gathering of underlay infrastructure data
- D. delivery of crypto keys
- E. segmentation and differentiation of traffic

**Answer: AB**

**Explanation:**

OMP is the control protocol that is used to exchange routing, policy, and management information between Cisco vSmart Controllers and Cisco IOS XE SD-WAN devices in the overlay network. These devices automatically initiate OMP peering sessions between themselves, and the two IP end points of the OMP session are the system IP addresses of the two devices.

**NEW QUESTION 36**

- (Topic 2)

How can an engineer prevent basic replay attacks from people who try to brute force a system via REST API?

- A. Add a timestamp to the request in the API header.
- B. Use a password hash
- C. Add OAuth to the request in the API header.
- D. UseHTTPS

Answer: B

**NEW QUESTION 40**

- (Topic 2)

Which access point mode allows a supported AP to function like a WLAN client would, associating and identifying client connectivity issues?

- A. client mode
- B. SE-connect mode
- C. sensor mode
- D. sniffer mode

Answer: C

**Explanation:**

As these wireless networks grow especially in remote facilities where IT professionals may not always be onsite, it becomes even more important to be able to quickly identify and resolve potential connectivity issues ideally before the users complain or notice connectivity degradation. To address these issues we have created Cisco's Wireless Service Assurance and a new AP mode called "sensor" mode. Cisco's Wireless Service Assurance platform has three components, namely, Wireless Performance Analytics, Real-time Client Troubleshooting, and Proactive Health Assessment. Using a supported AP or dedicated sensor the device can actually function much like a WLAN client would associating and identifying client connectivity issues within the network in real time without requiring an IT or technician to be on site.

Reference:

[https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/dam/en/us/td/docs/wireless/controller/technotes/8-5/b\\_Cisco\\_Aironet\\_Sensor\\_Deployment\\_Guide.html.xml](https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/dam/en/us/td/docs/wireless/controller/technotes/8-5/b_Cisco_Aironet_Sensor_Deployment_Guide.html.xml)

**NEW QUESTION 42**

- (Topic 2)

What does a northbound API accomplish?

- A. programmatic control of abstracted network resources through a centralized controller
- B. access to controlled network resources from a centralized node
- C. communication between SDN controllers and physical switches
- D. controlled access to switches from automated security applications

Answer: A

**NEW QUESTION 43**

- (Topic 2)

```
interface Vlan10
ip vrf forwarding Clients
ip address 192.168.1.1 255.255.255.0
!
interface Vlan20
ip vrf forwarding Servers
ip address 172.16.1.1 255.255.255.0
!
interface Vlan30
ip vrf forwarding Printers
ip address 10.1.1.1 255.255.255.0
-- output omitted for brevity --
router eigrp 1
10.0.0.0
172.16.0.0
192.168.1.0
```

Refer to the exhibit. An engineer attempts to configure a router on a stick to route packets between Clients, Servers, and Printers; however, initial tests show that this configuration is not working. Which command set resolves this issue?

A)

```
router eigrp 1
network 10.0.0.0 255.255.255.0
network 172.16.0.0 255.255.255.0
network 192.168.1.0 255.255.255.0
```

B)

```
interface Vlan10
no ip vrf forwarding Clients
!
interface Vlan20
no ip vrf forwarding Servers
!
interface Vlan30
no ip vrf forwarding Printers
```

C)

```
interface Vlan10
no ip vrf forwarding Clients
ip address 192.168.1.2 255.255.255.0
!
interface Vlan20
no ip vrf forwarding Servers
ip address 172.16.1.2 255.255.255.0
!
interface Vlan30
no ip vrf forwarding Printers
ip address 10.1.1.2 255.255.255.0
```

D)

```
router eigrp 1
network 10.0.0.0 255.0.0.0
network 172.16.0.0 255.255.0.0
network 192.168.1.0 255.255.0.0
```

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

Answer: C

**Explanation:**

We must reconfigure the IP address after assigning or removing an interface to a VRF. Otherwise that interface does not have an IP address.

**NEW QUESTION 46**

DRAG DROP - (Topic 2)

Drag and drop the tools from the left onto the agent types on the right.

Puppet	Agent-based
Ansible	
SaltStack	
	Agentless

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Puppet	Agent-based
Ansible	
SaltStack	
	Agentless

**NEW QUESTION 48**

- (Topic 2)

When are multicast RPs required?

- A. RPs are required only when using protocol independent multicast dense mode.
- B. By default, the RP is needed periodically to maintain sessions with sources and receivers.
- C. RPs are required for protocol Independent multicast sparse mode and dense mode.
- D. By default, the RP is needed only to start new sessions with sources and receivers.

**Answer: D**

**NEW QUESTION 52**

- (Topic 2)

Refer to the exhibit.

```
enable secret cisco

username cisco privilege 15 secret cisco

aaa new-model
aaa authentication login default group radius local
aaa authorization network default group radius
```

The network administrator must be able to perform configuration changes when all the RADIUS servers are unreachable. Which configuration allows all commands to be authorized if the user has successfully authenticated?

- A. aaa authorization exec default group radius none
- B. aaa authentication login default group radius local none
- C. aaa authorization exec default group radius if-authenticated
- D. aaa authorization exec default group radius

**Answer: C**

**NEW QUESTION 56**

- (Topic 2)

Which outcome is achieved with this Python code?

```
client.connect ( ip, port= 22, username= usr, password= pswd )
stdin, stdout, stderr = client.exec_command ( 'show ip bgp 192.168.101.0 bestpath\n ' )
print (stdout)
```

- A. connects to a Cisco device using SSH and exports the routing table information
- B. displays the output of the show command in a formatted way
- C. connects to a Cisco device using SSH and exports the BGP table for the prefix
- D. connects to a Cisco device using Telnet and exports the routing table information

**Answer: C**

**NEW QUESTION 61**

- (Topic 2)

Refer to the exhibit.

```

0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: access-group name SNMP
police:
  cir 8000 bps, bc 1500 bytes
  conformed 0 packets, 0 bytes; actions:
  transmit
  exceeded 0 packets, 0 bytes; actions:
  drop
  conformed 0000 bps, exceeded 0000 bps

Class-map: class-default (match-any)
13858 packets, 1378745 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
  
```

How does the router handle traffic after the CoPP policy is configured on the router?

- A. Traffic coming to R1 that does not match access list SNMP is dropped.
- B. Traffic coming to R1 that matches access list SNMP is policed.
- C. Traffic passing through R1 that matches access list SNMP is policed.
- D. Traffic generated by R1 that matches access list SNMP is policed.

Answer: C

**NEW QUESTION 62**

- (Topic 2)

What is required for a virtual machine to run?

- A. a Type 1 hypervisor and a host operating system
- B. a hypervisor and physical server hardware
- C. only a Type 1 hypervisor
- D. only a Type 2 hypervisor

Answer: B

**NEW QUESTION 67**

- (Topic 2)

Refer to the exhibit.

```

Router1#
Router1#show run int tunnel 0
Building configuration...

Current configuration : 95 bytes
:
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 tunnel destination 192.168.10.2
end

Router1#show ip int br
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0 192.168.1.1    YES manual up          up
GigabitEthernet0/1 unassigned      YES unset   administratively down down
GigabitEthernet0/2 unassigned      YES unset   administratively down down
GigabitEthernet0/3 unassigned      YES unset   administratively down down
Loopback0          192.168.10.1   YES manual up          up
Tunnel0            172.16.1.1     YES manual up          down
Router1#
  
```

Which command must be applied to Router 1 to bring the GRE tunnel to an up/up state?

- A. Routed (config if funnel mode gre multipoint
- B. Router1(config-if)&tunnel source Loopback0
- C. Router1(config-if)#tunnel source GigabitEthernet0/1
- D. Router1 (config)#interface tunnel0

Answer: B

**NEW QUESTION 72**

DRAG DROP - (Topic 2)

Drag and drop the descriptions from the left onto the routing protocol they describe on the right.

- summaries can be created anywhere in the IGP topology
- uses areas to segment a network
- summaries can be created in specific parts of the IGP topology

OSPF

EIGRP

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

- summaries can be created anywhere in the IGP topology
- uses areas to segment a network
- summaries can be created in specific parts of the IGP topology

OSPF

summaries can be created anywhere in the IGP topology

uses areas to segment a network

EIGRP

summaries can be created in specific parts of the IGP topology

**NEW QUESTION 77**

- (Topic 2)

```

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
                    
```

Refer to the exhibit. Which configuration must be applied to R1 to enable R1 to reach the server at 172.16.0.1?

- 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
- 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
- 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
- interface Ethernet0/0  
 vrf forwarding bank  
 ip address 172.16.0.7 255.255.0.0

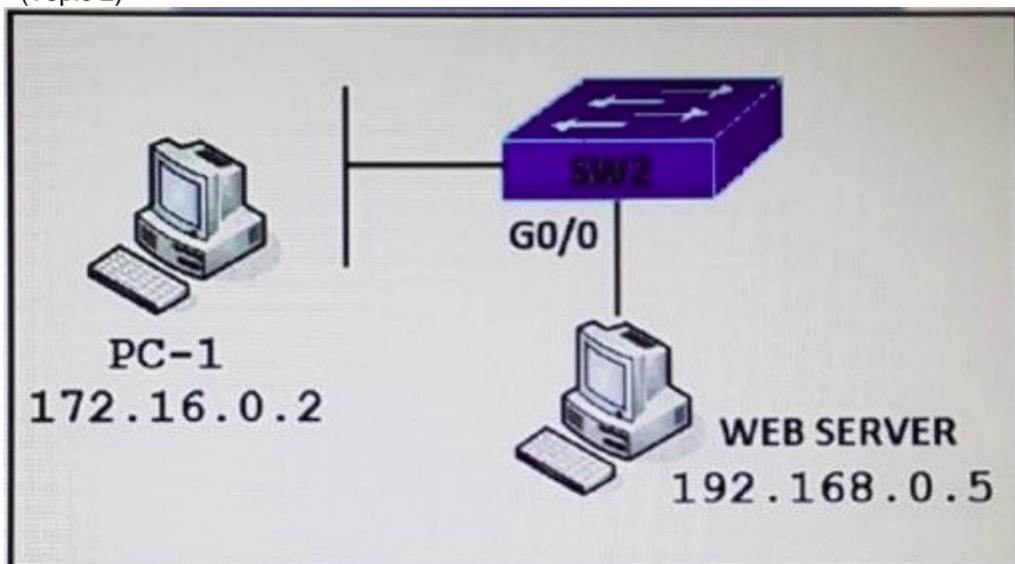
router ospf 44 vrf bank  
 network 172.16.0.0 0.0.255.255 area 0

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

Answer: D

**NEW QUESTION 80**

- (Topic 2)



Refer to the exhibit. PC-1 must access the web server on port 8080. To allow this traffic, which statement must be added to an access control list that is applied on SW2 port G0/0 in the inbound direction?

- A. permit host 172.16.0.2 host 192.168.0.5 eq 8080
- B. permit host 192.168.0.5 host 172.16.0.2 eq 8080
- C. permit host 192.168.0.5 eq 8080 host 172.16.0.2
- D. permit host 192.168.0.5 it 8080 host 172.16.0.2

Answer: C

**Explanation:**

The inbound direction of G0/0 of SW2 only filter traffic from Web Server to PC-1 so the source IP address and port is of the Web Server.

**NEW QUESTION 83**

- (Topic 2)

What Is a Type 2 hypervisor?

- A. installed as an application on an already installed operating system
- B. runs directly on a physical server and includes its own operating system
- C. supports over-allocation of physical resources
- D. also referred to as a "bare metal hypervisor" because it sits directly on the physical server

**Answer: A**

**NEW QUESTION 85**

- (Topic 2)

Refer to the exhibit.

```

headers = {
    'Accept': 'application/yang-data+json',
    'Content-Type': 'application/yang-data+json'
},
data = json.dumps({
    'Cisco-IOS-XE-native:GigabitEthernet': {
        'ip': {
            'address': {
                'primary': {
                    'address': '10.10.10.1',
                    'mask': '255.255.255.0'
                }
            }
        }
    }
}),
verify = False)

# Print the HTTP response code
print('Response Code: ' + str(response.status_code))

```

After the code is run on a Cisco IOS-XE router, the response code is 204. What is the result of the script?

- A. The configuration fails because another interface is already configured with IP address 10.10.10.1/24.
- B. The configuration fails because interface GigabitEthernet2 is missing on the target device.
- C. The configuration is successfully sent to the device in cleartext.
- D. Interface GigabitEthernet2 is configured with IP address 10.10.10.1/24

**Answer: D**

**NEW QUESTION 90**

- (Topic 2)

Refer to the exhibit.

```

Switch1#show lacp internal
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode

Channel group 1

Port      Flags  State    LACP port  Admin  Oper  Port  Port
Port      Flags  State    Priority   Key    Key   Number State
Gi0/0    SP     hot-sby  20         0x1    0x1   0x1   0x5
Gi0/1    SA     bnd1    15         0x1    0x1   0x2   0x3C

```

An engineer attempts to bundle interface Gi0/0 into the port channel, but it does not function as expected. Which action resolves the issue?

- A. Configure channel-group 1 mode active on interface Gi0/0.
- B. Configure no shutdown on interface Gi0/0
- C. Enable fast LACP PDUs on interface Gi0/0.
- D. Set LACP max-bundle to 2 on interface Port-channelM

**Answer: D**

**NEW QUESTION 92**

- (Topic 2)

Which two parameters are examples of a QoS traffic descriptor? (Choose two)

- A. MPLS EXP bits
- B. bandwidth

- C. DSCP
- D. ToS
- E. packet size

**Answer:** AC

**NEW QUESTION 93**

- (Topic 2)

An engineer must create an EEM script to enable OSPF debugging in the event the OSPF neighborship goes down. Which script must the engineer apply?

- event manager applet ENABLE\_OSPF\_DEBUG  
 event syslog pattern "%OSPF-5-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from LOADING to FULL"  
 action 1.0 cli command "enable"  
 action 2.0 cli command "debug ip ospf event"  
 action 3.0 cli command "debug ip ospf adj"  
 action 4.0 syslog priority informational msg "ENABLE\_OSPF\_DEBUG"
- event manager applet ENABLE\_OSPF\_DEBUG  
 event syslog pattern "%OSPF-5-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from LOADING to FULL"  
 action 1.0 cli command "debug ip ospf event"  
 action 2.0 cli command "debug ip ospf adj"  
 action 3.0 syslog priority informational msg "ENABLE\_OSPF\_DEBUG"
- event manager applet ENABLE\_OSPF\_DEBUG  
 event syslog pattern "%OSPF-5-ADJCHG: Process 6, Nbr 1.1.1.1 on Serial0/0 from FULL to DOWN"  
 action 1.0 cli command "enable"  
 action 2.0 cli command "debug ip ospf event"  
 action 3.0 cli command "debug ip ospf adj"  
 action 4.0 syslog priority informational msg "ENABLE\_OSPF\_DEBUG"
- event manager applet ENABLE\_OSPF\_DEBUG  
 event syslog pattern "%OSPF-1-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from FULL to DOWN"  
 action 1.0 cli command "debug ip ospf event"  
 action 2.0 cli command "debug ip ospf adj"  
 action 3.0 syslog priority informational msg "ENABLE\_OSPF\_DEBUG"

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

**Answer:** C

**NEW QUESTION 97**

- (Topic 2)

How does a fabric AP fit in the network?

- A. It is in local mode and must be connected directly to the fabric border node
- B. It is in FlexConnect mode and must be connected directly to the fabric edge switch.
- C. It is in FlexConnect mode and must be connected directly to the fabric border node
- D. It is in local mode and must be connected directly to the fabric edge switch.

**Answer:** D

**NEW QUESTION 100**

- (Topic 2)

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

**Explanation:**

A virtual network identifier (VNI) is a value that identifies a specific virtual network in the data plane.

**NEW QUESTION 104**

- (Topic 1)

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 109**

- (Topic 1)

Which LISP component is required for a LISP site to communicate with a non-LISP site?

- A. ETR
- B. ITR
- C. Proxy ETR
- D. Proxy ITR

**Answer: C**

**NEW QUESTION 113**

- (Topic 1)

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 116**

- (Topic 1)

In cisco SD\_WAN, which protocol is used to measure link quality?

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

**Answer: B**

**Explanation:**

The BFD (Bidirectional Forwarding Detection) is a protocol that detects link failures as part of the Cisco SD-WAN (Viptela) high availability solution, is enabled by default on all vEdge routers, and you cannot disable it.

**NEW QUESTION 117**

- (Topic 1)

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 122**

- (Topic 1)

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 124**

- (Topic 1)

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: D**

**NEW QUESTION 127**

- (Topic 1)

Which features does Cisco EDR use to provide threat detection and response protection?

- A. containment, threat intelligence, and machine learning
- B. firewalling and intrusion prevention
- C. container-based agents
- D. cloud analysis and endpoint firewall controls

**Answer: B**

**NEW QUESTION 128**

- (Topic 1)

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**

**Explanation:**

Coverage defines the ability of wireless clients to connect to a wireless AP with a signal strength and quality high enough to overcome the effects of RF interference. The edge of the coverage for an AP is based on the signal strength and SNR measured as the client device moves away from the AP. The signal strength required for good coverage varies dependent on the specific type of client devices and applications on the network. To accommodate the requirement to support wireless Voice over IP (VoIP), refer to the RF guidelines specified in the Cisco 7925G Wireless IP Phone Deployment Guide. The minimum recommended wireless signal strength for voice applications is -67 dBm and the minimum SNR is 25 dB. The first step in the analysis of a post site survey is to verify the 'Signal Coverage'. The signal coverage is measured in dBm. You can adjust the color-coded signal gauge to your minimum-allowed signal level to view areas where there are sufficient and insufficient coverage. The example in Figure 8 shows blue, green, and yellow areas in the map have signal coverage at -67 dBm or better. The areas in grey on the coverage maps have deficient coverage. Source from Cisco [https://www.cisco.com/c/en/us/td/docs/wireless/technology/vowlan/troubleshooting/vowlan\\_troubleshoot/8\\_Site\\_Survey\\_RF\\_Design\\_Valid.html](https://www.cisco.com/c/en/us/td/docs/wireless/technology/vowlan/troubleshooting/vowlan_troubleshoot/8_Site_Survey_RF_Design_Valid.html)

**NEW QUESTION 133**

- (Topic 1)

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: C**

**NEW QUESTION 138**

- (Topic 1)

