



**Cisco**

**Exam Questions 350-401**

Implementing and Operating Cisco Enterprise Network Core Technologies

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### 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)

```
SW1# show etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
-----+-----+-----+-----
1 Po1(S D ) PAgP Gi1/0(I) Gi1/1(I)

SW2# show etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
-----+-----+-----+-----
1 Po1(S D ) LACP Gi1/0(I) Gi1/1(I)
```

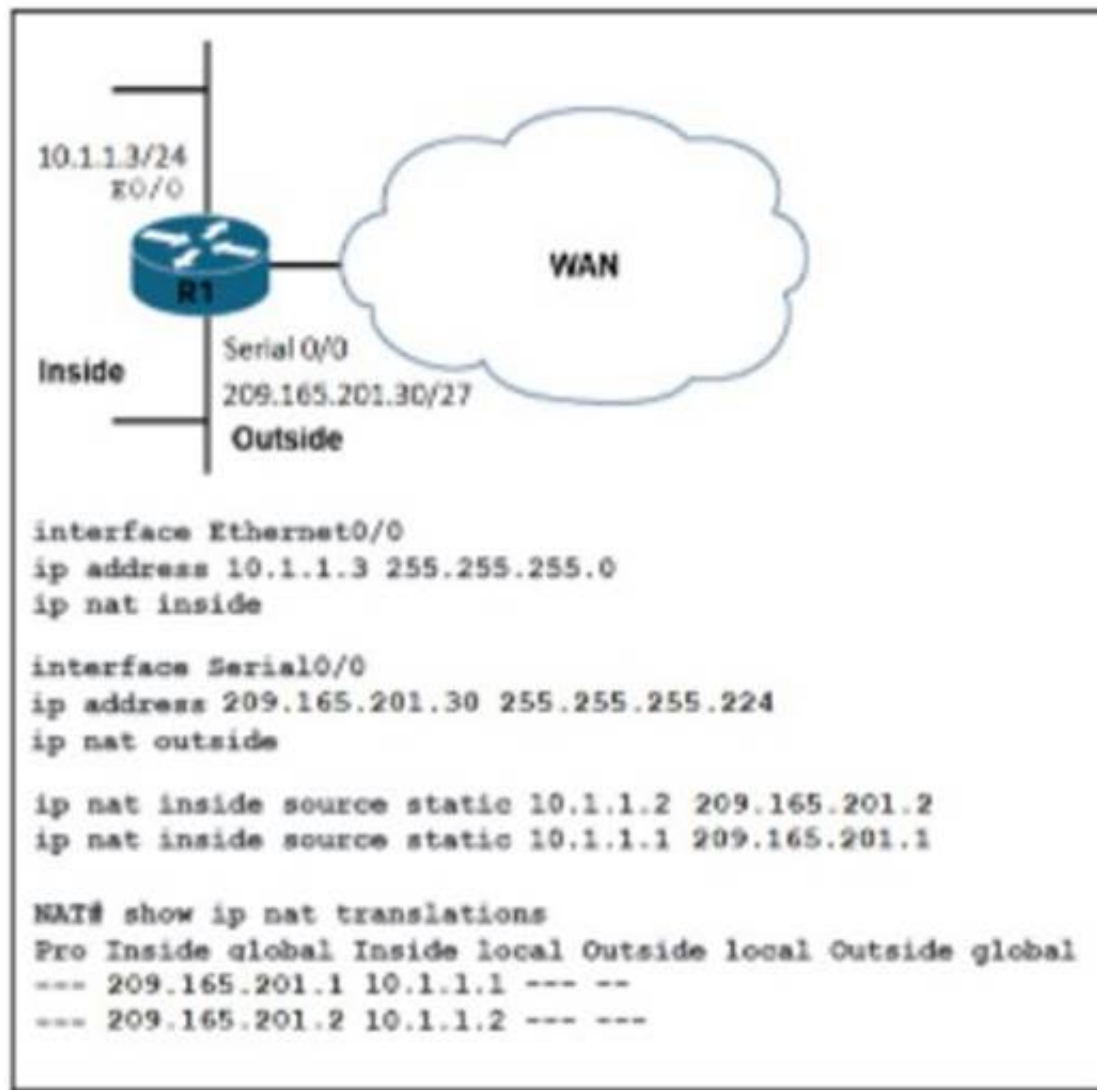
Refer to the exhibit. The EtherChannel between SW1 and SW2 is not operational. Which action will resolve the issue?

- A. Configure channel-group 1 mode active on GVO and G1 1 of SW2.
- B. Configure trunks on SW1 and SW2.
- C. Configure channel-group 1 mode active on Gi0 and Gi1 of SW1.
- D. Configure switchport mode dynamic desirable on SW1 and SW2

**Answer: C**

### NEW QUESTION 3

- (Topic 4)



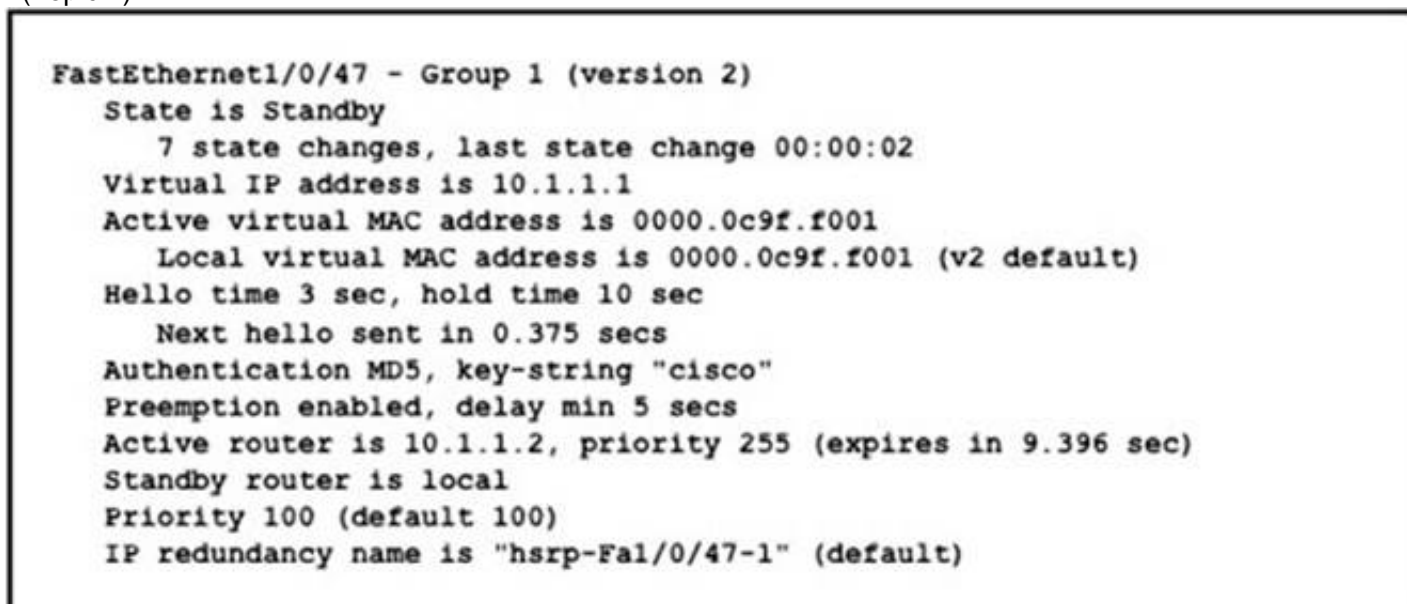
Refer to the exhibit. What are two results of the NAT configuration? (Choose two.)