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state      conn-id  status
209.165.201.6 209.165.201.1 QM_IDLE    1001    ACTIVE
```

Refer to the exhibit. After configuring an IPsec VPN, an engineer enters the show command to verify the ISAKMP SA status. What does the status show?

- A. ISAKMP SA is authenticated and can be used for Quick Mode.
- B. Peers have exchanged keys, but ISAKMP SA remains unauthenticated.
- C. VPN peers agreed on parameters for the ISAKMP SA
- D. ISAKMP SA has been created, but it has not continued to form.

**Answer: B**

**Explanation:**

The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM\_IDLE, and a Quick Mode exchange begins. <https://www.ciscopress.com/articles/article.asp?p=606584>

**NEW QUESTION 143**

- (Topic 1)

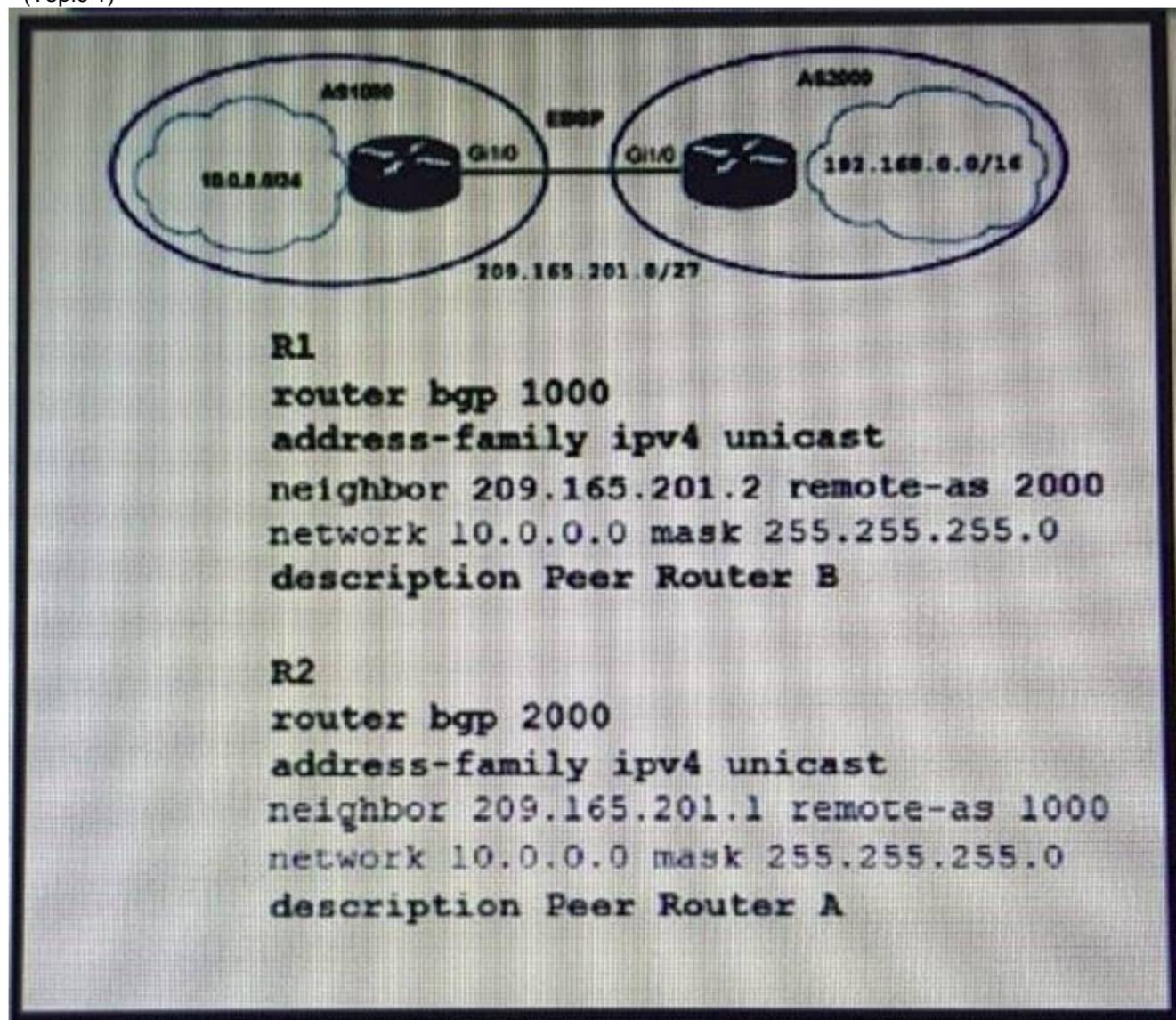
What is the centralized control policy in a Cisco SD-WAN deployment?

- A. list of ordered statements that define user access policies
- B. set of statements that defines how routing is performed
- C. set of rules that governs nodes authentication within the cloud
- D. list of enabled services for all nodes within the cloud

**Answer: B**

**NEW QUESTION 145**

- (Topic 1)



Refer to the exhibit. Which two commands are needed to allow for full reachability between AS 1000 and AS 2000? (Choose two)

- A. R1#network 192.168.0.0 mask 255.255.0.0
- B. R2#no network 10.0.0.0 255.255.255.0
- C. R2#network 192.168.0.0 mask 255.255.0.0
- D. R2#network 209.165.201.0 mask 255.255.192.0
- E. R1#no network 10.0.0.0 255.255.255.0

**Answer:** BC

**NEW QUESTION 149**

- (Topic 1)

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

**Explanation:**

The Cisco TrustSec solution simplifies the provisioning and management of network access control through the use of software-defined segmentation to classify network traffic and enforce policies for more flexible access controls. Traffic classification is based on endpoint identity, not IP address, enabling policy change without network redesign.

**NEW QUESTION 152**

- (Topic 1)

When a wireless client roams between two different wireless controllers, a network connectivity outage is experienced for a period of time. Which configuration issue would cause this problem?

- A. Not all of the controllers in the mobility group are using the same mobility group name.
- B. Not all of the controllers within the mobility group are using the same virtual interface IP address.
- C. All of the controllers within the mobility group are using the same virtual interface IP address.
- D. All of the controllers in the mobility group are using the same mobility group name.

**Answer:** B

**NEW QUESTION 153**

DRAG DROP - (Topic 1)

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 154**

- (Topic 1)

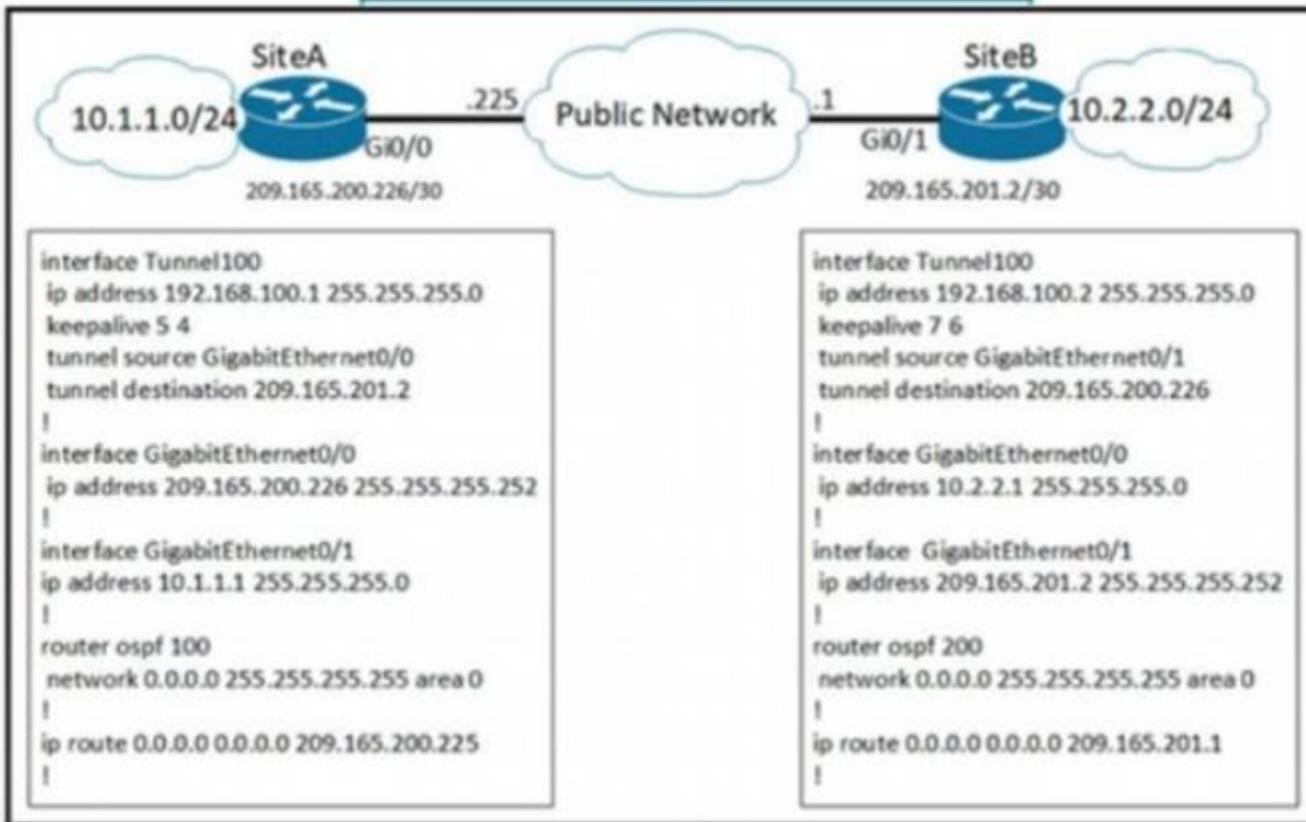
An engineer configures HSRP group 37. The configuration does not modify the default virtual MAC address. Which virtual MAC address does the group use?

- 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 159**

- (Topic 1)



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 164**

- (Topic 1)

Refer to the exhibit.

```

PYTHON CODE:
import requests
import json

url='http://YOUR_IP/ins'
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": "07.01",
          "kickstart_ver_str": "7.0(3)I7(4)",
          "bios_cmt_time": "04/06/2017",
          "kick_file_name": "bootflash://iosx7.0.3.i7.4.bin",
          "kick_cmt_time": "6/14/1970 2:00:00",
          "kick_instmp": "06/14/1970 09:49:04",
          "chassis_id": "Nexus9000 93180YC-EX chassis",
          "cpu_name": "Intel(R) Xeon(R) CPU @ 1.80GHz",
          "memory": 24633486,
          "mem_type": "x86",
          "n_inocs": 134703,
          "tr_ctime": "Sun Mar 10 15:41:46 2019",
          "tr_reason": "Reset Requested by CLI command reload",
          "tr_sys_ver": "7.0(3)I7(4)",
          "tr_service": "",
          "manufacturer": "Cisco Systems, Inc.",
          "TABLE_package_inst": {
            "ROW_package_inst": {
              "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 166**

- (Topic 1)

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 168**

- (Topic 1)

```
%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
```

Refer to me exhibit. 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 171**

- (Topic 1)

Refer to the exhibit.

```
SW1#sh monitor session all
Session 1
-----
Type                : Remote Destination Session
Source RSPAN VLAN   : 50

Session 2
-----
Type                : Local Session
Source Ports        :
  Both              : Fa0/14
Destination Ports   : Fa0/15
Encapsulation       : Native
Ingress             : Disables
```

An engineer configures monitoring on SW1 and enters the show command to verify operation. What does the output confirm?

- A. SPAN session 1 monitors activity on VLAN 50 of a remote switch
- B. SPAN session 2 only monitors egress traffic exiting port FastEthernet 0/14.
- C. SPAN session 2 monitors all traffic entering and exiting port FastEthernet 0/15.
- D. RSPAN session 1 is incompletely configured for monitoring

Answer: D

**Explanation:**

SW1 has been configured with the following commands: SW1(config)#monitor session 1 source remote vlan 50 SW1(config)#monitor session 2 source interface fa0/14 SW1(config)#monitor session 2 destination interface fa0/15

The session 1 on SW1 was configured for Remote SPAN (RSPAN) while session 2 was configured for local SPAN. For RSPAN we need to configure the destination port to complete the configuration.

Note: In fact we cannot create such a session like session 1 because if we only configure Source RSPAN VLAN 50 (with the command monitor session 1 source remote vlan 50) then we will receive a Type: Remote Source Session (not Remote Destination Session).

**NEW QUESTION 173**

- (Topic 1)

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.

Reference: <https://restfulapi.net/security-essentials/>

**NEW QUESTION 176**

- (Topic 1)

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

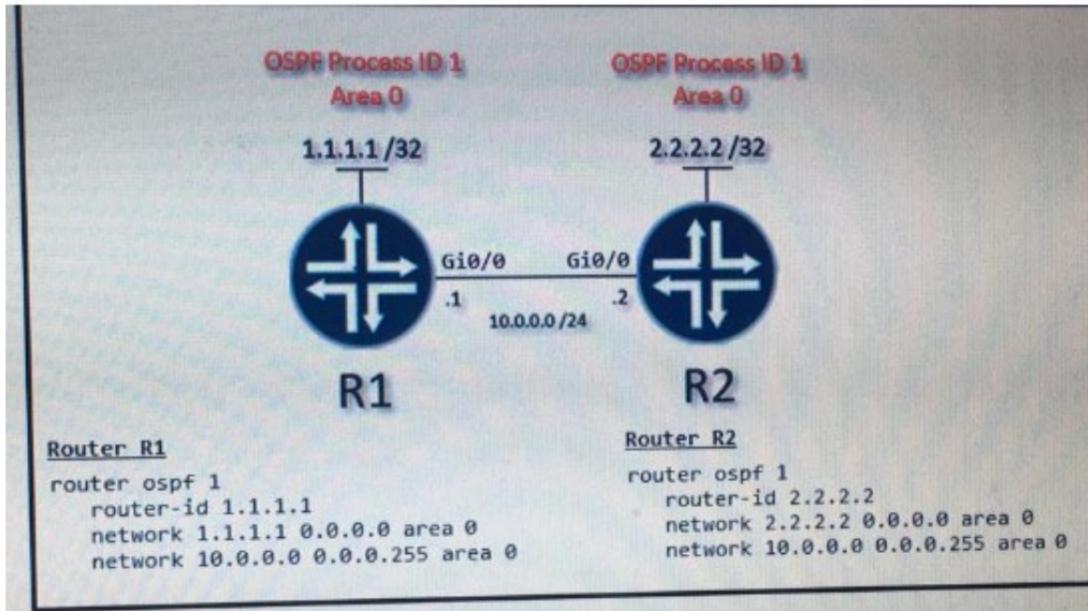
- A. sniffer
- B. monitor
- C. bridge
- D. local

**Answer: B**

**NEW QUESTION 181**

- (Topic 1)

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
    
```

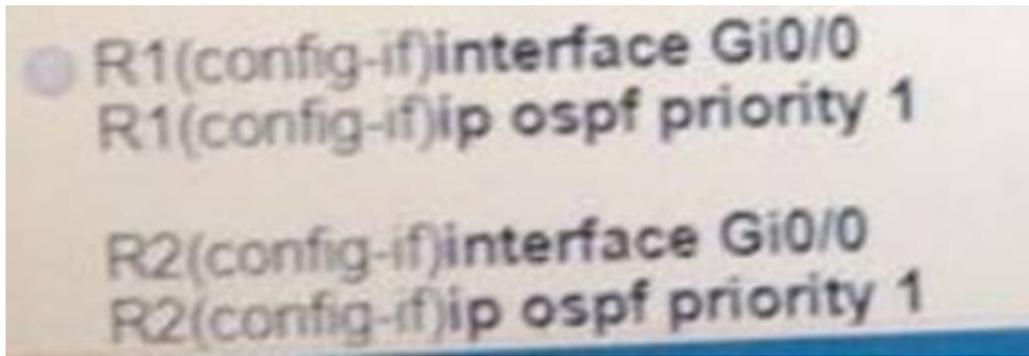
C)

```

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)



- 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-to-point/ 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 185**

- (Topic 1)



Refer to the exhibit. An engineer has configured Cisco ISE to assign VLANs to clients based on their method of authentication, but this is not working as expected. Which action will resolve this issue?

- A. require a DHCP address assignment
- B. utilize RADIUS profiling
- C. set a NAC state
- D. enable AAA override

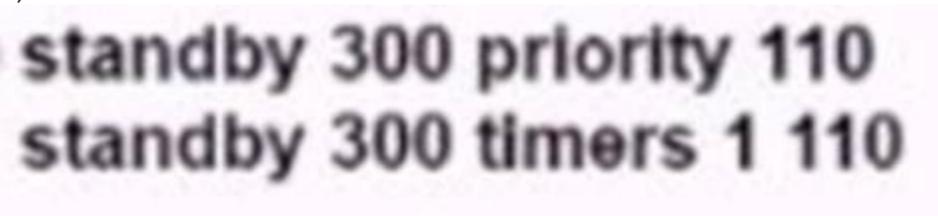
**Answer:** B

**NEW QUESTION 187**

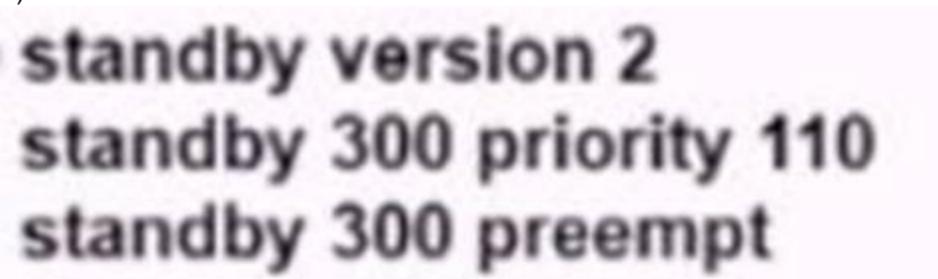
- (Topic 1)

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

A)



B)



C)

**standby 300 priority 90**  
**standby 300 preempt**

D)

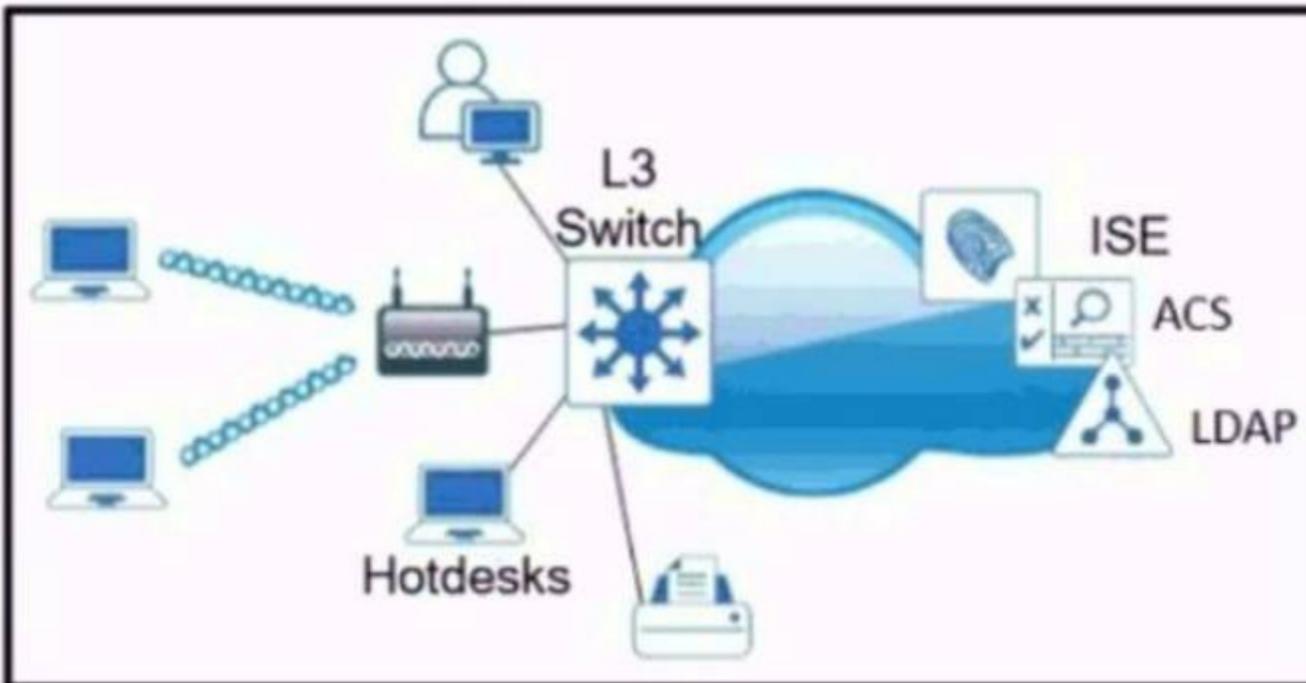
**standby version 2**  
**standby 300 priority 90**  
**standby 300 preempt**

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

**Answer: B**

**NEW QUESTION 188**

- (Topic 1)



Refer to the exhibit Which single security feature is recommended to provide Network Access Control in the enterprise?

- A. MAB
- B. 802.1X
- C. WebAuth
- D. port security sticky MAC

**Answer: B**

**NEW QUESTION 189**

- (Topic 1)

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 is 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 193**

- (Topic 1)

Under which network conditions is an outbound QoS policy that is applied on a router WAN interface most beneficial?

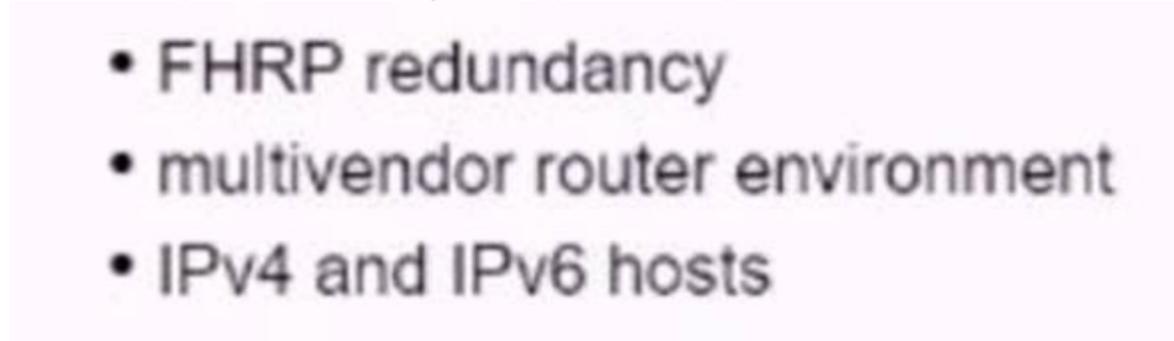
- A. under interface saturation condition
- B. under network convergence condition
- C. under all network condition
- D. under traffic classification and marking conditions.

**Answer: A**

**NEW QUESTION 198**

- (Topic 1)

A customer requests a network design that supports these requirements:



Which protocol does the design include?

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

**Answer: D**

**NEW QUESTION 202**

- (Topic 1)

```

{
  "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": "CS300-24UX",
      "reachabilityFailureReason": "",
      "reachabilityStatus": "Authentication Failed",
      "hostname": "cat9000-1",
      "macAddress": "78:7b:20:67:62:80",
    },
    {
      "family": "Switches and Hubs",
      "interfaceCount": "59",
      "lineCardCount": "2",
      "platformId": "WS-C3850-48U-E",
      "reachabilityFailureReason": "",
      "reachabilityStatus": "Unreachable",
      "hostname": "cat3850-1",
      "macAddress": "cc:d8:c1:15:d2:80",
    }
  ],
  "version": "1.0"
}

```

What does the cisco DNA REST response indicate?

- 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 204**

- (Topic 1)

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: C**

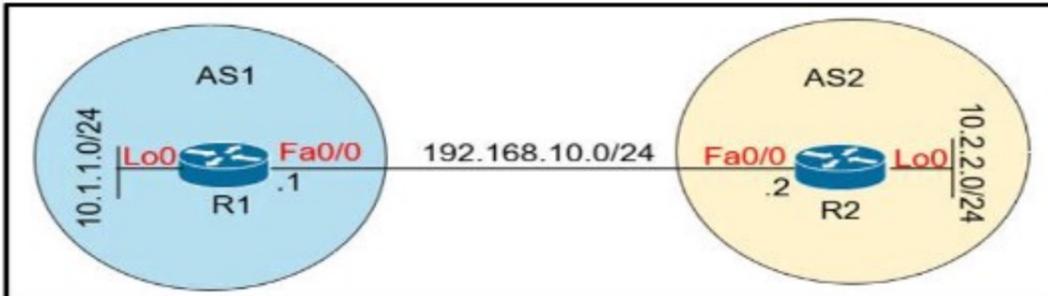
**Explanation:**

Support Virtual Switching System (VSS) to provide resiliency, and increased operational efficiency with a single point of management; VSS increases operational efficiency by simplifying the network, reducing switch management overhead by at least 50 percent. – Single configuration file and node to manage. Removes the need to configure redundant switches twice with identical policies.

**NEW QUESTION 206**

- (Topic 1)

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

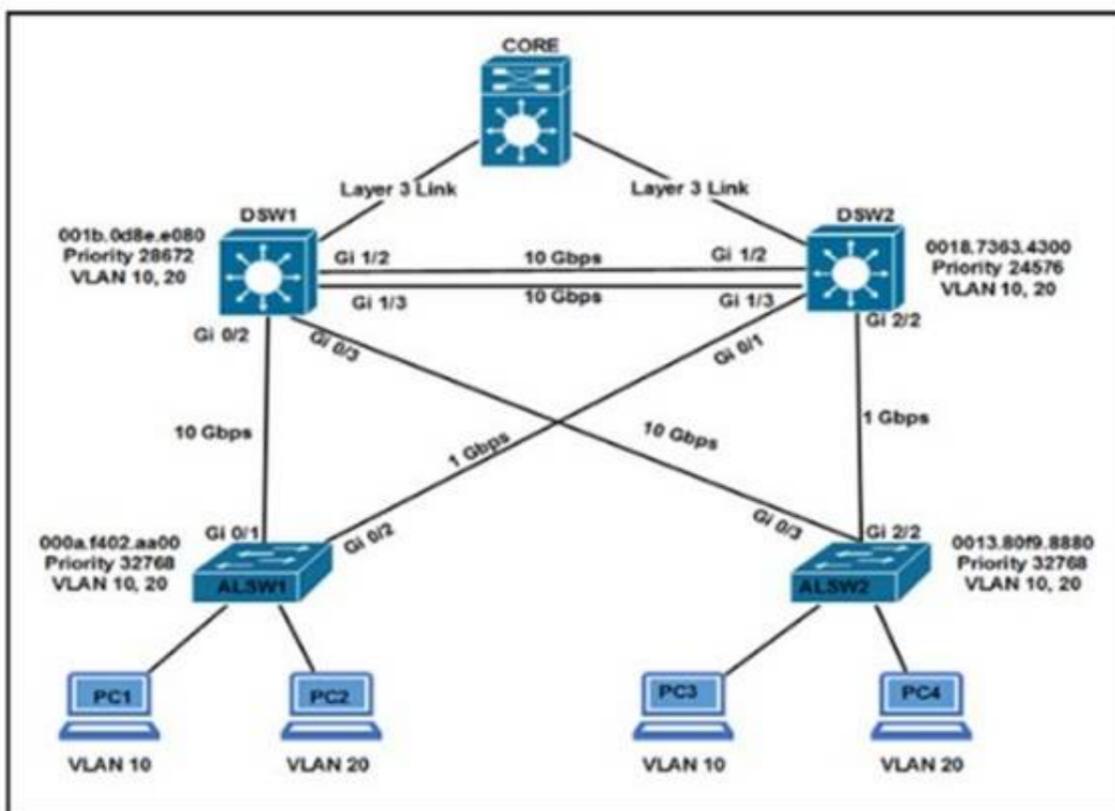
channel to a remote machine where you can use protocol analysis tool (Wireshark, Airopeek, etc) to review the packets and diagnose issues. Strictly used for troubleshooting purposes.

+ 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 209**

- (Topic 4)



Refer to the exhibit. Which two commands ensure that DSW1 becomes root bridge for VLAN 10? (Choose two)

- A. DSW1(config)#spanning-tree vlan 10 priority 4096 Most Voted
- B. DSW1(config)#spanning-tree vlan 10 priority root
- C. DSW2(config)#spanning-tree vlan 10 priority 61440 Most Voted
- D. DSW1(config)#spanning-tree vlan 10 port-priority 0
- E. DSW2(config)#spanning-tree vlan 20 priority 0

**Answer: CD**

**Explanation:**

Ref: Scaling Networks v6 Companion Guide

“STP

...

Extended System ID

...

Bridge Priority

The bridge priority is a customizable value that can be used to influence which switch becomes the root bridge. The switch with the lowest priority, which implies the lowest BID, becomes the root bridge because a lower priority value takes precedence.

...

The default priority value for all Cisco switches is the decimal value 32768. The range is 0 to 61440, in increments of 4096. Therefore, valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. A bridge priority of 0 takes precedence over all other bridge priorities. All other values are rejected.

**NEW QUESTION 214**

- (Topic 4)

What is one characteristic of Cisco DNA Center and vManage northbound APIs?

- A. They push configuration changes down to devices.
- B. They implement the RESTCONF protocol.
- C. They exchange XML-formatted content.
- D. They implement the NETCONF protocol.

**Answer: B**

**NEW QUESTION 218**

- (Topic 4)

What is a characteristic of a traditional WAN?

- A. low complexity and high overall solution scale
- B. centralized reachability, security, and application policies
- C. operates over DTLS and TLS authenticated and secured tunnels
- D. united data plane and control plane

**Answer: D**

**NEW QUESTION 220**

- (Topic 4)

Which two features are available only in next-generation firewalls? (Choose two.)

- A. virtual private network
- B. deep packet inspection
- C. stateful inspection
- D. application awareness
- E. packet filtering

**Answer: CD**

**NEW QUESTION 221**

- (Topic 4)

What is stateful switchover?

- A. mechanism used to prevent routing protocol loops during an RP switchover
- B. mechanism to take control from a failed RP while maintaining connectivity
- C. First Hop Redundancy Protocol for host gateway connectivity
- D. cluster protocol used to facilitate switch failover

**Answer: D**

**NEW QUESTION 222**

DRAG DROP - (Topic 4)

Drag and drop the characteristics from the left onto the routing protocol they describe on the right

supports unequal path load balancing	OSPF
link state routing protocol	
distance vector routing protocol	
metric is based on delay and bandwidth by default	EIGRP
makes it easy to segment the network logically	
constructs three tables as part of its operation: neighbor table, topology table, and routing table	

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

supports unequal path load balancing	OSPF
link state routing protocol	
distance vector routing protocol	
metric is based on delay and bandwidth by default	EIGRP
makes it easy to segment the network logically	
constructs three tables as part of its operation: neighbor table, topology table, and routing table	

**NEW QUESTION 225**

- (Topic 4)

What mechanism does PIM use to forward multicast traffic?

- A. PIM sparse mode uses a pull model to deliver multicast traffic.
- B. PIM dense mode uses a pull model to deliver multicast traffic.
- C. PIM sparse mode uses receivers to register with the RP.
- D. PIM sparse mode uses a flood and prune model to deliver multicast traffic.

**Answer: A**

**Explanation:**

PIM sparse mode uses a pull model to deliver multicast traffic. This means that multicast traffic is only forwarded to routers that have explicitly requested it, using join messages. This reduces the amount of unnecessary traffic on the network and allows for efficient use of bandwidth. The source of this answer is the Cisco ENCOR v1.1 course, module 5, lesson 5.2: Implementing PIM Sparse Mode.

**NEW QUESTION 229**

- (Topic 4)

When a branch location loses connectivity, which Cisco FlexConnect state rejects new users but allows existing users to function normally?

- A. Authentication-Down / Switch-Local
- B. Authentication-Down / Switching-Down
- C. Authentication-Local / Switch-Local
- D. Authentication-Central / Switch-Local

**Answer: A**

**Explanation:**

This is because Cisco FlexConnect is a feature that allows wireless access points to operate in standalone mode when they lose connectivity to the wireless LAN controller. Cisco FlexConnect has different states depending on the status of the authentication and switching functions. Authentication-Down means that the access point cannot authenticate new users with the central server, such as a RADIUS server. Switch-Local means that the access point can switch the traffic locally without sending it to the wireless LAN controller. Therefore, Authentication-Down / Switch-Local is the state that rejects new users but allows existing users to function normally. The source of this answer is the Cisco ENCOR v1.1 course, module 7, lesson 7.3: Implementing FlexConnect.

**NEW QUESTION 231**

- (Topic 4)

A script contains the statement "while loop != 999:" Which value terminates the loop?

- A. A value equal to 999.
- B. A value less than or equal to 999.
- C. A value not equal to 999.
- D. A value greater than or equal to 999.

**Answer: A**

**NEW QUESTION 233**

- (Topic 4)

Why does the vBond orchestrator have a public IP?

to enable vBond to team the public IP of WAN Edge devices that are behind NAT gateways or in private address space

- A. to facilitate downloading and distribution of operational and security patches
- B. to allow for global reachability from all WAN Edges in the Cisco SD-WAN and
- C. to facilitate NAT traversal to provide access
- D. to Cisco Smart Licensing servers for license enablement

**Answer: C**

**NEW QUESTION 238**

- (Topic 4)

```
R1# show ip bgp summary
BGP router identifier 10.255.255.1, local AS number 65000
BGP table version is 1, main routing table version 1

Neighbor      V  AS  MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.255.255.3  4 65000    0         0        1     0     0     Never    Idle

R1# ping 10.255.255.3 source lo0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.255.255.3, timeout is 2 seconds
Packet sent with a source address of 10.255.255.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms

R1# telnet 10.255.255.3 179 /source-interface lo0
Trying 10.255.255.3, 179 . . .
% Destination unreachable; gateway or host down

R1# debug ip tcp transactions
TCP special event debugging is on
R1#
*Sep 12 10:15:07.958: TCB7F0E49C5AA38 created
*Sep 12 10:15:07.958: TCP0: state was LISTEN -> SYNRCVD [179 -> 10.255.255.3(55290)]
*Sep 12 10:15:07.958: TCP: tcb 7F0E49C5AA38 connection to 10.255.255.3:55290, peer MSS 1460, MSS is 516
*Sep 12 10:15:07.958: TCP: pmtu enabled, mss is now set to 1460
*Sep 12 10:15:07.958: TCP: sending SYN, seq 2953990054, ack 2359850152
*Sep 12 10:15:07.958: TCP0: Connection to 10.255.255.3:55290, advertising MSS 1460
*Sep 12 10:15:07.958: TCP0: ICMP destination unreachable received
```

Refer to the exhibit An engineer is troubleshooting a newly configured BGP peering that does not establish What is the reason for the failure?

- A. BGP peer 10 255 255 3 is not configured for peening with R1
- B. Mandatory BOP parameters between R1 and 10 255 255 3 are mismatched
- C. A firewall is blocking access to TCP port 179 on the BGP peer 10 255 255.3
- D. Both BGP pern are configured for passive TCP transport

**Answer: A**

**NEW QUESTION 243**

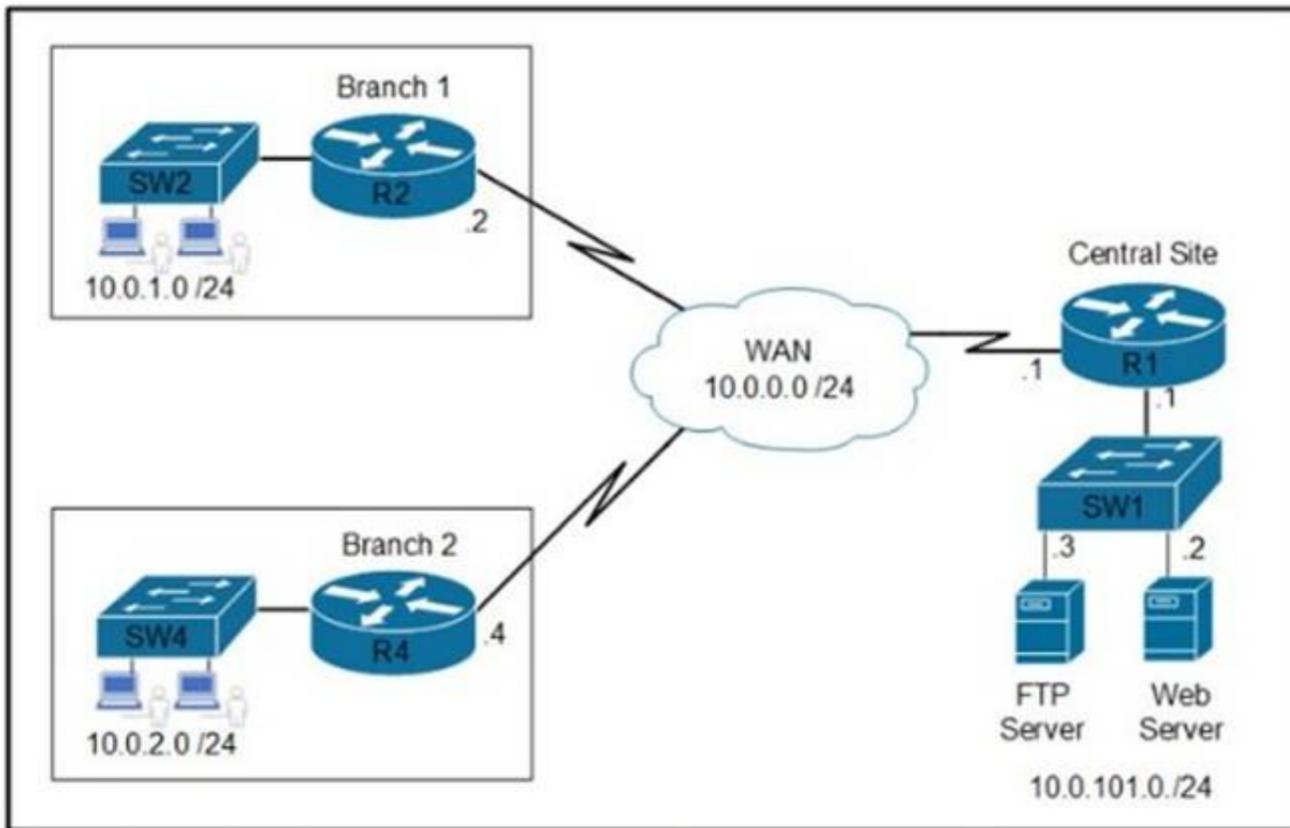
- (Topic 4)

Which solution simplifies management ot secure access to network resources?

- A. RFC 3580-based solution to enable authenticated access leveraging RADIUS and AV pairs
- B. TrustSec to logically group internal user environments and assign policies
- C. 802.1AE to secure communication in the network domain
- D. ISE to automate network access control leveraging RADIUS AV pairs

**Answer: B**

**NEW QUESTION 244**  
 - (Topic 4)



Refer to the exhibit Which two commands are required on route» R1 to block FTP and allow all other traffic from the Branch 2 network' (Choose two)

- access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp-data  
access-list 101 permit ip any any
- access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp  
access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp-data  
access-list 101 permit ip any any
- interface GigabitEthernet0/0  
ip address 10.0.0.1 255.255.255.252  
ip access-group 101 out
- interface GigabitEthernet0/0  
ip address 10.0.101.1 255.255.255.252  
ip access-group 101 in
- access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp  
access-list 101 permit ip any any

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

**Answer: BC**

**NEW QUESTION 247**  
 - (Topic 4)

```
Request URL: https://www.cisco.com/libs/granite/csrf/token.json
Request Method: GET
Status Code: 403
Remote Address: 23.207.65.173:443
Referrer Policy: strict-origin-when-cross-origin
```

Refer to the exhibit. Why was the response code generated?

- A. The resource was unreachable
- B. Access was denied based on the user permissions.
- C. The resource 15 no longer available on the server.
- D. There is a conflict in the current state of the resource.

**Answer: B**

**NEW QUESTION 249**

- (Topic 4)

Refer to the exhibit.

**Recording**

Tracing the route to 172.16.1.2

```

1 172.16.250.1 2 msec
   172.16.250.5 5 msec
   172.16.250.1 2 msec
2 172.16.250.1 2 msec
   172.16.250.5 5 msec
   172.16.250.1 2 msec
3 172.16.1.2 6 msec 5 msec 5 msec
  
```

```

R2# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
Gateway of last resort is not set
C    172.16.0.0/16 is directly connected, Loopback0
   172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.16.40.0/24 is directly connected, Gigabit Ethernet 0/1
D    172.16.1.0/24 [110/7445] via 172.16.250.1, 00:39:08, Gigabit Ethernet 0/0
     [110/7445] via 172.16.250.5, 00:39:08, Gigabit Ethernet 0/4
  
```

Clients are reporting an issue with the voice traffic from the branch site to the central site. What is the cause of this issue?

- A. The voice traffic is using the link with less available bandwidth.
- B. There is a routing loop on the network.
- C. Traffic is load-balancing over both links, causing packets to arrive out of order.
- D. There is a high delay on the WAN links.

**Answer: C**

**Explanation:**

Traffic is load-balancing over both links, causing packets to arrive out of order. This can cause voice quality issues, such as jitter and delay. To avoid this problem, voice traffic should be sent over a single path, using a routing protocol that supports unequal-cost load balancing, such as EIGRP. The source of this answer is the Cisco ENCOR v1.1 course, module 4, lesson 4.3: Implementing EIGRP.

**NEW QUESTION 252**

- (Topic 4)

```

ip access-list extended 101
 10 deny ip any any
!
event manager applet Block_Users
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "interface GigabitEthernet1"
 action 4.0 cli command "ip access-group 101 in"
 action 5.0 cli command "ip access-group 101 out"
  
```

Refer to the exhibit. An engineer builds an EEM script to apply an access list. Which statement must be added to complete the script?

- A. event none
- B. action 2.1 cli command "ip action 3.1 ell command 101"
- C. action 6.0 ell command "ip access-list extended 101"
- D. action 6.0 cli command "ip access-list extended 101"

**Answer: A**

**NEW QUESTION 253**

- (Topic 4)

Refer to the exhibit.

**Add a new network**

Network name

Security type

EAP method

Authentication method

Connect automatically

Connect even if this network is not broadcasting

A company has an internal wireless network with a hidden SSID and RADIUS-based client authentication for increased security. An employee attempts to manually add the company network to a laptop, but the laptop does not attempt to connect to the network. The regulatory domains of the access points and the laptop are identical. Which action resolves this issue?

- A. Ensure that the "Connect even if this network is not broadcasting" option is selected.
- B. Limit the enabled wireless channels on the laptop to the maximum channel range that is supported by the access points.
- C. Change the security type to WPA2-Personal AES.
- D. Use the empty string as the hidden SSID network name.

**Answer: A**

**NEW QUESTION 257**

- (Topic 4)

In the Cisco DNA Center Image Repository, what is a golden image?

- A. The latest software image that is available for a specific device type
- B. The Cisco recommended software image for a specific device type.
- C. A software image that is compatible with multiple device types.
- D. A software image that meets the compliance requirements of the organization.

**Answer: B**

**NEW QUESTION 259**

- (Topic 4)

Which element is unique to a Type 2 hypervisor?

- A. memory
- B. VM OS
- C. host OS
- D. host hardware

**Answer: C**

**NEW QUESTION 262**

- (Topic 4)

Which two methods are used to assign security group tags to the user in a Cisco Trust Sec architecture? (Choose two )

- A. modular QoS
- B. policy routing
- C. web authentication
- D. DHCP
- E. IEEE 802.1x

**Answer: CE**

**NEW QUESTION 263**

DRAG DROP - (Topic 4)

Drag and drop the code snippets from the bottom onto the blanks in the script to convert a Python object into a JSON string. Not all options are used.

```
import json

data = {
    "measurement": "cefcFRUPowerOperStatus",
    "maxDataPoints": 45,
    "alert": "True",
    "errorDescription": None,
    "devices": [{"model": "Cisco 4331 ISR"}, {"model": "Cisco 3500 S"}]
}

obj = json. [ ] (. [ ] ([ [ ] ])

print(obj)
```

JSONEncoder

.encode

data

JSONDecoder

decode

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

obj = json.JSONEncoder().encode(data)

**NEW QUESTION 264**

- (Topic 4)

```
>tracert www.crmABC.com
Tracing route to www.crmABC.com [192.168.100.1]
 0  0ms  0ms  0ms  10.10.10.1
 1  3ms  5ms  3ms  10.10.10.1
 2  4ms  6ms  4ms  10.100.100.1
 3  4ms  6ms  4ms  10.100.200.1
 4  4ms  6ms  4ms  10.100.100.1
 5  4ms  6ms  4ms  10.100.200.1
 6  4ms  6ms  4ms  10.100.100.1
 7  4ms  6ms  4ms  10.100.200.1
<output truncated>
```

Refer to the exhibit Users cannot reach the web server at 192.168 100 1. What is the root cause for the failure?