- A. Packets with a destination of 200.1.1.1 are translated to 10.1.1.1 or .2. respectively.
- B. A packet that is sent to 200.1.1.1 from 10.1.1.1 is translated to 209.165.201.1 on R1.
- C. R1 looks at the destination IP address of packets entering S0/0 and destined for inside hosts.
- D. R1 processes packets entering E0/0 and S0/0 by examining the source IP address.
- E. R1 is performing NAT for inside addresses and outside address.

**Answer:** BC

#### NEW QUESTION 4

- (Topic 4)



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.

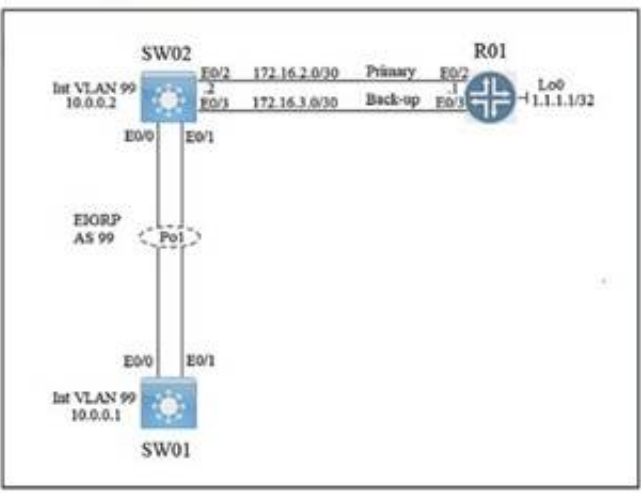
**Answer:** BE

#### NEW QUESTION 5

SIMULATION - (Topic 4)

Simulation 07

Guidelines
Topology
Tasks



R01
SW01
SW02

```

SW01>

```

Guidelines
Topology
Tasks

Configure logging on SW01 and NetFlow on R01 to achieve these goals:

1. Enable archive logging on SW01 to track each time a change is made to the configuration and the user who made the change.
2. The NetFlow Top Talkers feature has been preconfigured on R01. Enable the feature for all inbound traffic on interface E0/2 of R01.

R01
SW01
SW02

```

SW01>

```

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Sw1 Config t Archive Log config  
 Logging enable Notify syslog  
 R1  
 Config t  
 Ip flow-top-talkers  
 Match source address 172.16.2.1/30 Int et0/2  
 Ip flow ingress Copy run start

**NEW QUESTION 6**

- (Topic 4)

Which Cisco DNA Center application is responsible for group-based access control permissions?

- A. Provision
- B. Design
- C. Policy
- D. Assurance

**Answer:** C

**NEW QUESTION 7**

- (Topic 4)

A network administrator wants to install new VoIP switches in a small network closet but is concerned about the current heat level of the room. Which of the following should the administrator take into consideration before installing the new equipment?

- A. The power load of the switches
- B. The humidity in the room
- C. The fire suppression system
- D. The direction of airflow within the switches

**Answer:** D

**Explanation:**

This is because the direction of airflow within the switches can affect the heat level of the room, as the switches can either exhaust or intake hot air from the environment. The network administrator should take into consideration the direction of airflow within the switches before installing the new equipment, and ensure that the switches are aligned in the same direction and have enough space for ventilation. The network administrator should also avoid mixing switches with different airflow directions, as this can create a hot spot and reduce the cooling efficiency. The source of this answer is the Cisco ENCOR v1.1 course, module 2, lesson 2.1: Implementing Device Hardening.

**NEW QUESTION 8**

- (Topic 4)



Refer to the exhibit.

```
vlan 222
  remote-span
!
vlan 223
  remote-span
!
monitor session 1 source interface FastEthernet0/1 tx
monitor session 1 source interface FastEthernet0/2 rx
monitor session 1 source interface port-channel 5
monitor session 1 destination remote vlan 222
!
```

These commands have been added to the configuration of a switch. Which command flags an error if it is added to this configuration?

- A. monitor session 1 source interface port-channel 6
- B. monitor session 1 source vlan 10
- C. monitor session 1 source interface FastEthernet0/1 x
- D. monitor session 1 source interface port-channel 7, port-channel 8

**Answer: B**

#### NEW QUESTION 9

- (Topic 4)

Refer to the exhibit.

```
Router#show running-config | include aaa
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
aaa session-id common
```

Which configuration enables fallback to local authentication and authorization when no TACACS+ server is available?

- A. Router(config)# aaa authentication login default local Router(config)# aaa authorization exec default local
- B. Router(config)# aaa authentication login default group tacacs+ local Router(config)# aaa authorization exec default group tacacs+ local
- C. Router(config)# aaa fallback local
- D. Router(config)# aaa authentication login FALLBACK local Router(config)# aaa authorization exec FALLBACK local

**Answer: B**

#### NEW QUESTION 10

- (Topic 4)

By default, which virtual MAC address does HSRP group 30 use?

- A. 00:05:0c:07:ac:30
- B. 00:00:0c:07:ac:1e
- C. 05:0c:5e:ac:07:30
- D. 00:42:18:14:05:1e

**Answer: B**

#### NEW QUESTION 10

- (Topic 4)

An engineer must configure router R1 to validate user logins via RADIUS and fall back to the local user database if the RADIUS server is not available. Which configuration must be applied?

- A. aaa authorization exec default radius local
- B. aaa authorization exec default radius
- C. aaa authentication exec default radius local
- D. aaa authentication exec default radius

**Answer: C**

#### NEW QUESTION 12

- (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 14

DRAG DROP - (Topic 4)

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

It optimizes the switching process to handle larger packet volumes.

It is referred to as "software switching."

The general-purpose CPU is in charge of packet switching.

Process Switching

Cisco Express Forwarding

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

It optimizes the switching process to handle larger packet volumes.

It is referred to as "software switching."

The general-purpose CPU is in charge of packet switching.

Process Switching

It optimizes the switching process to handle larger packet volumes.

The general-purpose CPU is in charge of packet switching.

Cisco Express Forwarding

It is referred to as "software switching."

NEW QUESTION 16

- (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 21

- (Topic 4)

Refer to the exhibit.

```
from ncclient import manager

netconf_host = manager.connect(host='ios-xe-example.com',
                               port=22,
                               username='cisco',
                               password='cisco',
                               hostkey_verify=False,
                               device_params={'name':'iosxe'})

print (netconf_host.get_config('running'))
netconf_host.close_session()
```

An engineer deploys a script to retrieve the running configuration from a NETCONF- capable Cisco IOS XE device that is configured with default settings. The script fails. Which configuration must be applied to retrieve the configurauon using NETCONF?

- A. Print (netconf\_host.get\_config('show running!'))
- B. hostkey\_verify=True,
- C. device\_params={name:'ios-xe'})
- D. port=830

**Answer:** A

### NEW QUESTION 23

- (Topic 4)

Which JSON script is properly formatted?

A)

```
"car":{
  {
    "type":"A New Book",
    "model":"J Doe",
    "year":"1"
  }
}
```

B)

```
{
  "host":
  [
    "name":"SwitchA,
    "model":"Catalyst",
    "serial":"0438045649",
  ]
}
```

C)

```
{
  "book":[
    {
      "title":"A New Book,
      "author":"J P Doe",
      "edition":"2"
    }
  ]
}
```

D)

```
[
  "class":{
    "title":"Science",
    "grade":"11",
    "location":"Room C".
  }
]
```



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

Answer: B

NEW QUESTION 28

- (Topic 4)  
Which IP SLA operation requires the IP SLA responder to be configured on the remote end?

- A. TCP connect
- B. ICMP echo
- C. ICMP jitter
- D. UDP jitter

Answer: D

NEW QUESTION 32

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

saves on capital costs

provides full control of sensitive data

fast deployment of new services

improves service availability by supporting multiple WAN connectivity options

Cloud

On-Premises

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
CLOUD1 and 3ON-PREMISES2 and 4

NEW QUESTION 36

- (Topic 4)

```
interface GigabitEthernet1
ip address 10.10.10.1 255.255.255.0
!
access-list 10 permit 10.10.10.1
!
monitor session 10 type erspan-source
source interface Gi1
destination
erspan-id 10
ip address 192.168.1.1
!
```

Refer to the exhibit. Which command filters the ERSPAN session packets only to interface GigabitEthernet1?