- A. The server is attempting to load balance between links 10.100 100.1 and 10 100.200.1.
- B. The server is out of service.
- C. There is a loop in the path to the server.
- D. The gateway cannot translate the server domain name.

**Answer:** C

**NEW QUESTION 267**

- (Topic 4)

```
!
interface FastEthernet0/1
 ip address 209.165.200.225 255.255.255.224
 ip nat outside
!
interface FastEthernet0/2
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
!
access-list 10 permit 10.10.10.0 0.0.0.255
!
```

Refer to the exhibit. Which command allows hosts that are connected to FastEthernet0/2 to access the Internet?

- A. ip nat inside source list 10 interface FastEthernet0/1 overload
- B. ip nat inside source list 10 interface FastEthernet0/2 overload
- C. ip nat outside source list 10 interface FastEthernet0/2 overload
- D. ip nat outside source static 209.165.200.225 10.10.10.0 overload

Answer: A

**NEW QUESTION 269**

- (Topic 4)

Which router is elected the IGMP Querier when more than one router is in the same LAN segment?

- A. The router with the shortest uptime
- B. The router with the lowest IP address
- C. The router with the highest IP address
- D. The router with the longest uptime

Answer: B

**NEW QUESTION 270**

- (Topic 4)

Which tool is used in Cisco DNA Center to build generic configurations that are able to be applied on device with similar network settings?

- A. Command Runner
- B. Template Editor
- C. Application Policies
- D. Authentication Template

Answer: B

**NEW QUESTION 272**

- (Topic 4)

Which configuration enables a device to be configured via NETCONF over SSHv2?

A)

```
hostname Device
!
username admin password 0 admin
!
ip domain-name cisco.com
crypto key generate rsa modulus 2048
ip ssh version 2
!
netconf-yang
!
line vty 0 15
 login local
```

B)

```
hostname Device
!
aaa new-model
!
username cisco privilege 15 password cisco
!
ip domain-name cisco.com
crypto key generate rsa modulus 2048
ip ssh version 2
!
aaa authentication login default local
aaa authorization exec default local
!
netconf-yang
netconf ssh
```

C)

```
hostname Device
!
aaa new-model
!
username admin privilege 15 password 0 admin
!
ip domain-name cisco.com
crypto key generate rsa modulus 2048
ip ssh version 2
!
netconf-yang
```

D)

```
hostname Device
!
username cisco1 privilege 15 password 0 cisco1
!
ip domain-name cisco.com
crypto key generate rsa modulus 2048
ip ssh version 2
!
netconf ssh
!
line vty 0 15
login local
```

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

Answer: C

**NEW QUESTION 277**  
SIMULATION - (Topic 4)  
Simulation 10

The image shows a network topology and a terminal window. The topology includes PC-1, ACCESS-SW1, DISTRO-SW1, and DISTRO-SW2. PC-1 is connected to ACCESS-SW1 (E0/0/0) via VLAN100. ACCESS-SW1 (E0/0/1) is connected to DISTRO-SW1 (E0/2) and DISTRO-SW2 (E0/2) via VLAN100. DISTRO-SW1 (E0/3) and DISTRO-SW2 (E0/3) are connected to a PoE switch. The terminal window shows the configuration of VRRP on DISTRO-SW1.

```

ACCESS-SW1  DISTRO-SW1  DISTRO-SW2

DISTRO-SW1#show vrrp br
DISTRO-SW1#show vrrp brief
Interface          Grp Pri Time   Own Pre State  Master addr  Group a
ddr
Vl100              200 200 60218   Y  Master 192.168.1.2 192.168
.1.200
DISTRO-SW1#copy run start
DISTRO-SW1#copy run startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 2067 bytes to 1255 bytes[OK]
DISTRO-SW1#
DISTRO-SW1#
DISTRO-SW1#sh run int vlan 100
Building configuration...

Current configuration : 143 bytes
!
interface Vlan100
 ip address 192.168.1.2 255.255.255.0
 vrrp 200 ip 192.168.1.200
 vrrp 200 timers advertise 20
 vrrp 200 priority 200
end
DISTRO-SW1#
    
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The terminal window shows the configuration of VRRP on DISTRO-SW1. The output of the 'show vrrp brief' command shows that VRRP is configured on interface Vlan100 with group 200, priority 200, and state Master. The configuration is then copied to the startup configuration and verified.

```

ACCESS-SW1  DISTRO-SW1  DISTRO-SW2

DISTRO-SW1#show vrrp br
DISTRO-SW1#show vrrp brief
Interface          Grp Pri Time   Own Pre State  Master addr  Group a
ddr
Vl100              200 200 60218   Y  Master 192.168.1.2 192.168
.1.200
DISTRO-SW1#copy run start
DISTRO-SW1#copy run startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 2067 bytes to 1255 bytes[OK]
DISTRO-SW1#
DISTRO-SW1#
DISTRO-SW1#sh run int vlan 100
Building configuration...

Current configuration : 143 bytes
!
interface Vlan100
 ip address 192.168.1.2 255.255.255.0
 vrrp 200 ip 192.168.1.200
 vrrp 200 timers advertise 20
 vrrp 200 priority 200
end
DISTRO-SW1#
    
```

```

ACCESS-SW1  DISTRO-SW1  DISTRO-SW2
Building configuration...

Current configuration : 90 bytes
!
interface Vlan100
 ip address 192.168.1.3 255.255.255.0
 vrrp 200 ip 192.168.1.200
end
DISTRO-SW1#show vrrp brief
Interface      Grp Pri Time  Own Pre State  Master addr  Group a
ddr
Vl100         200 200 60218      Y  Master 192.168.1.2 192.168
.1.200
DISTRO-SW1#

```

**NEW QUESTION 278**

DRAG DROP - (Topic 4)

Drag and drop the code snippets from the bottom onto the blanks in the Python script to convert a Python object into a JSON string. Not all options are used.

```

import [ ]

data = {
    "measurement": "freeMemory",
    "maxDataPoints": 30,
    "alert": True,
    "policy": "1.2.1",
    "devices": [{"model": "Cisco 2921 ISR", "ipv4": '10.10.10.1'}]
}
model = data["devices"][0]["model"]

json_string = [ ] (data)

print( [ ] )

```

- model
- json.loads
- json
- json\_string
- json.dumps

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

<https://stackoverflow.com/questions/45834577/turn-python-object-into-json-output>

**NEW QUESTION 283**

DRAG DROP - (Topic 4)

Drag and drop the characteristics from the left onto the switching mechanisms they describe on the right.

The forwarding table is created in advance.	Cisco Express Forwarding
The router processor is involved with every forwarding decision.	
All forwarding decisions are made in software.	Process Switching
All packets are switched using hardware.	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

The forwarding table is created in advance.	Cisco Express Forwarding
The router processor is involved with every forwarding decision.	
All forwarding decisions are made in software.	Process Switching
All packets are switched using hardware.	

**NEW QUESTION 288**

- (Topic 4)  
 Refer to the exhibit. What is the result of this Python code?

- A. 1
- B. 7
- C. 7.5

**Answer:** D

**Explanation:**

The Python code in the exhibit defines a function called average that takes two parameters a and b and returns the arithmetic mean of them. The function is then called with the arguments 5 and 10, which are assigned to a and b respectively. The function returns (5 + 10) / 2, which is 7.5. Therefore, the result of the Python code is 7.5. References: Python Functions, Python Arithmetic Operators

**NEW QUESTION 289**

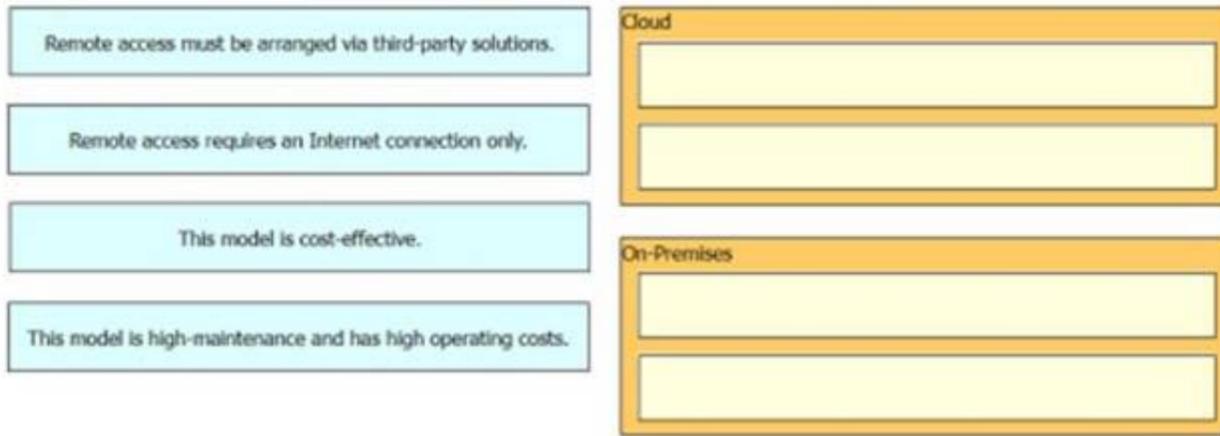
- (Topic 4)  
 A network administrator is preparing a Python scrip to configure a Cisco IOS XE-based device on the network. The administrator is worried that colleagues will make changes to the device while the script is running. Which operation of he in client manager prevent colleague making changes to the device while the scrip is running?

- A. m.lock(config='running')
- B. m.lock(target='running')
- C. m.freeze(target='running')
- D. m.freeze(config='running')

**Answer:** B

**NEW QUESTION 293**

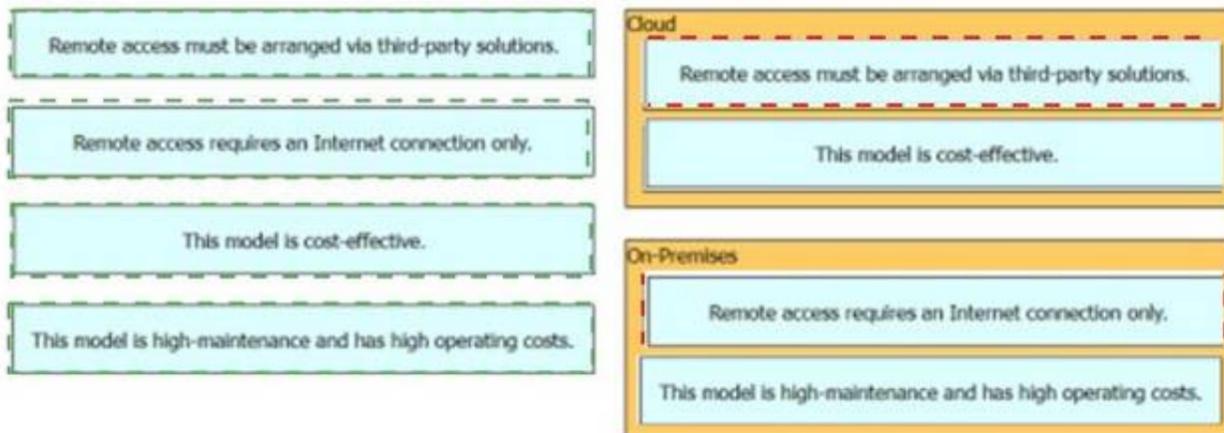
DRAG DROP - (Topic 4)  
 Drag and drop the characteristics from the left onto the deployment models on the right.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



**NEW QUESTION 296**

- (Topic 4)

Which of the following fiber connector types is the most likely to be used on a network interface card?

- A. LC
- B. SC
- C. ST
- D. MPO

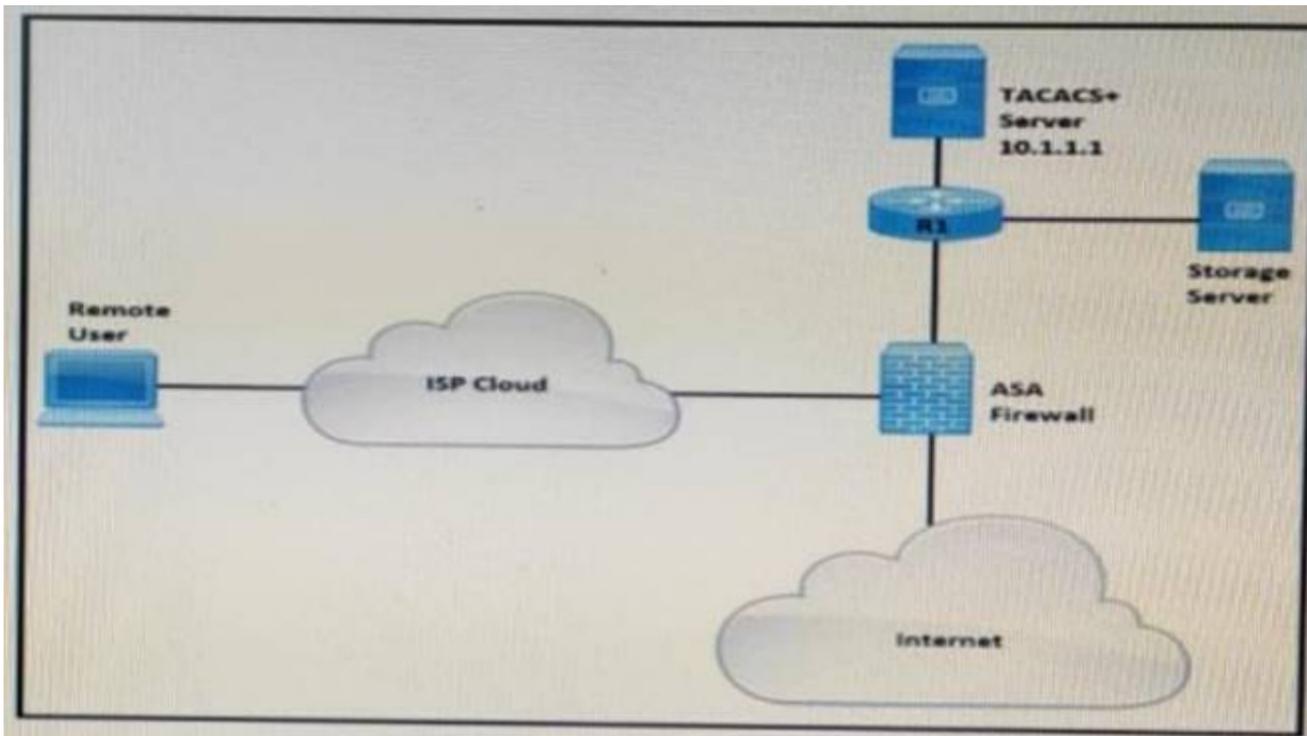
Answer: A

Explanation:

This is because the LC connector is a small form factor connector that is commonly used on network interface cards (NICs) and transceivers. The LC connector has a push-pull locking mechanism that makes it easy to insert and remove. The LC connector can support both single-mode and multimode fibers. The LC connector is also compatible with the SFP and SFP+ transceiver modules that are widely used on NICs. The source of this answer is the Cisco ENCOR v1.1 course, module 1, lesson 1.3: Comparing Copper and Fiber Cabling.

**NEW QUESTION 300**

- (Topic 4)



Refer to the exhibit Remote users cannot access the Internet but can upload files to the storage server Which configuration must be applied to allow Internet access?

- A)
 

```
ciscoasa (config)# access-list MAIL_AUTH extended permit tcp any any eq www
ciscoasa (config)# aaa authentication listener http inside redirect
```
- B)
 

```
ciscoasa(config)# access-list MAIL_AUTH extended permit tcp any any eq http
ciscoasa(config)# aaa authentication listener http inside port 43
```
- C)
 

```
ciscoasa(config)# access-list HTTP_AUTH extended permit udp any any eq http
ciscoasa(config)# aaa authentication listener http outside port 43
```
- D)
 

```
ciscoasa(config)# access-list MAIL_AUTH extended permit udp any any eq http
ciscoasa(config)# aaa authentication listener http outside redirect
```

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

**Answer: A**

**NEW QUESTION 301**

- (Topic 4)

An engineer must configure a multicast UDP jitter operation. Which configuration should be applied?

- A)
 

```
Router(config)#ip sla 1
Router(config)#udp-jitter 192.0.2.115 65051 num-packets 20
```
- B)
 

```
Router(config)#ip sla 1
Router(config)#udp jitter 10.0.0.1 source-ip 192.168.1.1
```
- C)
 

```
Router(config)#ip sla 1
Router(config)#udp-jitter 192.0.2.115 65051
```
- D)
 

```
Router(config)#ip sla 1
Router(config)#udp jitter 239.1.1.1 65051 end-point list List source-ip 192.168.1.1
```

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

Answer: D

**NEW QUESTION 306**

- (Topic 4)

How does Cisco Express Forwarding switching differ from process switching on Cisco devices?

- A. Cisco Express Forwarding switching uses adjacency tables built by the CDP protocol, and process switching uses the routing table.
- B. Cisco Express Forwarding switching uses dedicated hardware processors, and process switching uses the main processor.
- C. Cisco Express Forwarding switching saves memory by storing adjacency tables in dedicated memory on the line cards, and process switching stores all tables in the main memory.
- D. Cisco Express Forwarding switching uses a proprietary protocol based on IS-IS for MAC address lookup, and process switching uses the MAC address table.

Answer: C

**NEW QUESTION 311**

- (Topic 4)

Which NTP mode must be activated when using a Cisco router as an NTP authoritative server?

- A. primary
- B. server
- C. broadcast client
- D. peer

Answer: D

**NEW QUESTION 313**

SIMULATION - (Topic 4)

Simulation 02

Configure HSRP between DISTRO-SW1 and DISTRO-SW2 on VLAN 100 for hosts connected to ACCESS-SW1 to achieve these goals:

- \* 1. Configure group number 1 using the virtual IP address of 192.168.1.1/24.
- \* 2. Configure DISTRO-SW1 as the active router using a priority value of 110 and DISTRO-SW2 as the standby router.
- \* 3. Ensure that DISTRO-SW2 will take over the active role when DISTRO-SW1 goes down, and when DISTRO-SW1 recovers, it automatically resumes the active role.

The screenshot shows a simulation environment with a 'Tasks' tab. The instructions are: 'Configure HSRP between DISTRO-SW1 and DISTRO-SW2 on VLAN100 for hosts connected to ACCESS-SW1 to achieve these goals: 1. Configure group number 1 using the virtual IP address of 192.168.1.1 /24. 2. Configure DISTRO-SW1 as the active router using a priority value of 110 and DISTRO-SW2 as the standby router. 3. Ensure that DISTRO-SW2 will take over the active role when DISTRO-SW1 goes down, and when DISTRO-SW1 recovers, it automatically resumes the active role.' To the right is a terminal window for DISTRO-SW1 with the prompt 'DISTRO-SW1>'.

The screenshot shows a network topology diagram and a terminal window. The topology includes PC-1 connected to Access-SW1 (VLAN 100, IP 192.168.1.100). Access-SW1 is connected to DISTRO-SW1 (VLAN 100, IP 192.168.1.2) and DISTRO-SW2 (VLAN 100, IP 192.168.1.3). The terminal window for DISTRO-SW1 shows the prompt 'DISTRO-SW1>'.

```

DISTRO-SW1#sh run
DISTRO-SW1#sh running-config
Building configuration...

Current configuration : 1661 bytes
!
! Last configuration change at 02:15:58 PST Fri May 20 2022
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname DISTRO-SW1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
!

```

```

hostname DISTRO-SW1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
!
!
!
!
!
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.2
ip dhcp excluded-address 192.168.1.3
ip dhcp excluded-address 192.168.1.100
!
ip dhcp pool CISCO123
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
!
!
!
ip cef
no ip igmp snooping
no ipv6 cef
!
!

```

```

!
interface Port channel1
switchport trunk encapsulation dot1q
switchport trunk native vlan 100
switchport mode trunk
!
interface Ethernet0/0
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 100
switchport mode trunk
!
interface Ethernet0/2
switchport trunk encapsulation dot1q
switchport trunk native vlan 100
switchport mode trunk
channel-group 1 mode active
!
interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport trunk native vlan 100
switchport mode trunk
channel-group 1 mode active
!
interface Vlan100
ip address 192.168.1.2 255.255.255.0
!

```



```

!
interface Ethernet0/1
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 100
  switchport mode trunk
!
interface Ethernet0/2
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 100
  switchport mode trunk
  channel-group 1 mode passive
!
interface Ethernet0/3
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 100
  switchport mode trunk
  channel-group 1 mode passive
!
interface Vlan100
  ip address 192.168.1.3 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!

```

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

DISTRO-SW1  
 Sw1  
 int vlan 100  
 standby 1 ip 192.168.1.1  
 standby 1 priority 110  
 standby 1 preempt copy run start  
 DISTRO-SW2 SW2  
 int vlan 100  
 standby 1 ip 192.168.1.1  
 standby 1 preempt  
 copy run start  
 OR  
 MINOR CHANGE IN ABOVE HSRP SCENERIO

Implement GLBP between DISTRO-SW1 and DISTRO-SW2 on VLAN100 for hosts connected to ACCESS-SW1 to achieve these goals:

1. Configure group 1 using the virtual IP address of 192.168.1.254.
2. Configure DISTRO-SW1 as the AVG using a priority value of 110.
3. If DISTRO-SW1 suffers a failure and recovers, ensure that it automatically resumes the AVG role after waiting for a minimum of 15 seconds.

Description automatically generated

Check the IP address 1.254 check the minimum 15 seconds solution get change.

DISTRO-SW1

Sw1

```
int vlan 100
```

```
glbp 1 ip 192.168.1.254
```

```
glbp 1 priority 110
```

```
glbp 1 timers 5 15
```

```
glbp 1 preempt
```

```
copy run start
```

DISTRO-SW2 SW2

```
int vlan 100
```

```
glbp 1 ip 192.168.1.254
```

```
glbp 1 timers 5 15
```

```
glbp 1 preempt copy run start
```

**NEW QUESTION 316**

- (Topic 4)

```

1 def main():
2     vlans = {'vlan10':'192.168.1.0',
3             'vlan20':'192.168.2.0',
4             'vlan30':'192.168.3.0' }
5     vlans_key(vlans)
6
7 def vlans_key(vlans):
8     for key in vlans.keys():
9         print(str(key) + ' ' + str(vlans[key]))
10
11 if __name__ == '__main__':
12     main()

```

Refer to the exhibit. What is printed to the console when this script is run?

- A. a key-value pair in tuple type
- B. a key-value pair in list type
- C. a key-value pair in string type
- D. an error

**Answer: C**

**NEW QUESTION 320**

- (Topic 4)

High bandwidth utilization is occurring on interface Gig0/1 of a router. An engineer must identify the flows that are consuming the most bandwidth. Cisco DNA Center is used as a flow exporter and is configured with the IP address 192.168.23.1 and UDP port 23000. Which configuration must be applied to set NetFlow data export and capture on the router?

A)

```
R1(config)# ip flow-export version 9
R1(config)# ip flow-export destination 192.168.23.1 23000
R1(config)# interface Gig0/1
R1(config-if)# ip flow-top-talkers
```

B)

```
R1(config)# ip flow-export
R1(config)# ip flow-export destination 192.168.23.1
R1(config)# interface Gig0/1
R1(config-if)# collect counter bytes
R1(config-if)# collect counter packets
```

C)

```
R1(config)# ip flow-export
R1(config)# ip flow-export destination 192.168.23.1 23000
R1(config)# interface Gig0/1
R1(config-if)# ip flow monitor
```

D)

```
R1(config)# ip flow-export version 9
R1(config)# ip flow-export destination 192.168.23.1 23000
R1(config)# interface Gig0/1
R1(config-if)# ip flow ingress
R1(config-if)# ip flow egress
```

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

**Answer:** A

**Explanation:**

Option A is the correct configuration to set NetFlow data export and capture on the router. This option enables NetFlow data export to the Cisco DNA Center with the IP address 192.168.23.1 and UDP port 23000, and also enables the ip flow-top-talkers command on the interface Gig0/1. The ip flow-top-talkers command displays the top talkers (the source and destination pairs that are consuming the most bandwidth) on the interface, based on the NetFlow statistics collected by the router<sup>1,2</sup>.

Option B is incorrect because it does not enable the ip flow-top-talkers command on the interface Gig0/1, which is required to identify the flows that are consuming the most bandwidth. The collect counter bytes command is used to specify the fields to be collected by Flexible NetFlow, which is a different feature from NetFlow<sup>3</sup>.

Option C is incorrect because it does not specify the UDP port for the NetFlow data export destination, which is required to send the NetFlow packets to the Cisco DNA Center. The default UDP port for NetFlow is 9996, which does not match the port configured on the Cisco DNA Center<sup>4</sup>.

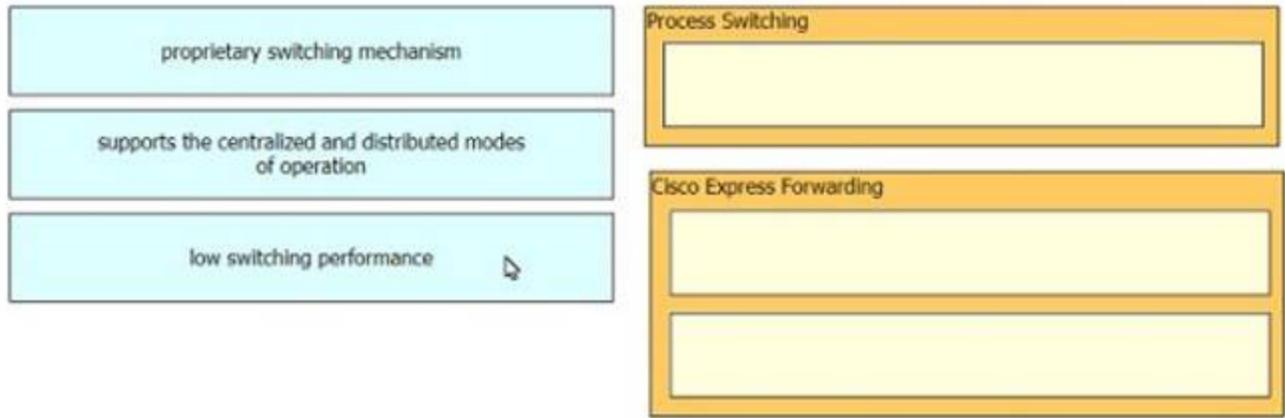
Option D is incorrect because it does not enable NetFlow data export on the router, which is required to send the NetFlow statistics to the Cisco DNA Center. The ip flow-export source command is used to specify the source IP address of the NetFlow packets, but it does not enable the NetFlow data export feature<sup>4</sup>.

References: 1: ip flow-top-talkers, 2: Capture NetFlow data, 3: collect counter bytes, 4: ip flow-export destination

**NEW QUESTION 322**

DRAG DROP - (Topic 4)

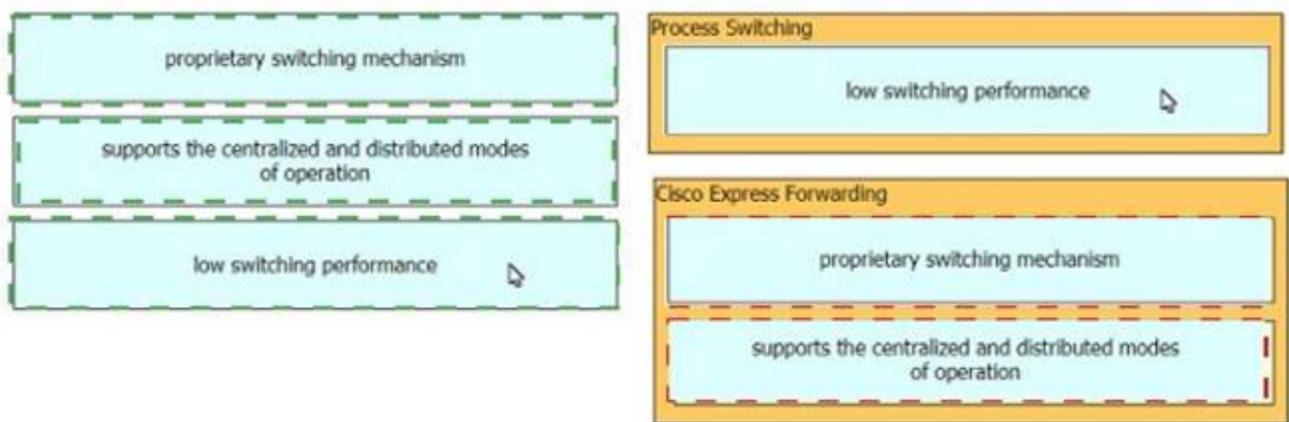
Drag and drop the characteristics from the left onto the switching architectures on the right.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



**NEW QUESTION 324**

- (Topic 2)

An engineer must create a new SSID on a Cisco 9800 wireless LAN controller. The client has asked to use a pre-shared key for authentication Which profile must the engineer edit to achieve this requirement?

- A. RF
- B. Policy
- C. WLAN
- D. Flex

**Answer:** B

**Explanation:**

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116880-config-wpa2-psk-00.html>

**NEW QUESTION 326**

- (Topic 2)

Refer to the exhibit.

```

AP(config)# aaa group server radius rad_auth
AP(config-sg-radius)# server 10.0.0.3 auth-port 1645 acct-port 1646
AP(config)# aaa new-model
AP(config)# aaa authentication login eap_methods group rad_auth
AP(config)# radius-server host 10.0.0.3 auth-port 1645 acct-port 1646 key
labapl200
AP(config)# interface dot11radio 0
AP(config-if)# ssid labapl200
AP(config-if-ssid)# encryption mode wep mandatory
    
```

A company requires that all wireless users authenticate using dynamic key generation. Which configuration must be applied?

- A. AP(config-if-ssid)# authentication open wep wep\_methods
- B. AP(config-if-ssid)# authentication dynamic wep wep\_methods
- C. AP(config-if-ssid)# authentication dynamic open wep\_dynamic
- D. AP(config-if-ssid)# authentication open eap eap\_methods

**Answer: D**

**NEW QUESTION 330**

- (Topic 2)  
 What is YANG used for?

- A. scraping data via CLI
- B. processing SNMP read-only polls
- C. describing data models
- D. providing a transport for network configuration data between client and server

**Answer: C**

**NEW QUESTION 333**

- (Topic 2)  
 Refer to the exhibit.

```

R1#show ip bgp
BGP table version is 32, local router ID is 192.168.101.5
Status codes: S suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
    
```

	Network	Next Hop	Metric	LocPrf	Weight	Path
*	192.168.102.0	192.168.101.18	80		0	64517 i
*		192.168.101.14	80	80	0	64516 i
*		192.168.101.10			0	64515 64515 i
*>		192.168.101.2			32768	64513 i
*		192.168.101.6		80	0	64514 64514 i

Which IP address becomes the active next hop for 192.168.102 0/24 when 192.168.101.2 fails?

- A. 192.168.101.18
- B. 192.168.101.6
- C. 192.168.101.10
- D. 192.168.101.14

**Answer: A**

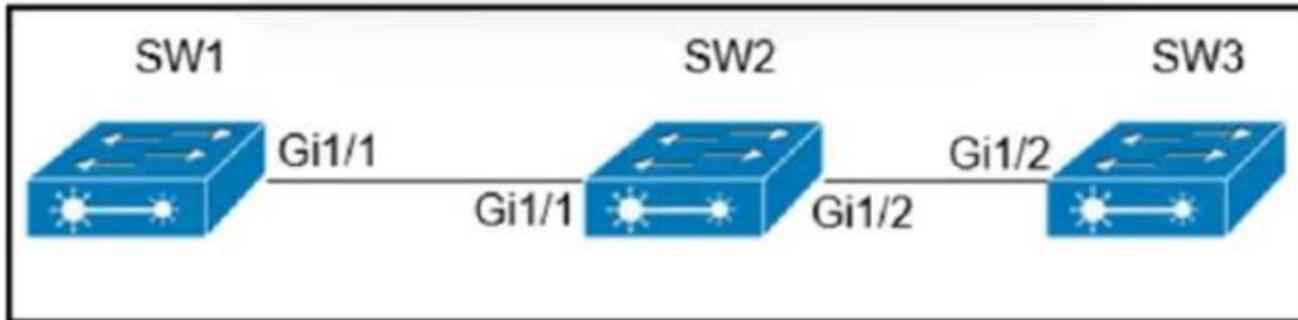
**Explanation:**

The '>' shown in the output above indicates that the path with a next hop of 192.168.101.2 is the current best path. Path Selection Attributes: Weight > Local Preference > Originate > AS Path > Origin > MED > External > IGP Cost > eBGP Peering > Router ID  
 BGP prefers the path with highest weight but the weights here are all 0 (which indicate all routes that are not originated by the local router) so we need to check the Local Preference.

Answer  
 '192.168.101.18' path without LOCAL\_PREF (LocPrf column) means it has the default value of 100.  
 Therefore we can find the two next best paths with the next hop of 192.168.101.18 and 192.168.101.10.  
 We have to move to the next path selection attribute: Originate. BGP prefers the path that the local router originated (which is indicated with the "next hop 0.0.0.0"). But none of the two best paths is self-originated.  
 The AS Path of the next hop 192.168.101.18 is shorter than the AS Path of the next hop 192.168.101.10 then the next hop 192.168.101.18 will be chosen as the next best path.

**NEW QUESTION 338**

- (Topic 4)



Company policy restricts VLAN 10 to be allowed only on SW1 and SW2. All other VLANs can be on all three switches. An administrator has noticed that VLAN 10 has propagated to SW3. Which configuration corrects the issue?

- A. SW1(config)#intgi1/1SW1(config)#switchport trunk allowed vlan 1-9,11-4094
- B. SW2(config)#intgi1/2 SW2(config)#switchport trunk allowed vlan 10
- C. SW2(config)#int gi1/2SW2(config)#switchport trunk allowed vlan 1-9,11-4094
- D. SW1(config)#intgi1/1 SW1(config)#switchport trunk allowed vlan 10

**Answer: C**

**NEW QUESTION 340**

- (Topic 4)

A company recently decided to use RESTCONF instead of NETCONF and many of their NETCONF scripts contain the operation <edit-config>(operation="create"). Which RESTCONF operation must be used to replace these statements?

- A. POST
- B. GET
- C. PUT
- D. CREATE

**Answer: A**

**NEW QUESTION 341**

- (Topic 4)

A network administrator received reports that a 40Gb connection is saturated. The only server the administrator can use for data collection in that location has a 10Gb connection to the network. Which of the following is the best method to use on the server to determine the source of the saturation?

- A. Port mirroring
- B. Log aggregation
- C. Flow data
- D. Packet capture

**Answer: C**

**Explanation:**

This is because flow data is a method of collecting and analyzing information about the traffic flows on a network. Flow data can provide details such as the source and destination IP addresses, ports, protocols, and bytes transferred for each flow. Flow data can help identify the source of the saturation by showing which hosts and applications are generating or consuming the most bandwidth. Flow data can be collected using protocols such as NetFlow, IPFIX, or sFlow. The source of this answer is the Cisco ENCOR v1.1 course, module 10, lesson 10.1: Implementing NetFlow and IPFIX.

**NEW QUESTION 346**

- (Topic 4)

Refer to the exhibit.

```

SW1#show cdp neighbors | include Local|0/1
Device ID    Local intrfce  Holdtme  Capability Platform Port ID
SW2         Fas 0/1       131      R S WS-C3750- Fas 0/1

SW1#show interfaces FastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On

SW2#show cdp neighbors | include Local|0/1
Device ID    Local intrfce  Holdtme  Capability Platform Port ID
SW1         Fas 0/1       142      R S WS-C3750- Fas 0/1

SW2#show interfaces FastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: isl
Operational Trunking Encapsulation: native
Negotiation of Trunking: On

```

An engineer configures a trunk between SW1 and SW2 but tagged packets are not passing. Which action fixes the issue?

- A. Configure SW1 with dynamic auto mode on interface FastEthernet0/1.
- B. Configure the native VLAN to be the same VLAN on both switches on interface FastEthernet0/1.
- C. Configure SW2 with encapsulation dot1q on interface FastEthernet0/1.
- D. Configure FastEthernet0/1 on both switches for static trunking.

**Answer: C**

**NEW QUESTION 347**

- (Topic 4)

In a wireless network environment, what is calculated using the numerical values of the transmitter power level, cable loss, and antenna gain?

- A. EIRP
- B. RSSI
- C. SNR
- D. bBi

**Answer: A**

**NEW QUESTION 352**

- (Topic 4)

Which of the following are examples of Type 2 hypervisors? (Choose three.)

- A. VMware ESXi
- B. Oracle VirtualBox
- C. Oracle Solaris Zones
- D. Microsoft Hyper-V
- E. Microsoft Virtual PC

**Answer: BCE**

**NEW QUESTION 353**

- (Topic 4)

Using the EIRP formula, what parameter is subtracted to determine the EIRP value?

- A. transmitter power
- B. antenna cable loss
- C. antenna gain
- D. signal-to-noise ratio

**Answer: B**

**NEW QUESTION 357**

- (Topic 4)

How do OSPF and EIGRP compare?

- A. OSPF and EIGRP use the same administrative distance.
- B. Both OSPF and EIGRP use the concept of areas.
- C. EIGRP shows a known route, and OSPF shows successor and feasible successor routes.
- D. EIGRP shows successor and feasible successor routes, and OSPF shows all known routes.

**Answer: D**

**NEW QUESTION 362**

- (Topic 4)  
 Why would a customer implement an on-premises solution instead of a cloud solution?

- A. On-premises Offers greater compliance for government regulations than cloud
- B. On-premises offers greater scalability than cloud.
- C. On-premises offers shorter deployment time than cloud.
- D. On-premises is more secure than cloud.

**Answer: D**

**NEW QUESTION 364**

- (Topic 4)  
 What is the function of vBond in a Cisco SD-WAN deployment?

- A. initiating connections with SD-WAN routers automatically
- B. pushing of configuration toward SD-WAN routers
- C. onboarding of SD-WAN routers into the SD-WAN overlay
- D. gathering telemetry data from SD-WAN routers

**Answer: C**

**NEW QUESTION 366**

- (Topic 4)  
 Refer to the exhibit.

```
router#debug ip packet detail 100
IP packet debugging is on (detailed) for access list 100
router#

12:11:05: IP: s=1.1.1.1 (Serial1/0), d=10.1.1.1 (Serial3/0),
g=10.1.1.1, len 100, forward
12:11:05:      ICMP type=0, code=0
12:11:05: IP: s=1.1.1.1 (Serial1/0), d=10.1.1.1 (Serial3/0),
g=10.1.1.1, len 100, forward
12:11:05:      ICMP type=0, code=0
12:11:05: IP: s=1.1.1.1 (Serial1/0), d=10.1.1.1 (Serial3/0),
g=10.1.1.1, len 100, forward
12:11:05:      ICMP type=0, code=0
```

A network engineer issues the debug command while troubleshooting a network issue. What does the output confirm?

- A. ACL100 is tracking ICMP traffic from 1.1.1.1 destined for 10.1.1.1.
- B. ACL100 is tracking all traffic from 10.1.1.1 destined for 1.1.
- C. ACL100 is tracking ICMP traffic from 10.1.1.1 destined for 11.1.1
- D. ACL100 is tracking ICMP traffic from Serial 1/0 destined for Serial3/0.

**Answer: A**

**NEW QUESTION 367**

DRAG DROP - (Topic 3)  
 Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.

declarative	Chef
communicates using knife tool	
communicates through SSH	SaltStack
procedural	

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Chef  
 Communicates using knife tool Procedural  
 SaltStack  
 Communicates through SSH Declarative

**NEW QUESTION 370**

- (Topic 3)

Which two Cisco SD-Access components provide communication between traditional network elements and controller layer? (choose two)

- A. network data platform
- B. network underlay
- C. fabric overlay
- D. network control platform
- E. partner ecosystem

**Answer: BC**

**NEW QUESTION 374**

- (Topic 3)

What is a characteristic of a WLC that is in master controller mode?

- A. All wireless LAN controllers are managed by the master controller.
- B. All new APs that join the WLAN are assigned to the master controller.
- C. Configuration on the master controller is executed on all wireless LAN controllers.
- D. The master controller is responsible for load balancing all connecting clients to other controllers

**Answer: B**

**Explanation:**

When should I use the master controller mode on a WLC? – When there is a master controller enabled, all newly added access points with no primary, secondary, or tertiary controllers assigned associate with the master controller on the same subnet. Reference: <https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/69561-wlc-faq.html>

**NEW QUESTION 375**

- (Topic 3)

**Router R1**

```
interface Ethernet0
ip address 131.108.1.1 255.255.255.0
interface Loopback1
ip address 1.1.1.1 255.255.255.255
```

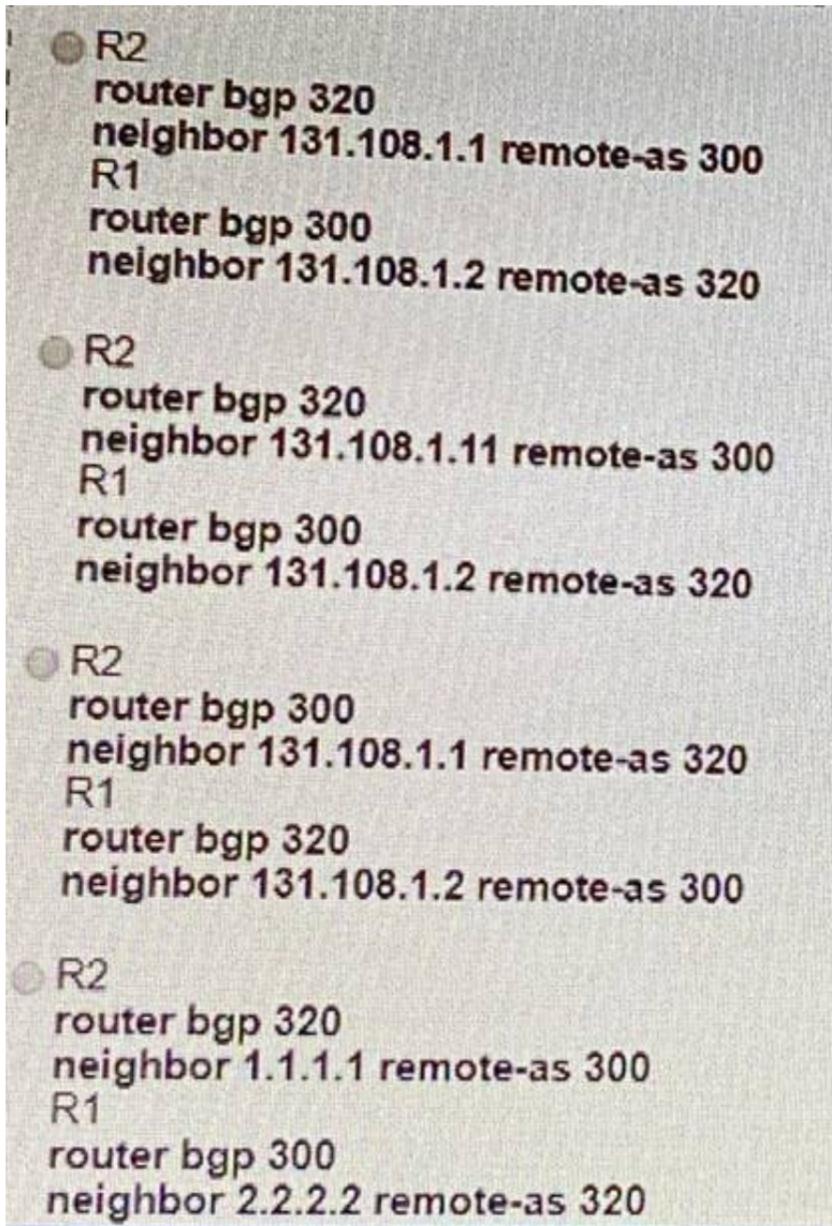
**Router R2**

```
interface Ethernet0
ip address 131.108.1.2 255.255.255.0
interface Loopback1
ip address 2.2.2.2 255.255.255.255
```

```
R2#debug ip bgp
BGP debugging is on
R2#
Nov 28 13:25:12: BGP: 131.108.1.11 open active, local address 131.108.1.2
Nov 28 13:25:42: BGP: 131.108.1.11 open failed: Connection timed out;
remote host not responding
```

```
R2#debug ip bgp
BGP debugging is on
R2#
Nov 28 13:25:12: BGP: 131.108.1.11 open active, local address 131.108.1.2
Nov 28 13:25:42: BGP: 131.108.1.11 open failed: Connection timed out;
remote host not responding
```

Refer to the exhibit. Which configuration must be implemented to establish EBGP peering between R1 and R2?



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

**Answer:** A

**NEW QUESTION 379**

- (Topic 3)

An administrator is configuring NETCONF using the following XML string. What must the administrator end the request with?