- A. source ip 10.10.10.1
- B. source interface gigabitethernet1 ip 10.10.10.1
- C. filter access-group 10
- D. destination ip 10.10.10.1

Answer: C

NEW QUESTION 39

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

proprietary syntax in configuration files based on Ruby

high availability offered through a multi-primary architecture

Ruby syntax in configuration files

Puppet

Chef

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

based on Python

proprietary syntax in configuration files based on Ruby

high availability offered through a multi-primary architecture

Ruby syntax in configuration files

Puppet

proprietary syntax in configuration files based on Ruby

high availability offered through a multi-primary architecture

Chef

Ruby syntax in configuration files

NEW QUESTION 42

- (Topic 4)

```
ip access-list extended ACL-CoPP-Management
permit udp any eq ntp any
permit udp any any eq snmp
permit tcp any any eq 22
permit tcp any eq 22 any established

class-map match-all CLASS-CoPP-Management
match access-group name ACL-CoPP-Management
```

Refer to the exhibit. An engineer must protect the CPU of the router from high rates of NTP, SNMP, and SSH traffic. Which two configurations must be applied to drop these types of traffic when it continuously exceeds 320 kbps? (Choose two)

- ☐ R1(config)#policy-map POLICY-CoPP  
R1(config-pmap)#class CLASS-CoPP-Management  
R1(config-pmap-c)#police 320000 conform-action transmit exceed-action transmit violate-action drop
- ☐ R1(config)#control-plane  
R1(config-cp)# service-policy input POLICY-CoPP
- ☐ R1(config-pmap)#class CLASS-CoPP-Management  
R1(config-pmap-c)#police 32 conform-action transmit exceed-action drop violate-action transmit
- ☐ R1(config)#control-plane  
R1(config-cp)# service-policy output POLICY-CoPP
- ☐ R1(config)#policy-map POLICY-CoPP  
R1(config-pmap)#class CLASS-CoPP-Management  
R1(config-pmap-c)#police 320000 conform-action transmit exceed-action drop violate-action drop

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

Answer: BE

NEW QUESTION 47

- (Topic 4)  
What is the rose 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 50

- (Topic 4)  
What is the result of applying this access control list?

```
ip access-list extended STATEFUL
10 permit tcp any any established
20 deny ip any any
```

- A. TCP traffic with the URG bit set is allowed
- B. TCP traffic with the SYN bit set is allowed
- C. TCP traffic with the ACK bit set is allowed
- D. TCP traffic with the DF bit set is allowed

Answer: C

NEW QUESTION 51

- (Topic 4)  
A wireless administrator must create a new web authentication corporate SSID that will be using ISE as the external RADIUS server. The guest VLAN must be specified after the authentication completes. Which action must be performed to allow the ISE server to specify the guest VLAN?

- A. Set AAA Policy name.
- B. Enable AAA Override
- C. Set RADIUS Profiling
- D. Enable Network Access Control State.

Answer: C

NEW QUESTION 55

DRAG DROP - (Topic 4)  
Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.

declarative

uses Ruby

uses Python

procedural

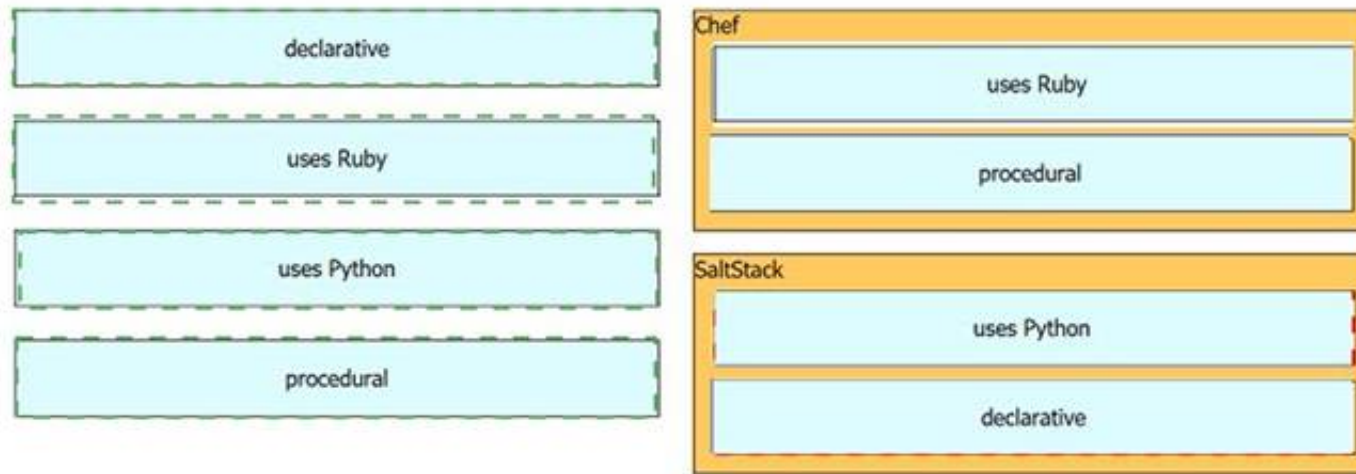
Chef

SaltStack

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



#### NEW QUESTION 59

- (Topic 4)

In a Cisco StackWise Virtual environment, which planes are virtually combined in the common logical switch?

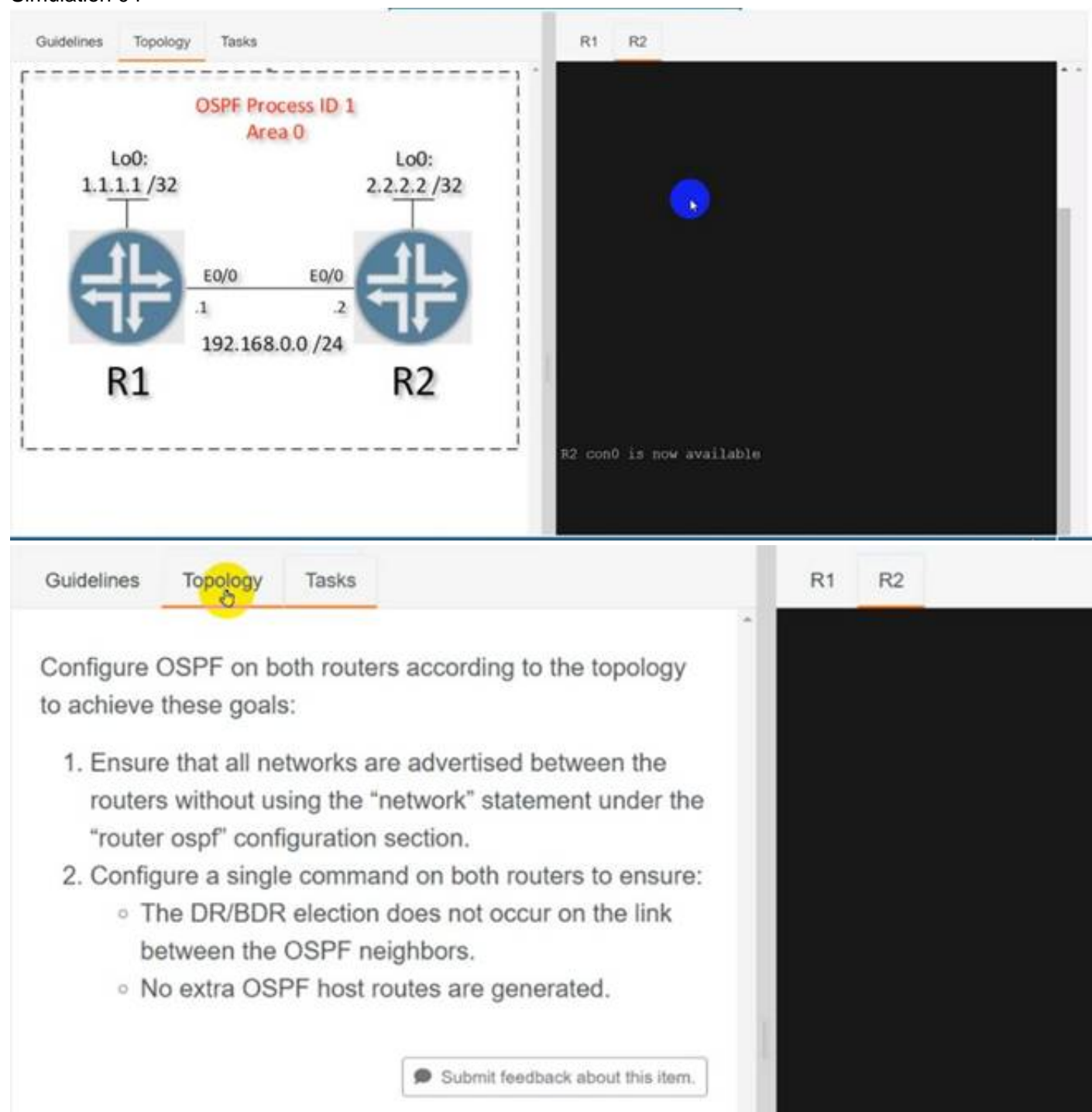
- A. control, and forwarding
- B. management and data
- C. control and management
- D. control and data

**Answer: C**

#### NEW QUESTION 60

SIMULATION - (Topic 4)

Simulation 04



The simulation interface is divided into two main sections. The top section, titled 'Topology', shows a network diagram with two routers, R1 and R2, connected via their Ethernet interfaces (E0/0). R1 has a loopback interface (Lo0) with IP 1.1.1.1/32. R2 has a loopback interface (Lo0) with IP 2.2.2.2/32. The network 192.168.0.0/24 is shared between them. The bottom section, titled 'Tasks', provides instructions for configuring OSPF on both routers. The instructions are as follows:

Configure OSPF on both routers according to the topology to achieve these goals:

1. Ensure that all networks are advertised between the routers without using the "network" statement under the "router ospf" configuration section.
2. Configure a single command on both routers to ensure:
  - The DR/BDR election does not occur on the link between the OSPF neighbors.
  - No extra OSPF host routes are generated.

A 'Submit feedback about this item.' button is located at the bottom of the tasks section.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**



R1  
Router ospf 1 Int loop0  
Ip ospf 1 area 0 Int et0/0  
Ip ospf 1 area 0  
Ip ospf network point-to-point Copy run start  
R2  
Router ospf 1 Int loop0  
Ip ospf 1 area 0 Int et0/0  
Ip ospf 1 area 0  
Ip ospf network point-to-point Copy run start  
Verification:-

```
R2#sh ip os
R2#sh ip ospf nei
R2#sh ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address
  Interface
1.1.1.1          0    FULL/  -        00:00:34    192.168.0
.1      Ethernet0/0
R2#
```

```
R1#sh ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address
  Interface
2.2.2.2          0    FULL/  -        00:00:32    192.168
.2      Ethernet0/0
R1#sh ip ospf route

          OSPF Router with ID (1.1.1.1) (Process ID 1)

          Base Topology (MTID 0)

          Area BACKBONE(0)

          Intra-area Route List

* 192.168.0.0/24, Intra, cost 10, area 0, Connected
  via 192.168.0.1, Ethernet0/0
* 1.1.1.1/32, Intra, cost 1, area 0, Connected
  via 1.1.1.1, Loopback0
*> 2.2.2.2/32, Intra, cost 11, area 0
  via 192.168.0.2, Ethernet0/0

          First Hop Forwarding Gateway Tree

192.168.0.1 on Ethernet0/0, count 1
192.168.0.2 on Ethernet0/0, count 1
1.1.1.1 on Loopback0, count 1
R1#
```

NEW QUESTION 64

- (Topic 4)  
Which TLV value must be added to Option 43 when DHCP is used to ensure that APs join the WLC?

- A. 0x77
- B. AAA
- C. 0xf1
- D. 642

Answer: C

NEW QUESTION 69



- (Topic 4)

Which collection contains the resources to obtain a list of fabric nodes through the vManage API?

- A. device management
- B. administration
- C. device inventory
- D. monitoring

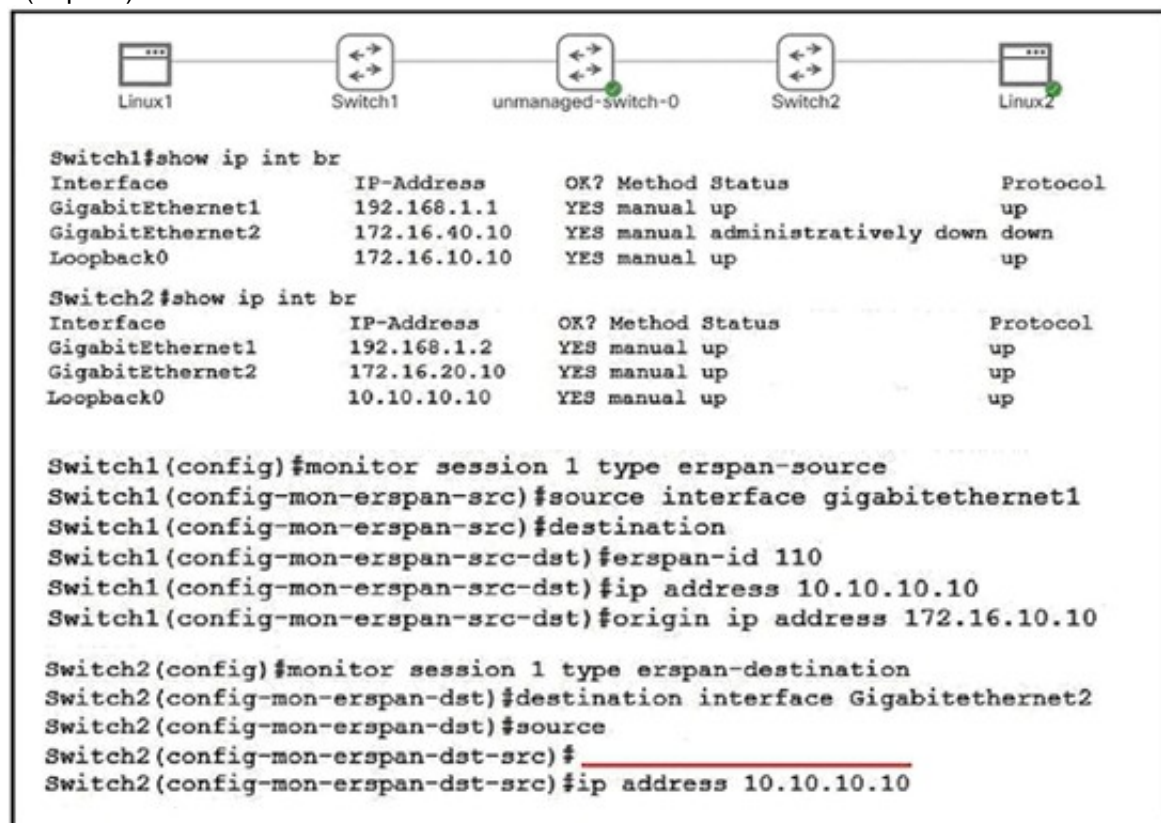
**Answer: C**

**Explanation:**

The collection that contains the resources to obtain a list of fabric nodes through the vManage API is the device inventory collection. This collection can be accessed through the Cisco Encor Documents and provides resources such as the Fabric Visualization, Device List, and Fabric Node Inventory APIs. These APIs can be used to obtain information about the fabric nodes, such as the device inventory, status, and version.