```
<?xml version="1.0" encoding="UTF-8" ?>
<rpc message-id="9.0"><notification-on/>
```

- A. </rpc>]]>]]>
- B. </rpc-reply>
- C. </rpc>
- D. <rpc message.id="9.0"><notificationoff/>

**Answer:** A

**NEW QUESTION 381**

- (Topic 3)

An engineer must configure a new loopback Interface on a router and advertise the interface as a fa4 in OSPF. Which command set accomplishes this task?

A)

```
R2(config)# interface Loopback0
R2(config-if)# ip address 172.22.2.1 255.255.255.0
R2(config-if)# ip ospf 100 area 0
```

B)

```
R2(config)# interface Loopback0
R2(config-if)# ip address 172.22.2.1 255.255.255.0
R2(config-if)# ip ospf network point-to-point
R2(config-if)# ip ospf 100 area 0
```

C)

```
R2(config)# interface Loopback0
R2(config-if)# ip address 172.22.2.1 255.255.255.0
R2(config-if)# ip ospf network point-to-multipoint
R2(config-if)# router ospf 100
R2(config-router)# network 172.22.2.0 0.0.0.255 area 0
```

D)

```
R2(config)# Interface Loopback0
R2(config-if)# ip address 172.22.2.1 255.255.255.0
R2(config-if)# ip ospf network broadcast
R2(config-if)# ip ospf 100 area 0
```

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

**Answer:** A

**Explanation:**

? Step 1. Create the loopback interface using the interface loopback number global configuration command.

? Step 2. Add a description. Although optional, it is a necessary component for documenting a network.

? Step 3. Configure the IP address.

For example, the following commands configure a loopback interface of the R1 router shown in (shown earlier in the chapter):

```
R1# configure terminal
R1(config)# interface loopback 0
R1(config-if)# ip address 10.0.0.1 255.255.255.0
R1(config-if)# exit
R1(config)#
```

**NEW QUESTION 382**

- (Topic 3)

What are the main components of Cisco TrustSec?

- A. Cisco ISE and Enterprise Directory Services
- B. Cisco IS
- C. network switches, firewalls, and routers
- D. Cisco ISE and TACACS+
- E. Cisco ASA and Cisco Firepower Threat Defense

**Answer:** B

**NEW QUESTION 386**

- (Topic 3)

What is the API keys option for REST API authentication?

- A. a predetermined string that is passed from client to server
- B. a one-time encrypted token
- C. a username that is stored in the local router database
- D. a credential that is transmitted unencrypted

**Answer:** A

**NEW QUESTION 389**

- (Topic 3)

Which two features does the Cisco SD-Access architecture add to a traditional campus network? (Choose two.)

- A. software-defined segmentation
- B. private VLANs
- C. SD-WAN
- D. modular QoS
- E. identity services

**Answer:** AE

**Explanation:**

<https://www.aspiretransforms.com/2018/06/06/insider-guide-cisco-sd-access/>

**NEW QUESTION 390**

- (Topic 3)

A system must validate access rights to all its resources and must not rely on a cached permission matrix. If the access level to a given resource is revoked but is not reflected in the permission matrix, the security is violated. Which term refers to this REST security design principle?

- A. economy of mechanism
- B. complete mediation

- C. separation of privilege
- D. least common mechanism

**Answer:** B

**Explanation:**

A system should validate access rights to all its resources to ensure that they are allowed and should not rely on the cached permission matrix. If the access level to a given resource is being revoked, but that is not being reflected in the permission matrix, it would be violating security.  
<https://medium.com/strike-sh/rest-security-design-principles-434bd6ee57ea>

**NEW QUESTION 391**

- (Topic 3)

Which method displays text directly into the active console with a synchronous EEM applet policy?

- A. event manager applet boom event syslog pattern 'UP'action 1.0 gets 'logging directly to console'
- B. event manager applet boom event syslog pattern 'UP'action 1.0 syslog priority direct msg 'log directly to console'
- C. event manager applet boom event syslog pattern 'UP'action 1.0 puts 'logging directly to console'
- D. event manager applet boom event syslog pattern 'UP'action 1.0 string 'logging directly to console'

**Answer:** B

**NEW QUESTION 392**

- (Topic 3)

Refer to the exhibit.

```
SW2#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
GigabitEthernet0/1 (1), with SW1 GigabitEthernet 0/1 (30).
SW2#
```

An engineer must set up connectivity between a campus aggregation layer and a branch office access layer. The engineer uses dynamic trunking protocol to establish this connection, however, management traffic on VLAN1 is not passing. Which action resolves the issue and allow communication for all configured VLANs?

- A. Allow all VLANs on the trunk links
- B. Disable Spanning Tree for the native VLAN.
- C. Configure the correct native VLAN on the remote interface
- D. Change both interfaces to access ports.

**Answer:** C

**NEW QUESTION 397**

- (Topic 3)

Refer to the exhibit.

```
Router# show running-config
! lines omitted for brevity

username cisco password 0 cisco

aaa authentication login group1 group radius line
aaa authentication login group2 group radius local
aaa authentication login group3 group radius none

line con 0
password 0 cisco123
login authentication group1

line aux 0
login authentication group3

line vty 0 4
password 0 test123
login authentication group2
```

A network engineer must log in to the router via the console, but the RADIUS servers are not reachable Which credentials allow console access1?

- A. the username "cisco" and the password "Cisco"
- B. no username and only the password "test123"
- C. no username and only the password "cisco123"

D. the username "cisco" and the password "cisco123"

Answer: D

**NEW QUESTION 401**

- (Topic 3)

What is used to validate the authenticity of the client and is sent in HTTP requests as a JSON object?

- A. SSH
- B. HTTPS
- C. JWT
- D. TLS

Answer: C

**NEW QUESTION 402**

- (Topic 3)

Refer to the exhibit.

```
import json
from requests import get

Headers = { "Content-Type" : "application/yang-data+json",
            "Accept" : "application/yang-data+json" }

Devices = open("devices.txt", "r")

for Device in Devices.readlines():
    Hostname, IP, Login, Pass = Device.strip().split(",")
    URL = f"https://{IP}/restconf/data/Cisco-IOS-XE-native:native"
    Creds = (Login, Pass)
    response = get(URL, auth = Creds, headers = Headers, verify = False)
```

How should the script be completed so that each device configuration is saved into a JSON-formatted file under the device name?

A)

Insert after the for loop:

```
with open(f"{Hostname}.json", "w") as OutFile:
    OutFile.write(Response)
```

B)

Insert after the for loop:

```
with open(f"{Hostname}.json", "w") as OutFile:
    OutFile.write(json.dumps(Response.text))
```

C)

Append to the body of the for loop:

```
with open(f"{Hostname}.json", "w") as OutFile:
    OutFile.write(Response.text)
```

D)

Insert immediately before the for loop:

```
with open(f"{Hostname}.json", "w") as OutFile:
    OutFile.write(json.load(Devices))
```

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

Answer: A

**NEW QUESTION 406**

DRAG DROP - (Topic 3)

Drag and drop the characteristics from the left onto the deployment types on the right.

It is responsible for hardware maintenance.	On-Premises
It provides on-demand scalability.	
Maintenance is handled by a third party.	Cloud-Based
Scalability requires time and effort.	

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

It is responsible for hardware maintenance.	On-Premises
Scalability requires time and effort.	
It provides on-demand scalability.	Cloud-Based
Maintenance is handled by a third party.	

**NEW QUESTION 411**

- (Topic 3)

Which function does a fabric wireless LAN controller perform In a Cisco SD-Access deployment?

- A. manages fabric-enabled APs and forwards client registration and roaming information to the Control Plane Node
- B. coordinates configuration of autonomous nonfabric access points within the fabric
- C. performs the assurance engine role for both wired and wireless clients
- D. is dedicated to onboard clients in fabric-enabled and nonfabric-enabled APs within the fabric

**Answer: A**

**Explanation:**

Fabric Enabled WLC:

Fabric enabled WLC is integrated with LISP control plane. This WLC is responsible for AP image /Config, Radio Resource Management, Client Session management and roaming and all other wireless control plane functions.

For WLC Fabric Integration:

- ? Wireless Client MAC address is used as EID
- ? It inform about Wireless MAC address with its other information like SGT and Virtual Network Information
- ? VN information is mapped to VLAN on FEs
- ? WLC is responsible for updating Host Database tracking DB with roaming information

<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#FabricWLC>

Both fabric WLCs and non-fabric WLCs provide AP image and configuration management, client session management, and mobility services. Fabric WLCs provide additional services for fabric integration such as registering MAC addresses of wireless clients into the host tracking database of the fabric control plane nodes during wireless client join events and supplying fabric edge node RLOC-association updates to the HTDB during client roam events.

**NEW QUESTION 416**

DRAG DROP - (Topic 3)

Drag and drop the automation characteristics from the left onto the appropriate tools on the right.

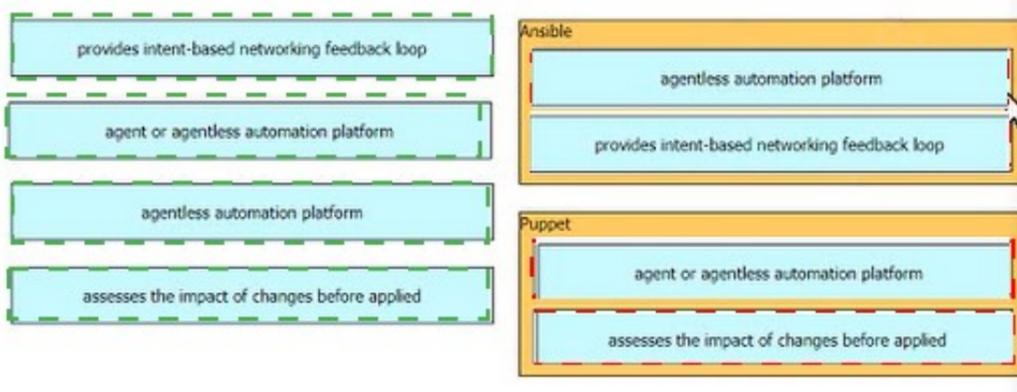
provides intent-based networking feedback loop	Ansible
agent or agentless automation platform	
agentless automation platform	Puppet
assesses the impact of changes before applied	

- A. Mastered

B. Not Mastered

**Answer:** A

**Explanation:**



**NEW QUESTION 421**

- (Topic 3)

A Cisco DNA Center REST API sends a PUT to the /dna/intent/api/v1/network-device endpoint A response code of 504 is received What does the code indicate?

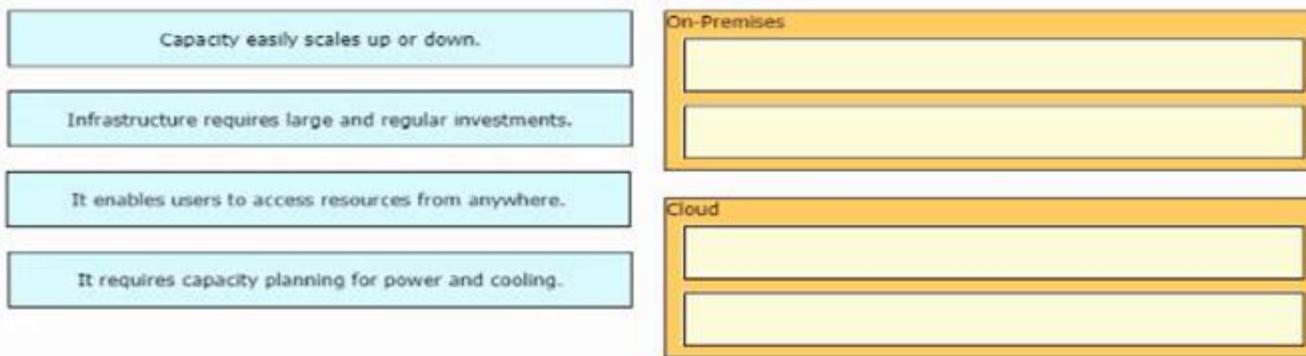
- A. The response timed out based on a configured interval
- B. The user does not have authorization to access this endpoint.
- C. The username and password are not correct
- D. The web server is not available

**Answer:** A

**NEW QUESTION 423**

DRAG DROP - (Topic 3)

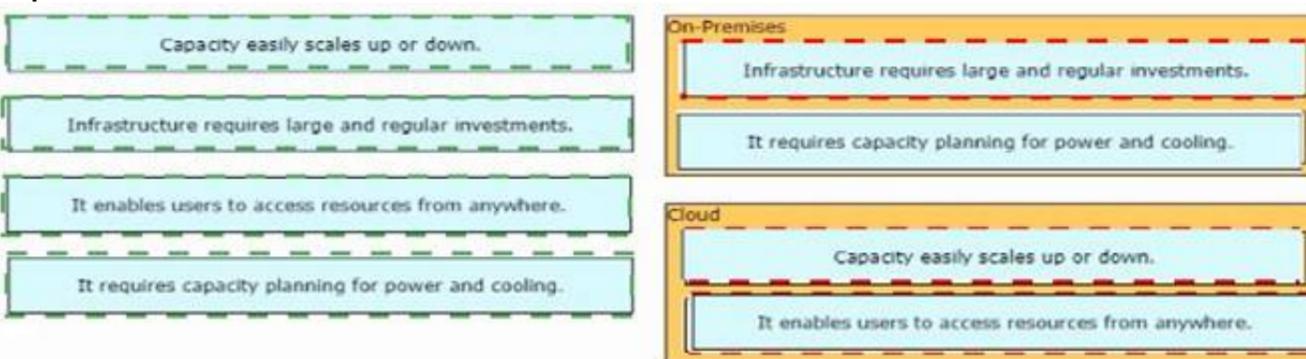
Drag and drop the characteristics from the left onto the infrastructure deployment models on the right.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



**NEW QUESTION 424**

- (Topic 3)

What happens when a FlexConnect AP changes to standalone mode?

- A. All controller-dependent activities stop working except the DFS.
- B. All client roaming continues to work
- C. Only clients on central switching WLANs stay connected.
- D. All clients on an WLANs are disconnected

**Answer:** A

**NEW QUESTION 427**

- (Topic 3)

```
import requests
import json

url='https://switchIP.foo.com/ins'
switchuser='username'
switchpassword='password123'

myheaders={'content-type':'application/json-rpc'}
payload=[
    {
        "jsonrpc": "2.0",
        "method": "cli",
        "params": {
            "cmd": "show clock",
            "version": 1
        },
        "id": 1
    }
]

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

Refer to the exhibit. Which python code parses the response and prints "18:32:21.474 UTC sun Mar 10 2019"?

- A. print(response['result'][0]['simple\_time'])
- B. print(response['result']['body']['simple\_time'])
- C. print(response['body']['simple\_time'])
- D. print(response['result']['body']['simple\_time'])

Answer: B

**NEW QUESTION 432**

DRAG DROP - (Topic 3)

Drag and drop the characteristics from the left onto the technology types on the right.

This type of technology provides automation across multiple technologies and domains.	Configuration Management
This type of technology enables consistent configuration of infrastructure resources.	
Puppet is used for this type of technology.	Orchestration
Ansible is used for this type of technology.	

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Orchestration

Orchestration means arranging or coordinating multiple systems. It's also used to mean "running the same tasks on a bunch of servers at once, but not necessarily all of them." Configuration Management

Config Management is part of provisioning. Basically, that's using a tool like Chef, Puppet or Ansible to configure our server. "Provisioning" often implies it's the first time we do it. Config management usually happens repeatedly.

Configuration management (CM) is a systems engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life Configuration management is all about bringing consistency in the infrastructure.

Configuration Orchestration vs Configuration Management

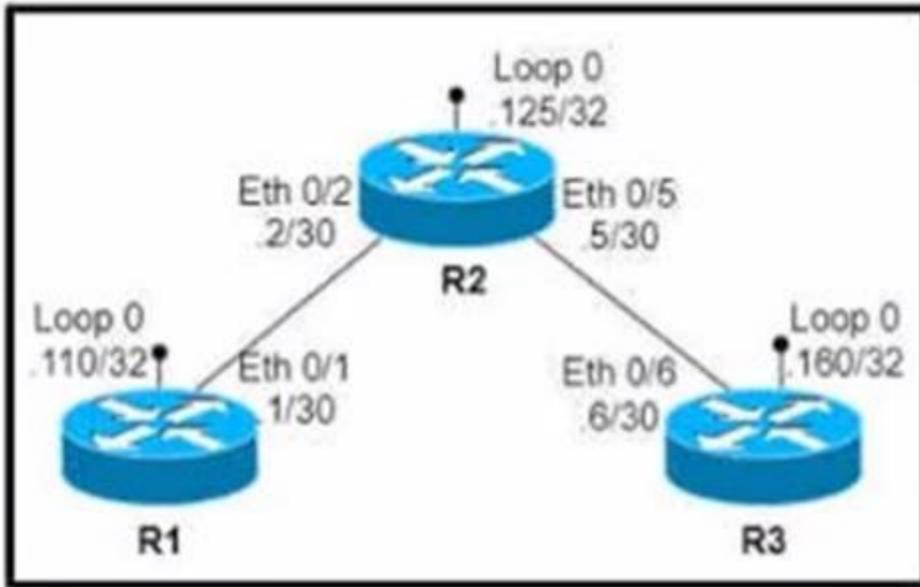
The first thing that should be clarified is the difference between "configuration orchestration" and "configuration management" tools, both of which are considered IaC tools and are included on this list.

Configuration orchestration tools, which include Terraform and AWS CloudFormation, are designed to automate the deployment of servers and other infrastructure. Configuration management tools like Chef, Puppet, and the others on this list help configure the software and systems on this infrastructure that has already been provisioned.

**NEW QUESTION 435**

- (Topic 3)

Refer to the exhibit.