**NEW QUESTION 73**

- (Topic 4)



Refer to the exhibit. An engineer must configure an ERSPAN tunnel that mirrors traffic from linux1 on Switch1 to Linux2 on Switch2. Which command must be added to the destination configuration to enable the ERSPAN tunnel?

- A. (config-mon-erspan-dst-src)# origin ip address 172.16.10.10
- B. (config-mon-erspan-dst-src)# erspan-id 172.16.10.10
- C. (config-mon-erspan-dst-src)# no shut
- D. (config-mon-erspan-dst-src)# erspan-id 110

**Answer: D**

**NEW QUESTION 76**

- (Topic 4)

Where is the wireless LAN controller located in a mobility express deployment?

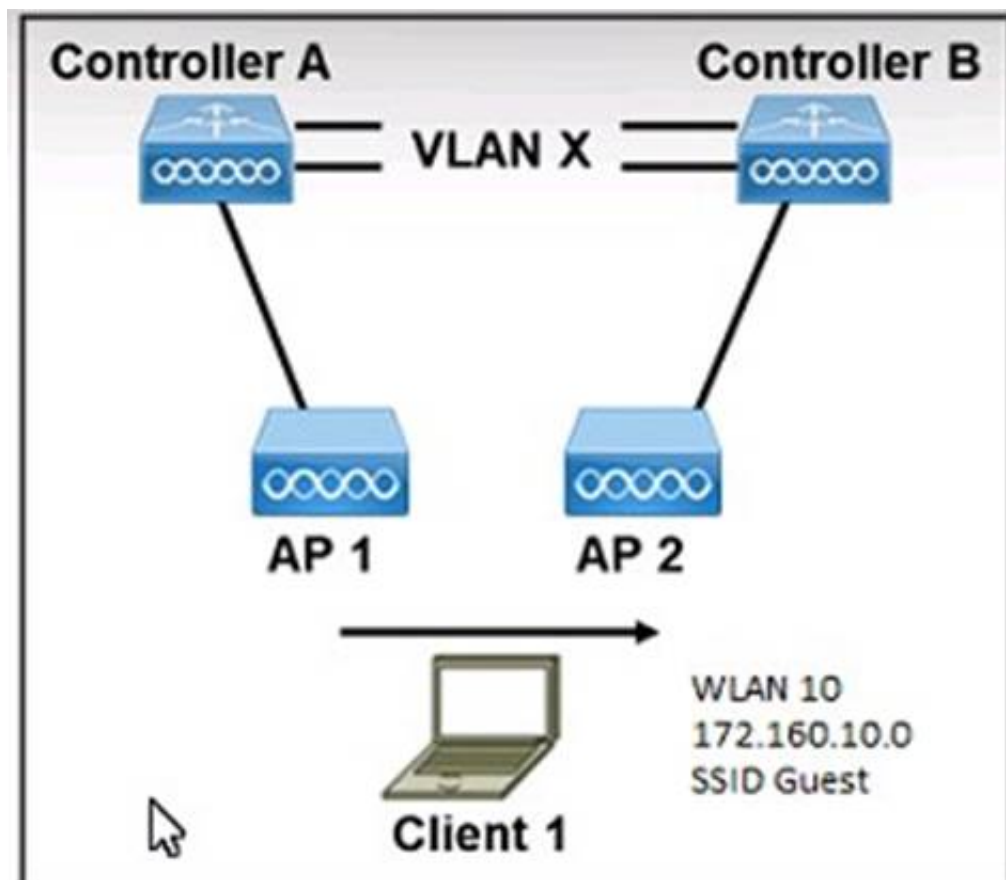
- A. There is no wireless LAN controller in the network.
- B. The wireless LAN controller is embedded into the access point.
- C. The wireless LAN controller exists in the cloud.
- D. The wireless LAN controller exists in a server that is dedicated for this purpose.

**Answer: B**

**NEW QUESTION 78**

- (Topic 4)

Refer to the exhibit.



Both controllers are in the same mobility group. Which result occurs when client 1 roams between APs that are registered to different controllers in the same WLAN?

- A. Client 1 contact controller B by using an EoIP tunnel.
- B. CAPWAP tunnel is created between controller A and controller B.
- C. Client 1 users an EoIP tunnel to contact controller A.
- D. The client database entry moves from controller A to controller B.

**Answer:** D

#### NEW QUESTION 81

- (Topic 4)

Based on the router's API output in JSON format below, which Python code will display the value of the "hostname" key?

```
{
  "response": [{
    "family": "Switches",
    "macAddress": "00:42:50:62:99:00",
    "hostname": "SwitchIDF14",
    "upTime": "352 days, 6:17:26:10",
    "lastUpdated": "2020-07-12 21:15:29"
  }]
}
```

- ☐ json\_data = json.loads(response.text)  
print(json\_data[response][0][hostname])
- ☐ json\_data = json.loads(response.text)  
print(json\_data["response"]["family"]["hostname"])
- ☐ json\_data = response.json()  
print(json\_data["response"][0]["hostname"])
- ☐ json\_data = response.json()  
print(json\_data["response"][family][hostname])

- A. Option A
- B. Option B

C. Option C  
D. Option D

**Answer:** B

#### NEW QUESTION 82

- (Topic 4)

An engineer must configure a new WLAN that allows a user to enter a passphrase and provides forward secrecy as a security measure. Which Layer 2 WLAN configuration is required on the Cisco WLC?

- A. WPA2 Personal
- B. WPA3 Enterprise
- C. WPA3 Personal
- D. WPA2 Enterprise

**Answer:** C

#### NEW QUESTION 86

- (Topic 4)

```
R1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 65001
BGP table version is 1, main routing table version 1

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.2  4      65002    0      0       1   0   0 00:00:15 Idle

R1#show ip interface brief | include 192.168.12
FastEthernet0/0      192.168.12.1  YES NVRAM  up            up

R2#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 65002
BGP table version is 1, main routing table version 1

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.1  4      65001    0      0       1   0   0 00:01:00 Idle (Admin)

R2#show ip interface brief | include 192.168.12
Ethernet0/0         192.168.12.2  YES NVRAM  up            up

R2#ping 192.168.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Refer to the exhibit. R1 and R2 are directly connected, but the BGP session does not establish. Which action must be taken to build an eBGP session?

- A. Configure ip route 1.1.1.1 0.0.0.0 192.168.12.1 on R2.
- B. Configure neighbor 192.168.12.1 activate under R2 BGP process.
- C. Configure neighbor 2.2.2.2 remote-as 65002 under R1 BGP process.
- D. Configure no neighbor 192.168.12.1 shutdown under R2 BGP process.

**Answer:** D

#### NEW QUESTION 87

- (Topic 4)

When using BFD in a network design, which consideration must be made?

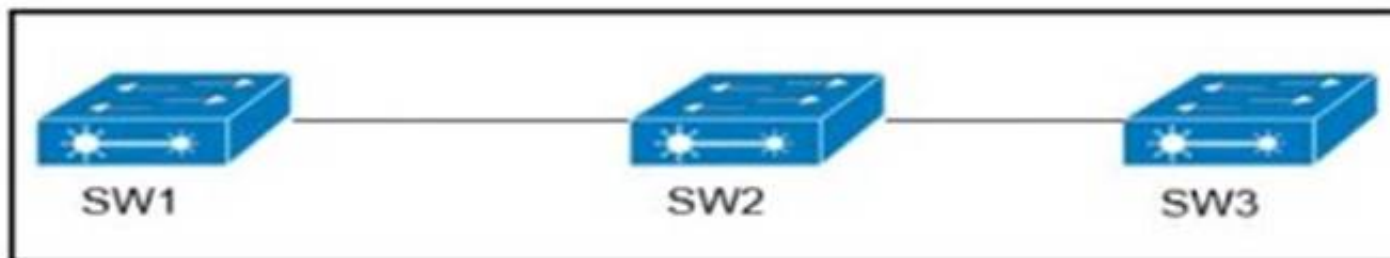
- A. BFD is used with first hop routing protocols to provide subsecond convergence.
- B. BFD is more CPU-intensive than using reduced hold timers with routing protocols.
- C. BFD is used with dynamic routing protocols to provide subsecond convergence.
- D. BFD is used with NSF and graceful to provide subsecond convergence.

**Answer:** C

#### NEW QUESTION 91

- (Topic 1)

Refer to exhibit.



VLANs 50 and 60 exist on the trunk links between all switches All access ports on SW3 are



configured for VLAN 50 and SW1 is the VTP server Which command ensures that SW3 receives frames only from VLAN 50?

- A. SW1 (config)#vtp pruning
- B. SW3(config)#vtp mode transparent
- C. SW2(config)=vtp pruning
- D. SW1 (config >»vtp mode transparent

**Answer:** A

**Explanation:**

SW3 does not have VLAN 60 so it should not receive traffic for this VLAN (sent from SW2). Therefore we should configure VTP Pruning on SW3 so that SW2 does not forward VLAN 60 traffic to SW3. Also notice that we need to configure pruning on SW1 (the VTP Server), not SW2.

**NEW QUESTION 94**

- (Topic 1)

Which method should an engineer use to deal with a long-standing contention issue between any two VMs on the same host?

- A. Adjust the resource reservation limits
- B. Live migrate the VM to another host
- C. Reset the VM
- D. Reset the host

**Answer:** A

**NEW QUESTION 95**

- (Topic 2)

In a Cisco StackWise Virtual environment, which planes are virtually combined in the common logical switch?

- A. management and data
- B. control and management
- C. control, and forwarding
- D. control and data

**Answer:** B

**NEW QUESTION 99**

- (Topic 2)

What is a characteristic of Cisco StackWise technology?

- A. It uses proprietary cabling
- B. It supports devices that are geographically separated
- C. It combines exactly two devices
- D. It is supported on the Cisco 4500 series.

**Answer:** C

**NEW QUESTION 100**

DRAG DROP - (Topic 2)

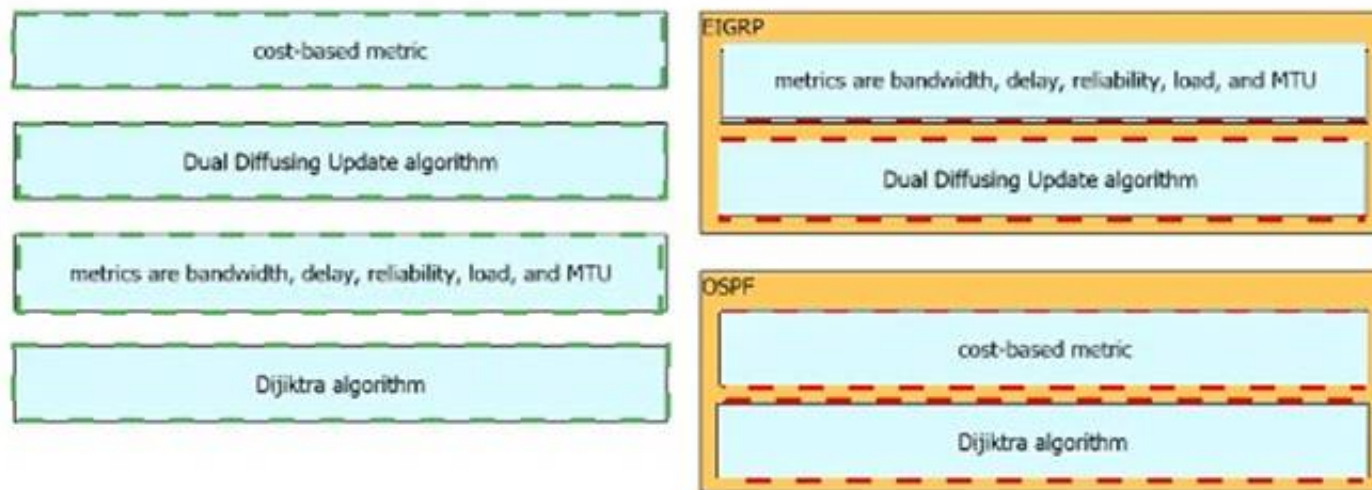
Drag and drop the characteristics from the left onto the routing protocols they describe on the right

cost-based metric	EIGRP
Dual Diffusing Update algorithm	
metrics are bandwidth, delay, reliability, load, and MTU	OSPF
Dijkstra algorithm	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



#### NEW QUESTION 104

- (Topic 2)

Why is an AP joining a different WLC than the one specified through option 43?

- A. The WLC is running a different software version.
- B. The API is joining a primed WLC
- C. The AP multicast traffic unable to reach the WLC through Layer 3.
- D. The APs broadcast traffic is unable to reach the WLC through Layer 2.

**Answer:** B

#### NEW QUESTION 107

- (Topic 2)

Which NGFW mode block flows crossing the firewall?

- A. Passive
- B. Tap
- C. Inline tap
- D. Inline

**Answer:** D

#### Explanation:

Firepower Threat Defense (FTD) provides six interface modes which are: Routed, Switched, Inline Pair, Inline Pair with Tap, Passive, Passive (ERSPAN). When Inline Pair Mode is in use, packets can be blocked since they are processed inline. When you use Inline Pair mode, the packet goes mainly through the FTD Snort engine. When Tap Mode is enabled, a copy of the packet is inspected and dropped internally while the actual traffic goes through FTD unmodified.

#### NEW QUESTION 112

- (Topic 2)

An engineer is implementing a route map to support redistribution within BGP. The route map must be configured to permit all unmatched routes. Which action must the engineer perform to complete this task?

- A. Include a permit statement as the first entry
- B. Include at least one explicit deny statement
- C. Remove the implicit deny entry
- D. Include a permit statement as the last entry

**Answer:** D

#### NEW QUESTION 114

- (Topic 2)

Refer to the exhibit.