An engineer configures routing between all routers and must build a configuration to connect R1 to R3 via a GRE tunnel Which configuration must be applied?  
 A)

```

R1
interface Tunnel1
 ip address 1.1.1.13 255.255.255.0
 tunnel source Loopback0
 tunnel destination x.y.z.110
  
```

```

R3
interface Tunnel1
 ip address 1.1.1.31 255.255.255.0
 tunnel source Loopback0
 tunnel destination x.y.z.160
  
```

B)

```

R1
interface Tunnel1
 ip address 1.1.1.13 255.255.255.0
 tunnel source Loopback0
 tunnel destination x.y.z.110
  
```

```

R3
interface Tunnel1
 ip address 1.1.1.31 255.255.255.0
 tunnel source Loopback0
 tunnel destination x.y.z.125
  
```

C)

```
R1
interface Tunnel2
 ip address 1.1.1.12 255.255.255.0
 tunnel source Loopback0
 tunnel destination x.y.z.125
```

```
R2
interface Tunnel1
 ip address 1.1.1.125 255.255.255.0
 tunnel source Loopback0
 tunnel destination x.y.z.110
interface Tunnel3
 ip address 1.1.1.125 255.255.255.0
 tunnel source Loopback0
 tunnel destination x.y.z.160
```

```
R3
interface Tunnel2
 ip address 1.1.1.32 255.255.255.0
 tunnel source Loopback0
 tunnel destination x.y.z.125
```

D)

```
R1
interface Tunnel1
 ip address 1.1.1.13 255.255.255.0
 tunnel source Loopback0
 tunnel destination x.y.z.160
```

```
R3
interface Tunnel1
 ip address 1.1.1.31 255.255.255.0
 tunnel source Loopback0
 tunnel destination x.y.z.110
```

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

**Answer: D**

**NEW QUESTION 436**

- (Topic 3)

Which option works with a DHCP server to return at least one WLAN management interface IP address during the discovery phase and is dependent upon the VCI of the AP?

- A. Option 42
- B. Option 15
- C. Option 125
- D. Option 43

**Answer: D**

**NEW QUESTION 438**

- (Topic 3)

What is one benefit of adopting a data modeling language?

- A. augmenting management process using vendor centric actions around models
- B. refactoring vendor and platform specific configurations with widely compatible configurations
- C. augmenting the use of management protocols like SNMP for status subscriptions
- D. deploying machine-friendly codes to manage a high number of devices

**Answer: B**

**NEW QUESTION 443**

- (Topic 3)

Which feature is used to propagate ARP broadcast, and link-local frames across a Cisco SD-Access fabric to address connectivity needs for silent hosts that require reception of traffic to start communicating?

- A. Native Fabric Multicast
- B. Layer 2 Flooding
- C. SOA Transit
- D. Multisite Fabric

**Answer: B**

**Explanation:**

Layer2 Flooding

Cisco SD-Access fabric provides many optimizations to improve unicast traffic flow, and to reduce the unnecessary flooding of data such as broadcasts. But, for some traffic and applications, it may be desirable to enable broadcast forwarding within the fabric.

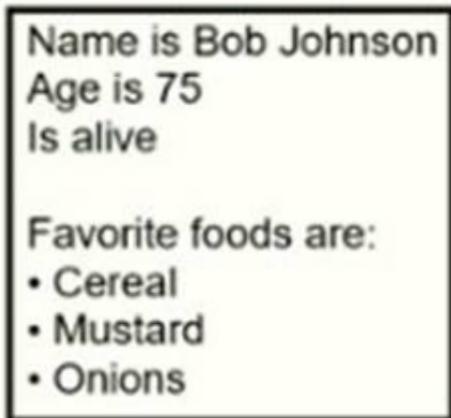
By default, this is disabled in the Cisco SD-Access architecture. If broadcast, Link local multicast and Arp flooding is required, it must be specifically enabled on a per-subnet basis using Layer 2 flooding feature.

Layer 2 flooding can be used to forward broadcasts for certain traffic and

application types which may require leveraging of Layer 2 connectivity, such as silent hosts, card readers, door locks, etc.

**NEW QUESTION 445**

- (Topic 3)



What is the JSON syntax that is formed the data?

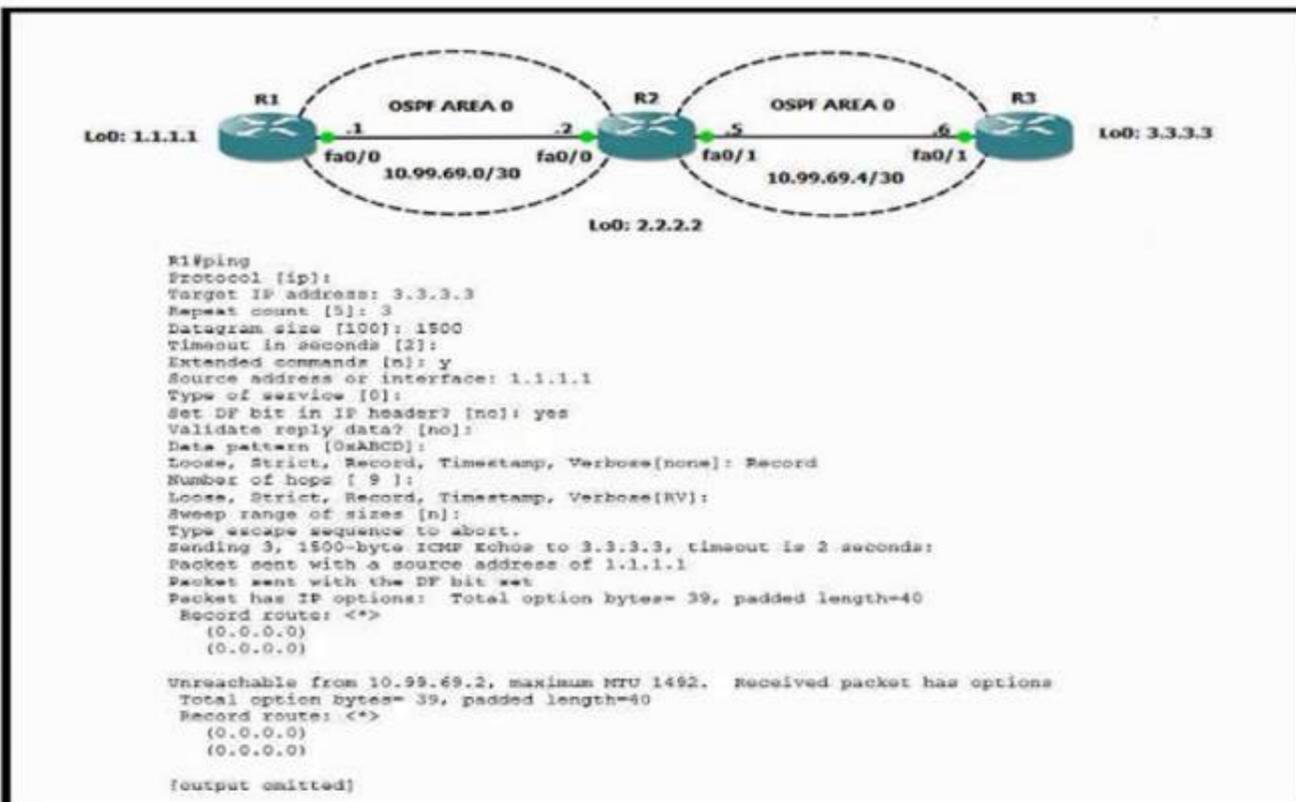
- A. {'Name';"Bob johnon";"Age': Sevenfive,"Alive":true,"FavoriteFoods':['Cereal';"Mustard';"Onions']}}}
- B. {'Name':"Bob johnon";"Age': 75 "Alive": true,"FavoriteFoods':['Cereal';"Mustard';"Onions']}}}
- C. {'Name':"Bob johnon";"Age: 75,"Alive: true, FavoriteFoods:[Cereal, Mustard';"Onions']}}}
- D. {'Name': 'Bob johnon','Age: 75,'Alive': true,"FavoriteFoods': 'Cereal';'Mustard';'Onions']}}}

**Answer: B**

**NEW QUESTION 447**

- (Topic 3)

Refer to the exhibit.



R1 is able to ping the R3 fa0/1 Interface. Why do the extended pings fail?

- A. The DF bit has been set
- B. The maximum packet size accepted by the command is 147G bytes
- C. R2 and R3 do not have an OSPF adjacency
- D. R3 is missing a return route to 10.99.69.0/30

**Answer: A**

**Explanation:**

If the DF bit is set, routers cannot fragment packets. From the output below, we learn that the maximum MTU of R2 is 1492 bytes while we sent ping with 1500 bytes. Therefore these ICMP packets were dropped.  
 Note: Record option displays the address(es) of the hops (up to nine) the packet goes through.

**NEW QUESTION 452**

- (Topic 3)

By default, which virtual MAC address does HSRP group 32 use?

- A. 00:5e:0c:07:ac:20
- B. 04:18:20:83:2e:32
- C. 05:5e:5c:ac:0c:32
- D. 00:00:0c:07:ac:20

**Answer: D**

**NEW QUESTION 457**

- (Topic 3)

What is the difference between the MAC address table and TCAM?

- A. The MAC address table supports partial matches
- B. TCAM requires an exact match.
- C. The MAC address table is contained in TCAM and ACL and QoS information is stored in CAM.
- D. Router prefix lookups happen in TCAM
- E. MAC address table lookups happen in CAM.
- F. TCAM is used to make L2 forwarding decisions
- G. CAM is used to build routing tables

**Answer: C**

**Explanation:**

"TCAM is most useful for building tables for searching on longest matches such as IP routing tables organized by IP prefixes. The TCAM table stores ACL, QoS and other information generally associated with upper-layer processing. As a result of using TCAM, applying ACLs does not affect the performance of the switch."  
<https://community.cisco.com/t5/networking-documents/cam-content-addressable-memory-vs-tcam-ternary-content/ta-p/3107938>

**NEW QUESTION 459**

- (Topic 3)

```

SF_router#show run int gig0/1
Building configuration...

Current configuration : 114 bytes
!
interface GigabitEthernet0/1
 ip address 10.10.1.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
end

SF_router#show run | s r o
router ospf 1
 router-id 1.1.1.1
 network 1.1.1.1 0.0.0.0 area 0

 network 192.168.13.0 0.0.0.255 area 0
SF_router#
    
```

Refer to the exhibit. Which configuration must be added to enable GigabitEthernet 0/1 to participate in OSPF?

- A. SF\_router (config-router)# network 10.10.1.0 0.0.0.255 area 0
- B. SF\_router (config)# network 10.10.1.0 0.0.0.255 area 1
- C. SF\_router (config-router)# network 10.10.1.0 0.0.0.255 area 1
- D. SF\_router (config-router)# network 10.10.1.0 255.255.255.0 area 0

**Answer: C**

**NEW QUESTION 461**

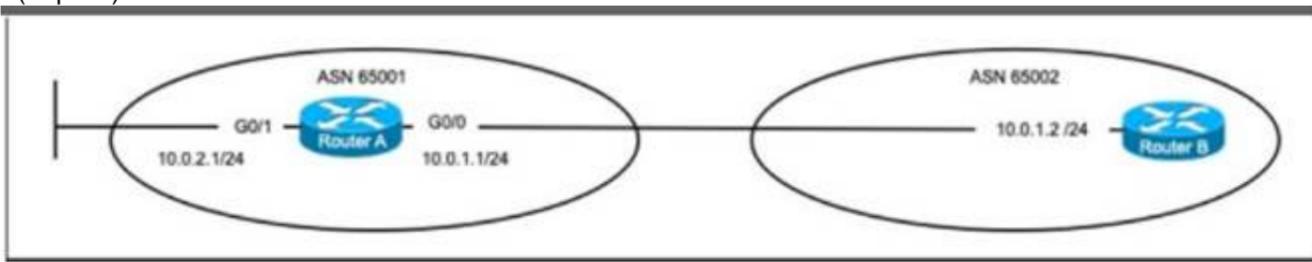
- (Topic 3)

By default, which virtual MAC address does HSRP group 14 use?

- A. 04.16.19.09.4c.0e
- B. 00:05:5e:19:0c:14
- C. 00:05:0c:07:ac:14
- D. 00:00:0c:07:ac:0e

**Answer: D**

**NEW QUESTION 466**  
 - (Topic 3)



Refer to the exhibit. An engineer must configure an eBGP neighborship to Router B on Router A. The network that is connected to GO/1 on Router A must be advertised to Router

A. Which configuration should be applied? A)

```
router bgp 65001
neighbor 10.0.1.2 remote-as 65002
redistribute static
```

B) router bgp 65002  
 neighbor 10.0.1.2 remote-as 65002  
 network 10.0.2.0 255.255.255.0

C) router bgp 65001  
 neighbor 10.0.1.2 remote-as 65002  
 network 10.0.2.0 255.255.255.0

D) router bgp 65001  
 neighbor 10.0.1.2 remote-as 65002  
 network 10.0.1.0 255.255.255.0

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

**Answer: C**

**NEW QUESTION 467**  
 - (Topic 3)  
 Refer to the exhibit.

```

RouterSF#show ip route 10.0.0.0
Routing entry for 10.0.0.0/24, 1 known subnets
B    10.0.0.0 [20/0] via 192.168.2.2, 00:03:23
RouterSF#
RouterSF#show bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/24, version 8
Paths: (2 available, best #2, table default)
Multipath: eiBGP
  Advertised to update-groups:
    2
  Refresh Epoch 1
  65002 65001
    192.168.3.2 from 192.168.3.2 (192.168.3.2)
      Origin IGP, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
      Updated on Sep 22 2020 21:32:27 UTC
  Refresh Epoch 2
  65003 65001
    192.168.2.2 from 192.168.2.2 (192.168.2.2)
      Origin IGP, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
      Updated on Sep 22 2020 21:31:57 UTC
RouterSF#
  
```

After configuring the BGP network, an engineer verifies that the path between Servers and Server2 Is functional. Why did RouterSF choose the route from RouterDAL instead of the route from RouterCHI?

- A. The Router-ID for Router DAL is lower than the Router-ID for RouterCHI.
- B. The route from RouterOAL has a lower MED.
- C. BGP is not running on RouterCHI.
- D. There is a static route in RouterSF for 10.0.0.0/24.

Answer: A

**NEW QUESTION 472**

- (Topic 2)  
 Refer to the exhibit

```

London(config)#interface fa0/1
London(config-if)#switchport trunk encapsulation dot1q
London(config-if)#switchport mode trunk

%LINEPROTO-5-UPDOWN:Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN:Line protocol on Interface FastEthernet0/1, changed state to up

London(config-if)#end

NewYork#show dtp interface fa0/1
DTP information for FastEthernet0/1:
TOS/TAS/TNS:          ACCESS/AUTO/ACCESS
TOT/TAT/TNT:          NATIVE/ISL/NATIVE
  
```

Communication between London and New York is down Which to resolve this issue?

A)

```

NewYork(config)#int f0/1
NewYork(config)#switchport trunk encap dot1q
NewYork(config)#end
NewYork#
  
```

B)

```
NewYork(config)#int f0/1
NewYork(config)#switchport mode trunk
NewYork(config)#end
NewYork#
```

C)

```
NewYork(config)#int f0/1
NewYork(config)#switchport nonegotiate
NewYork(config)#end
NewYork#
```

D)

```
NewYork(config)#int f0/1
NewYork(config)#switchport mode dynamic desirable
NewYork(config)#end
NewYork#
```

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

**Answer:** A

**Explanation:**

<https://learningnetwork.cisco.com/s/question/0D53i00000Ksyty/tostastns-tottatnt>

**NEW QUESTION 477**

- (Topic 2)

A network is being migrated from IPV4 to IPV6 using a dual-stack approach. Network management is already 100% IPV6 enabled. In a dual-stack network with two dual-stack NetFlow collections, how many flow exporters are needed per network device in the flexible NetFlow configuration?

- A. 1
- B. 2
- C. 4
- D. 8

**Answer:** B

**NEW QUESTION 479**

- (Topic 2)

An administrator must enable Telnet access to Router X using the router username and password database for authentication. Which configuration should be applied?

A)

```
RouterX(config)# line aux 0
RouterX(config-line)# password cisco
RouterX(config-line)# login
```

B)

```
RouterX(config)# aaa new-model
RouterX(config)# aaa authentication login auth-list local
```

C)

```
RouterX(config)# line vty 0 4
RouterX(config-line)# login local
RouterX(config-line)# end
```

D)

```
RouterX(config)# line vty 0 4
RouterX(config-line)# login
RouterX(config-line)# end
```

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

**Answer:** D

**NEW QUESTION 482**

- (Topic 2)

Which network devices secure API platform?

- A. next-generation intrusion detection systems
- B. Layer 3 transit network devices
- C. content switches
- D. web application firewalls

**Answer:** D

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/products/collateral/security/advanced-waf-bot-aag.pdf> Cisco® Secure Web Application Firewall (WAF) and bot protection defends your online presence and ensures that website, mobile applications, and APIs are secure, protected, and “always on.”

**NEW QUESTION 484**

- (Topic 2)

A customer requests a design that includes GLBP as the FHRP The network architect discovers that the members of the GLBP group have different throughput capabilities Which GLBP load balancing method supports this environment?

- A. host dependent
- B. least connection
- C. round robin
- D. weighted

**Answer:** D

**Explanation:**

Weighted: Defines weights to each device in the GLBP group to define the ratio of load balancing between the devices. This allows for a larger weight to be assigned to bigger routers that can handle more traffic. protocol is used by an extended

**NEW QUESTION 486**

- (Topic 2)

A client device roams between wireless LAN controllers that are mobility peers, Both controllers have dynamic interface on the same client VLAN which type of roam is described?

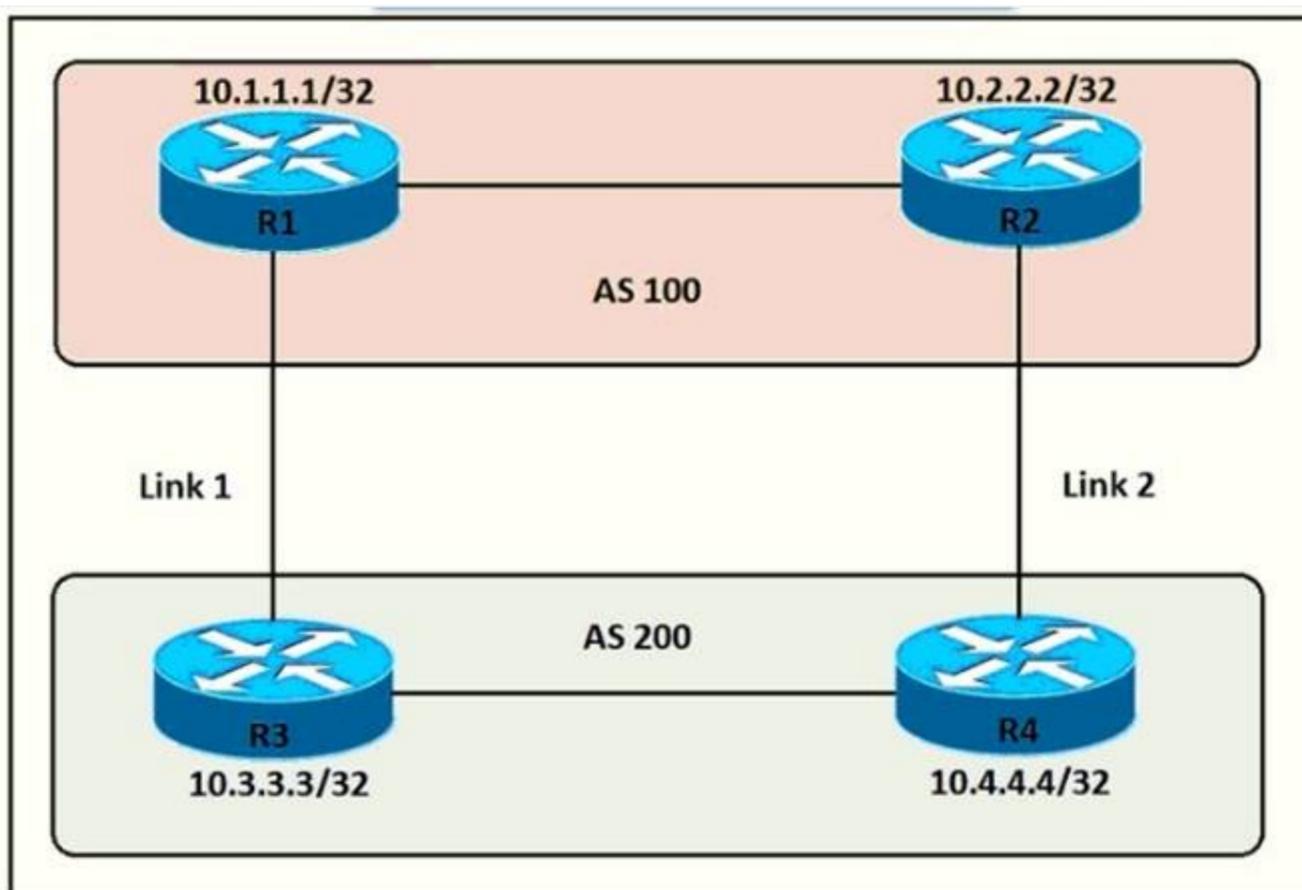
- A. intra-VLAN
- B. inter-controller
- C. intra-controller
- D. inter-subnet

**Answer:** B

**NEW QUESTION 487**

- (Topic 1)

Refer to the exhibit.



An engineer must ensure that all traffic leaving AS 200 will choose Link 2 as an entry 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?