```
vlan 222
  remote-span
!
vlan 223
  remote-span
!
monitor session 1 source interface FastEthernet0/1 tx
monitor session 1 source interface FastEthernet0/2 rx
monitor session 1 source interface port-channel 5
monitor session 1 destination remote vlan 222
!
```

What is the result when a technician adds the monitor session 1 destination remote vlan 223 command?

- A. The RSPAN VLAN is replaced by VLAN 223.
- B. RSPAN traffic is sent to VLANs 222 and 223



- C. An error is flagged for configuring two destinations.
- D. RSPAN traffic is split between VLANs 222 and 223.

**Answer:** A

#### NEW QUESTION 116

- (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 118

DRAG DROP - (Topic 2)

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

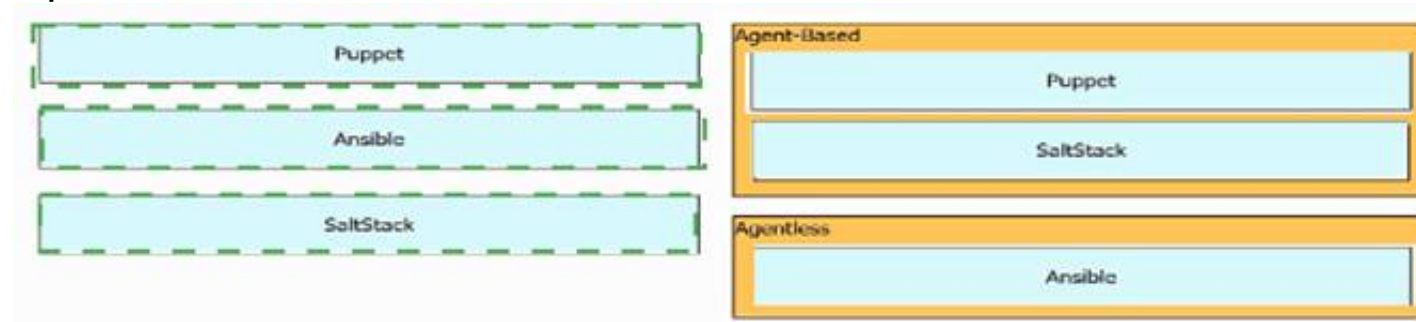


The interface shows three light blue boxes on the left labeled 'Puppet', 'Ansible', and 'SaltStack'. On the right, there are two yellow boxes with orange borders. The top box is labeled 'Agent-Based' and contains two empty slots. The bottom box is labeled 'Agentless' and contains one empty slot.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



The interface shows the same three light blue boxes on the left. On the right, the 'Agent-Based' box now contains 'Puppet' and 'SaltStack', and the 'Agentless' box contains 'Ansible'. The boxes on the left have dashed green borders, indicating they were dragged from there.

#### NEW QUESTION 121

- (Topic 2)

Which technology does VXLAN use to provide segmentation for Layer 2 and Layer 3 traffic?

- A. bridge domain
- B. VLAN
- C. VRF
- D. VNI

**Answer:** D

**Explanation:**

VXLAN has a 24-bit VXLAN network identifier (VNI), which allows for up to 16 million (= 2<sup>24</sup>) VXLAN segments to coexist within the same infrastructure. This surely solve the small number of traditional VLANs.

#### NEW QUESTION 126

- (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 penodically 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 start new sessions with sources and receivers.

**Answer:** D

#### NEW QUESTION 129

DRAG DROP - (Topic 2)

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

The default Administrative Distance is equal to 110.
It requires an Autonomous System number to create a routing instance for exchanging routing information.
It uses virtual links to connect two parts of a partitioned backbone through a non-backbone area.
It is an Advanced Distance Vector routing protocol.
It relies on the Diffused Update Algorithm to calculate the shortest path to a destination.
It requires a process ID that is local to the router.

EIGRP
OSPF

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The default Administrative Distance is equal to 110.
It requires an Autonomous System number to create a routing instance for exchanging routing information.
It uses virtual links to connect two parts of a partitioned backbone through a non-backbone area.
It is an Advanced Distance Vector routing protocol.
It relies on the Diffused Update Algorithm to calculate the shortest path to a destination.
It requires a process ID that is local to the router.

EIGRP
It requires an Autonomous System number to create a routing instance for exchanging routing information.
It is an Advanced Distance Vector routing protocol.
It relies on the Diffused Update Algorithm to calculate the shortest path to a destination.
OSPF
The default Administrative Distance is equal to 110.
It uses virtual links to connect two parts of a partitioned backbone through a non-backbone area.
It requires a process ID that is local to the router.

NEW QUESTION 131

- (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 134

- (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 136

- (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 138

- (Topic 2)

What is the function of a control-plane node In a Cisco SD-Access solution?

- A. to run a mapping system that manages endpoint to network device relationships
- B. to implement policies and communicate with networks outside the fabric
- C. to connect external Layer 3 networks to the SD-Access fabric
- D. to connect APs and wireless endpoints to the SD-Access fabric

**Answer:** A

#### NEW QUESTION 139

- (Topic 2)

A customer wants to provide wireless access to contractors using a guest portal on Cisco ISE. The portal is also used by employees. A solution is implemented, but contractors receive a certificate error when they attempt to access the portal. Employees can access the portal without any errors. Which change must be implemented to allow the contractors and employees to access the portal?

- A. Install a trusted third-party certificate on the Cisco ISE.
- B. Install an Internal CA signed certificate on the contractor devices
- C. Install an internal CA signed certificate on the Cisco ISE
- D. install a trusted third-party certificate on the contractor devices.

**Answer:** C

#### NEW QUESTION 143

- (Topic 2)

Which element enables communication between guest VMs within a virtualized environment?

- A. hypervisor



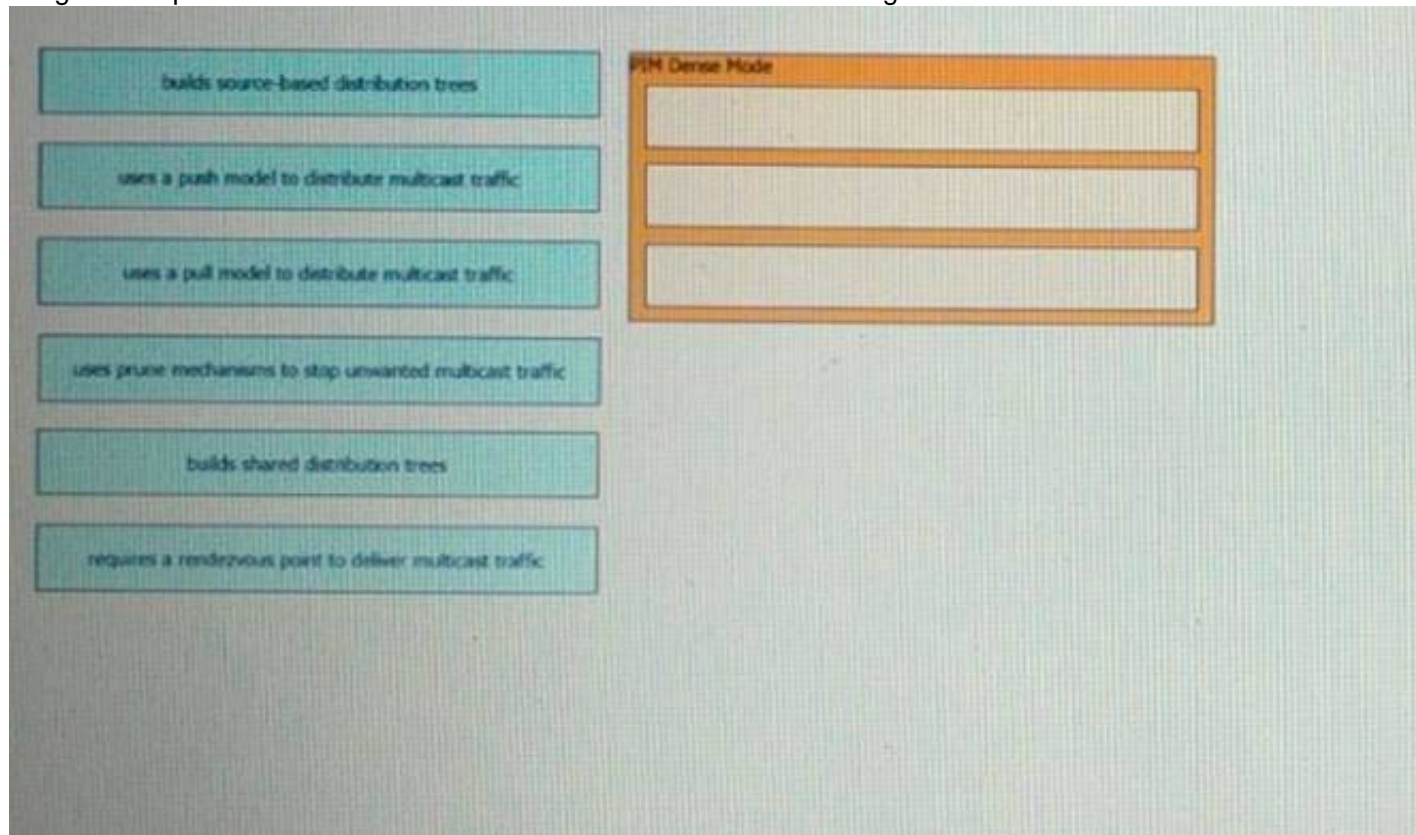
- B. vSwitch
- C. virtual router
- D. pNIC

**Answer:** B

#### NEW QUESTION 144

DRAG DROP - (Topic 2)

Drag and drop characteristics of PIM dense mode from the left to the right.



- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

PIM-DM supports only source trees – that is, (S,G) entries—and cannot be used to build a shared distribution tree.

#### NEW QUESTION 148

- (Topic 2)

Refer to the exhibit:

```
R1#show running-config interface fa0/0
Building configuration...