- R3(config)#route-map PREPEND permit 10  
 R3(config-route-map)#set as-path prepend 200 200 200

R3(config)#router bgp 200  
 R3(config-router)#neighbor 10.1.1.1 route-map PREPEND out
- R4(config)#route-map PREPEND permit 10  
 R4(config-route-map)#set as-path prepend 100 100 100

R4(config)#router bgp 200  
 R4(config-router)#neighbor 10.2.2.2 route-map PREPEND in
- R3(config)#route-map PREPEND permit 10  
 R3(config-route-map)#set as-path prepend 100 100 100

R3(config)#router bgp 200  
 R3(config-router)#neighbor 10.1.1.1 route-map PREPEND in
- R4(config)#route-map PREPEND permit 10  
 R4(config-route-map)#set as-path prepend 200 200 200

R4(config)#router bgp 200  
 R4(config-router)#neighbor 10.2.2.2 route-map PREPEND out

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

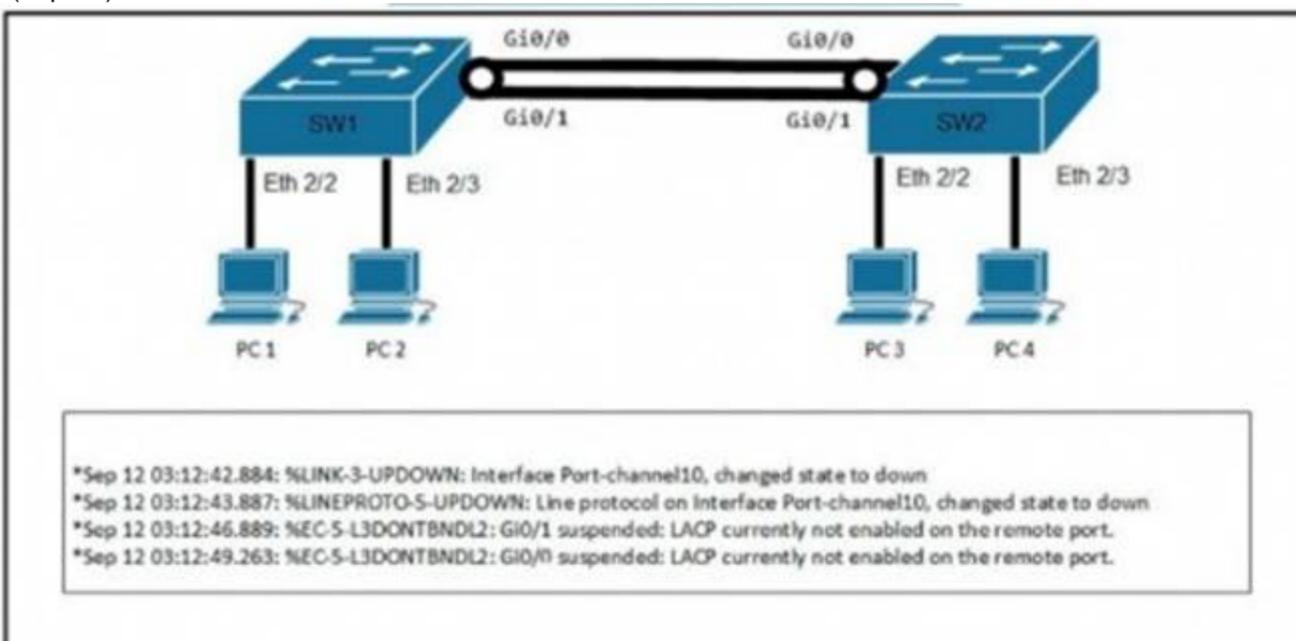
**Answer:** A

**Explanation:**

R3 advertises BGP updates to R1 with multiple AS 100 so R3 believes the path to reach AS 200 via R3 is farther than R2 so R3 will choose R2 to forward traffic to AS 200.

**NEW QUESTION 492**

- (Topic 1)



Refer to the exhibit. A network engineer troubleshoots an issue with the port channel between SW1 and SW2. which command resolves the issue?

A)  
**SW1(config-if)#channel-group 10 mode desirable**

B)  
**SW1(config-if)#channel-group 10 mode active**

- C) `SW2(config-if)#switchport mode trunk`
- D) `SW2(config-if)#channel-group 10 mode on`

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

**Answer: B**

**NEW QUESTION 496**

- (Topic 1)

```

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
:
    
```

Refer to the exhibit. A network engineer configures NAT on R1 and enters the show command to verify the configuration. What does the output confirm?

- A. The first packet triggered NAT to add an 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 is configured with PAT overload parameters

**Answer: A**

**NEW QUESTION 498**

- (Topic 1)

An engineer is troubleshooting the AP join process using DNS. Which FQDN must be resolvable on the network for the access points to successfully register to the WLC?

- A. wlcbostrname.domain.com
- B. cisco-capwap-controller.domain.com
- C. ap-manager.domain.com
- D. primary-wlc.domain.com

**Answer:** B

**Explanation:**

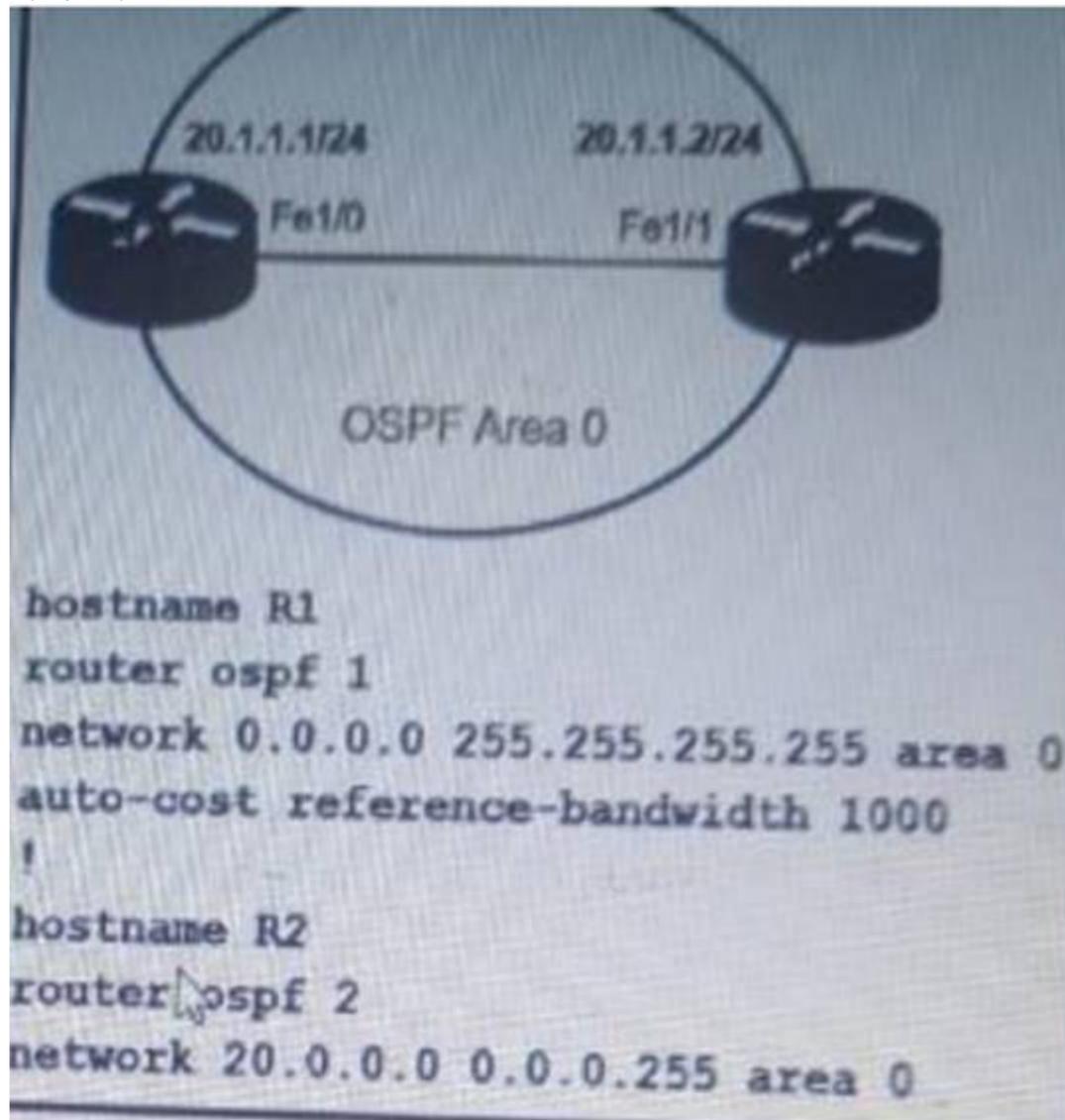
DNS: If you have configured your DHCP server to provide both option 006 (DNS server address) and option 015 (domain name) information, the AP can obtain WLC addresses from the DNS server. The process works as follows:

- \* 1. The AP gets its IP address from DHCP with options 6 and 15 configured.
- \* 2. The AP can obtain the IP address of the DNS server from the DHCP option.
- \* 3. The AP uses this information to perform a hostname lookup using CISCO-CAPWAP- CONTROLLER.<localdomain>, which resolves to available WLC management interface IP addresses (IPv4 or IPv6, or both).
- \* 4. The AP can then perform a directed message to associate to responsive WLCs.

To prevent all APs from joining a single controller based on a DNS name resolution, the domain name may vary; this is what is done to dispatch APs to different controllers across the enterprise network, based on different domain names that are configured in their respective DNS scopes.

**NEW QUESTION 499**

- (Topic 1)



Which command must be applied to R2 for an OSPF neighborship to form?

- A. network 20.1.1.2.0.0.0.0 area 0
- B. network 20.1.1.2 255.255.0.0. area 0
- C. network 20.1.1.2.0.0.255.255 area 0
- D. network 20.1.1.2 255.255.255 area 0

**Answer:** A

**Explanation:**

The network 20.0.0.0 0.0.0.255 area 0 command on R2 did not cover the IP address of Fa1/1 interface of R2 so OSPF did not run on this interface. Therefore we have to use the command network 20.1.1.2 0.0.255.255 area 0 to turn on OSPF on this interface.

Note: The command network 20.1.1.2 0.0.255.255 area 0 can be used too so this answer is also correct but answer C is the best answer here.

The network 0.0.0.0 255.255.255.255 area 0 command on R1 will run OSPF on all active

**NEW QUESTION 504**

- (Topic 1)

Which DHCP option helps lightweight APs find the IP address of a wireless LAN controller?

- A. Option 43
- B. Option 60
- C. Option 67
- D. Option 150

**Answer:** A

**NEW QUESTION 505**

DRAG DROP - (Topic 1)

Drag and drop the virtual components from the left onto their deceptions on the right.

VNIC	zip file connecting a virtual machine configuration file and a virtual disk
OVA	file containing a virtual machine disk drive
VMDK	configuration file containing settings for a virtual machine such as guest OS
VMX	component of a virtual machine responsible for sending packets to the hypervisor

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

VNIC	VMX
OVA	VMDK
VMDK	OVA
VMX	VNIC

**NEW QUESTION 506**

- (Topic 1)

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 507**

- (Topic 1)

A company has an existing Cisco 5520 HA cluster using SSO. An engineer deploys a new single Cisco Catalyst 9800 WLC to test new features. The engineer successfully configures a mobility tunnel between the 5520 cluster and 9800 WLC. Client connected to the corporate WLAN roam seamlessly between access points on the 5520 and 9800 WLC. After a failure on the primary 5520 WLC, all WLAN services remain functional; however, Client roam between the 5520 and 9800 controllers without dropping their connection. Which feature must be configured to remedy the issue?

- A. mobility MAC on the 5520 cluster
- B. mobility MAC on the 9800 WLC
- C. new mobility on the 5520 cluster
- D. new mobility on the 9800 WLC

Answer: B

**NEW QUESTION 508**

- (Topic 1)

Refer to the exhibit.

```
SwitchC#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 8
VTP Operating Mode         : Transparent
VTP Domain Name            : cisco.com
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MDS digest                  : 0xE5 0x28 0x5D 0x3E 0x2F 0xE5 0xAD 0x2B
Configuration last modified by 0.0.0.0 at 1-10-19 09:01:38

SwitchC#show vlan brief
VLAN Name                Status Ports
-----
1    default                active Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                Fa0/23, Fa0/24, Po1
110  Finance                 active
210  HR                      active Fa0/1
310  Sales                    active Fa0/2
[...output omitted...]

SwitchC#show int trunk
Port      Mode      Encapsulation  Status      Native vlan
Gig1/1    on        802.1q         trunking    1
Gig1/2    on        802.1q         trunking    1

Port      Vlans allowed on trunk
Gig1/1    1-1005
Gig1/2    1-1005

Port      Vlans allowed and active in management domain
Gig1/1    1, 110, 210, 310
Gig1/2    1, 110, 210, 310

Port      Vlans in spanning tree forwarding state and not pruned
Gig1/1    1, 110, 210, 310
Gig1/2    1, 110, 210, 310

SwitchC#show run interface port-channel 1
interface Port-channel 1
 description Uplink_to_Core
 switchport mode trunk
```

SwitchC connects HR and Sales to the Core switch However, business needs require that no traffic from the Finance VLAN traverse this switch Which command meets this requirement?

- A) `SwitchC(config)#vtp pruning`
- B) `SwitchC(config)#vtp pruning vlan 110`
- C) `SwitchC(config)#interface port-channel 1`  
`SwitchC(config-if)#switchport trunk allowed vlan add 210,310`
- D)

SwitchC(config)#interface port-channel 1  
 SwitchC(config-if)#switchport trunk allowed vlan remove 110

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

**Answer: D**

**NEW QUESTION 509**

- (Topic 1)

What is the data policy in a Cisco SD-WAN deployment?

- A. list of ordered statements that define node configurations and authentication used within the SD-WAN overlay
- B. Set of statements that defines how data is forwarded based on IP packet information and specific VPNs
- C. detailed database mapping several kinds of addresses with their corresponding location
- D. group of services tested to guarantee devices and links liveliness within the SD-WAN overlay

**Answer: B**

**NEW QUESTION 512**

- (Topic 1)

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**

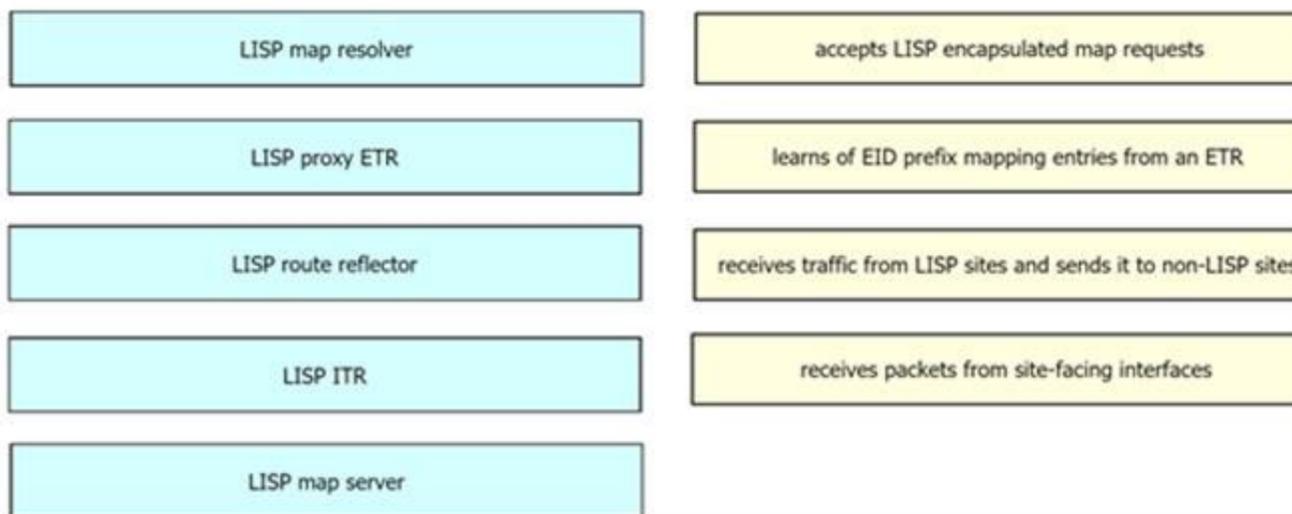
**Explanation:**

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 517**

DRAG DROP - (Topic 1)

Drag and drop the LISP components from the left onto the function they perform on the right. Not all options are used.



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Table

Description automatically generated

+ accepts LISP encapsulated map requests: LISP map resolver

+ learns of EID prefix mapping entries from an ETR: LISP map server

+ receives traffic from LISP sites and sends it to non-LISP sites: LISP proxy ETR

+ receives packets from site-facing interfaces: LISP ITR Explanation

ITR is the function that maps the destination EID to a destination RLOC and then encapsulates the original packet with an additional header that has the source IP address of

the ITR RLOC and the destination IP address of the RLOC of an Egress Tunnel Router (ETR).

After the encapsulation, the original packet become a LISP packet.

ETR is the function that receives LISP encapsulated packets, decapsulates them and forwards to its local EIDs. This function also requires EID-to-RLOC mappings so we need to

point out an "map-server" IP address and the key (password) for authentication.

A LISP proxy ETR (PETR) implements ETR functions on behalf of non-LISP sites. A PETR is

typically used when a LISP site needs to send traffic to non-LISP sites but the LISP site is connected through a service provider that does not accept no routable EIDs as packet sources. PETRs act just like ETRs but for EIDs that send traffic to destinations at non-LISP sites.

Map Server (MS) processes the registration of authentication keys and EID-to-RLOC mappings. ETRs sends periodic Map-Register messages to all its configured Map Servers. Map Resolver (MR): a LISP component which accepts LISP Encapsulated Map Requests, typically from an ITR, quickly determines whether or not the destination IP address is part of the EID namespace

**NEW QUESTION 520**

- (Topic 1)

Which configuration restricts the amount of SSH that a router accepts 100 kbps?

A)

```
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 209.145.200.225 255.255.255.0
  ip access-group EGRESS out
  duplex auto
  speed auto
  media-type rj45
  service-policy input CoPP_SSH
!
!
ip access-list extended CoPP_SSH
  permit tcp any any eq 22
!
```

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 209.145.200.225 255.255.255.0
  ip access-group EGRESS out
  duplex auto
  speed auto
  media-type rj45
  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
!

```

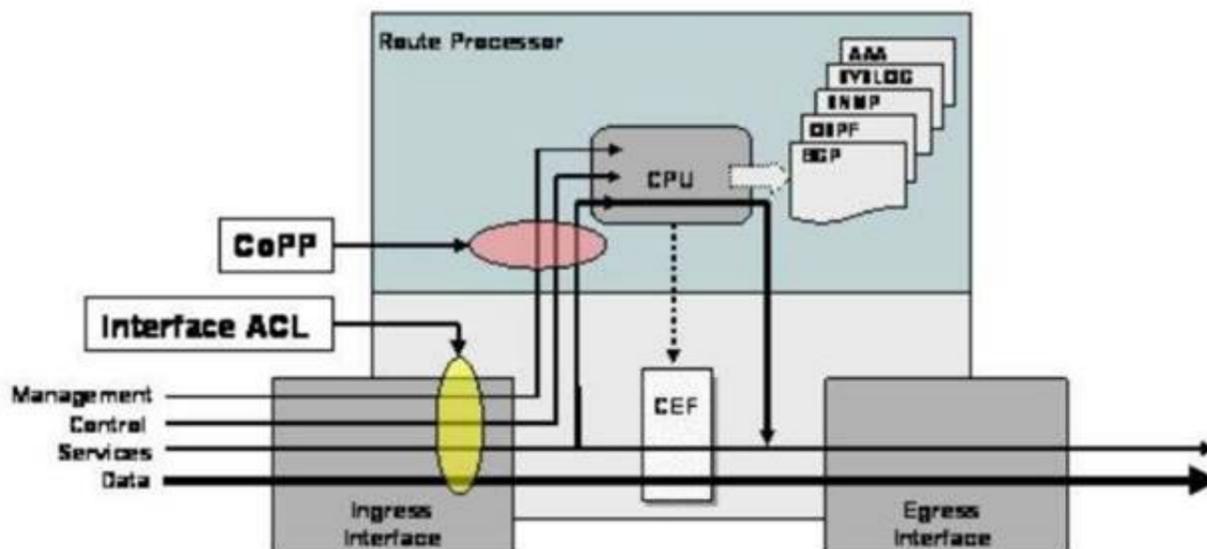
- A. Option A
- B. Option B
- C. Option C
- D. Option D

**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 523**

- (Topic 1)

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: A**

**Explanation:**

The Option 43 hexadecimal string is assembled as a sequence of the TLV values for the Option 43 suboption: Type + Length + Value. Type is always the suboption code 0xf1. Length is the number of controller management IP addresses times 4 in hex. Value is the IP address of the controller listed sequentially in hex.

On this question, there is 1 controller with management interface IP addresses 172.16.50.5/24. The type is 0xf1. The length is 1 \* 4 = 8 = 0x04. The mgmt IP addresses 172.16.50.5 translate to ac.10.32.05 (0xac103205). When the string is assembled, it yields f108c0a80a05c0a80a14. The Cisco IOS command that is added to the DHCP scope is: option 43 hex f104ac103205

**NEW QUESTION 526**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **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 First Try
- \* 350-401 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 350-401 Practice Test Here](#)**