Current configuration: 192 bytes
!
interface FastEthernet0/0
 ip address 192.68.3.5 255.255.255.0
 duplex full
 vrrp 1 ip 192.168.3.1
 vrrp 1 priority 110
 vrrp 1 authentication text cisco
 vrrp 1 track 20 decrement 20
end

R1#show running-config | include track 20
track 20 ip route 10.10.1.1 255.255.255.255 reachability
```

```
R2#show running-config interface fa0/0
Building configuration...

Current configuration: 141 bytes
!
interface FastEthernet0/0
 ip address 192.68.3.2 255.255.255.0
 duplex full
 vrrp 1 ip 192.168.3.1
 vrrp 1 authentication text cisco
end
```

An engineer configures VRRP and issues the show commands to verify operation. What does the engineer confirm about VRRP group 1 from the output?

- A. There is no route to 10.10.1.1/32 in R2's routing table
- B. If R1 reboots, R2 becomes the master virtual router until R2 reboots
- C. Communication between VRRP members is encrypted using MD5
- D. R1 is primary if 10.10.1.1/32 is in its routing table

**Answer:** D

#### NEW QUESTION 153

- (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 156

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

#### NEW QUESTION 158

- (Topic 2)

Which feature does Cisco TrustSec use to provide scalable, secure communication throughout a network?

- A. security group tag ACL assigned to each port on a switch
- B. security group tag number assigned to each port on a network
- C. security group tag number assigned to each user on a switch
- D. security group tag ACL assigned to each router on a network

Answer: B

Explanation:

Cisco TrustSec uses tags to represent logical group privilege. This tag, called a Security Group Tag (SGT), is used in access policies. The SGT is understood and is used to enforce traffic by Cisco switches, routers and firewalls . Cisco TrustSec is defined in three phases: classification, propagation and enforcement. When users and devices connect to a network, the network assigns a specific security group. This process is called classification. Classification can be based on the results of the authentication or by associating the SGT with an IP, VLAN, or port-profile (-> Answer 'security group tag ACL assigned to each port on a switch' and answer 'security group tag number assigned to each user on a switch' are not correct as they say "assigned ... on a switch" only. Answer 'security group tag ACL assigned to each router on a network' is not correct either as it says "assigned to each router").

#### NEW QUESTION 160

- (Topic 2)

Refer to the exhibit.

```
R1#show ip bgp sum
BGP router identifier 1.1.1.1, local AS number 65001
<output omitted>

Neighbor      V      AS MsgRcvd MsgSent   TblVer  InQ  OutQ  Up/Down   State/PfxRcd
192.168.50.2   4      65002    0        0         1    0    0 00:00:46 Idle (Admin)
```

Which command set changes the neighbor state from Idle (Admin) to Active?

A)

```
R1(config)#router bgp 65002
R1(config-router)#neighbor 192.168.50.2 activate
```

B)

```
R1(config)#router bgp 65001
R1(config-router)#neighbor 192.168.50.2 activate
```

C)

```
R1(config)#router bgp 65001
R1(config-router)#no neighbor 192.168.50.2 shutdown
```

D)

```
R1(config)#router bgp 65001
R1(config-router)#neighbor 192.168.50.2 remote-as 65001
```

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

**Answer: C**

#### NEW QUESTION 161

- (Topic 2)

Which action is performed by Link Management Protocol in a Cisco StackWise Virtual domain?

- A. It rejects any unidirectional link traffic forwarding
- B. It determines if the hardware is compatible to form the StackWise Virtual domain
- C. discovers the StackWise domain and brings up SVL interfaces.
- D. It determines which switch becomes active or standby

**Answer: A**

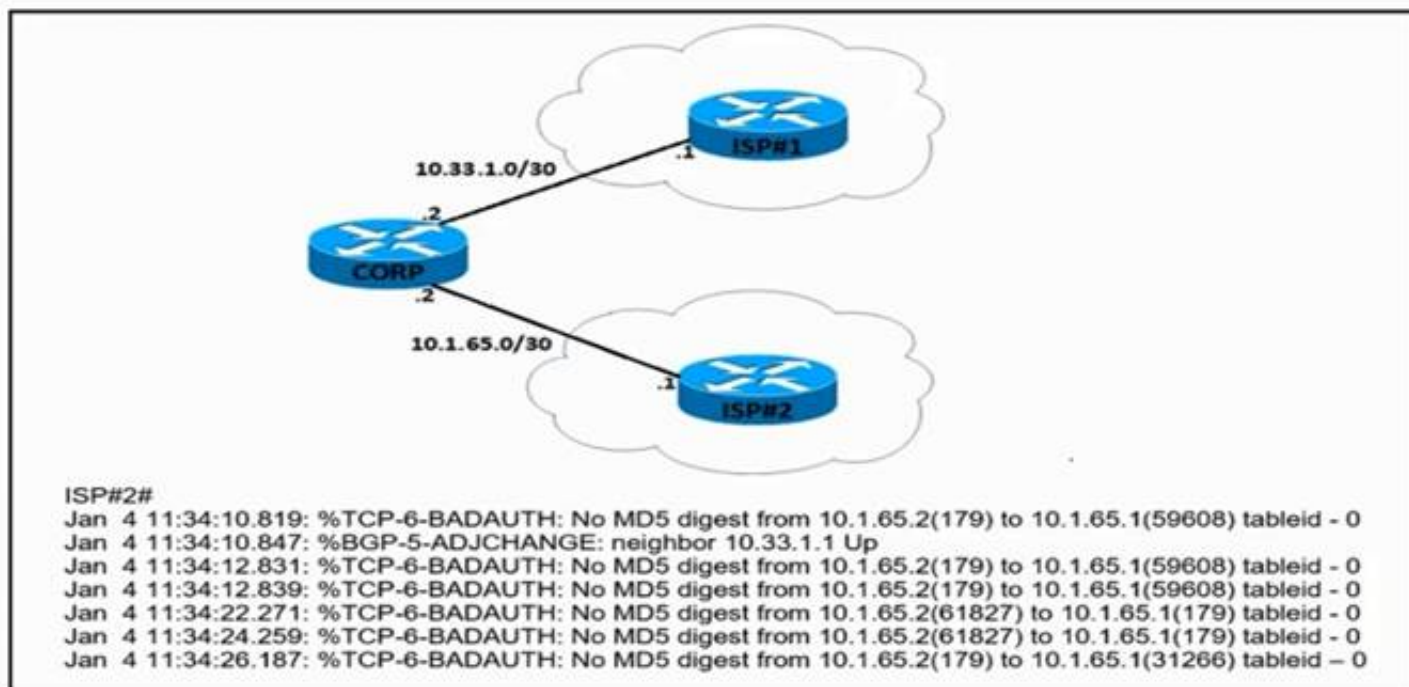
#### Explanation:

Reference: <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-stack-wp-cte-en.html>

#### NEW QUESTION 164

- (Topic 2)

Refer to the exhibit.



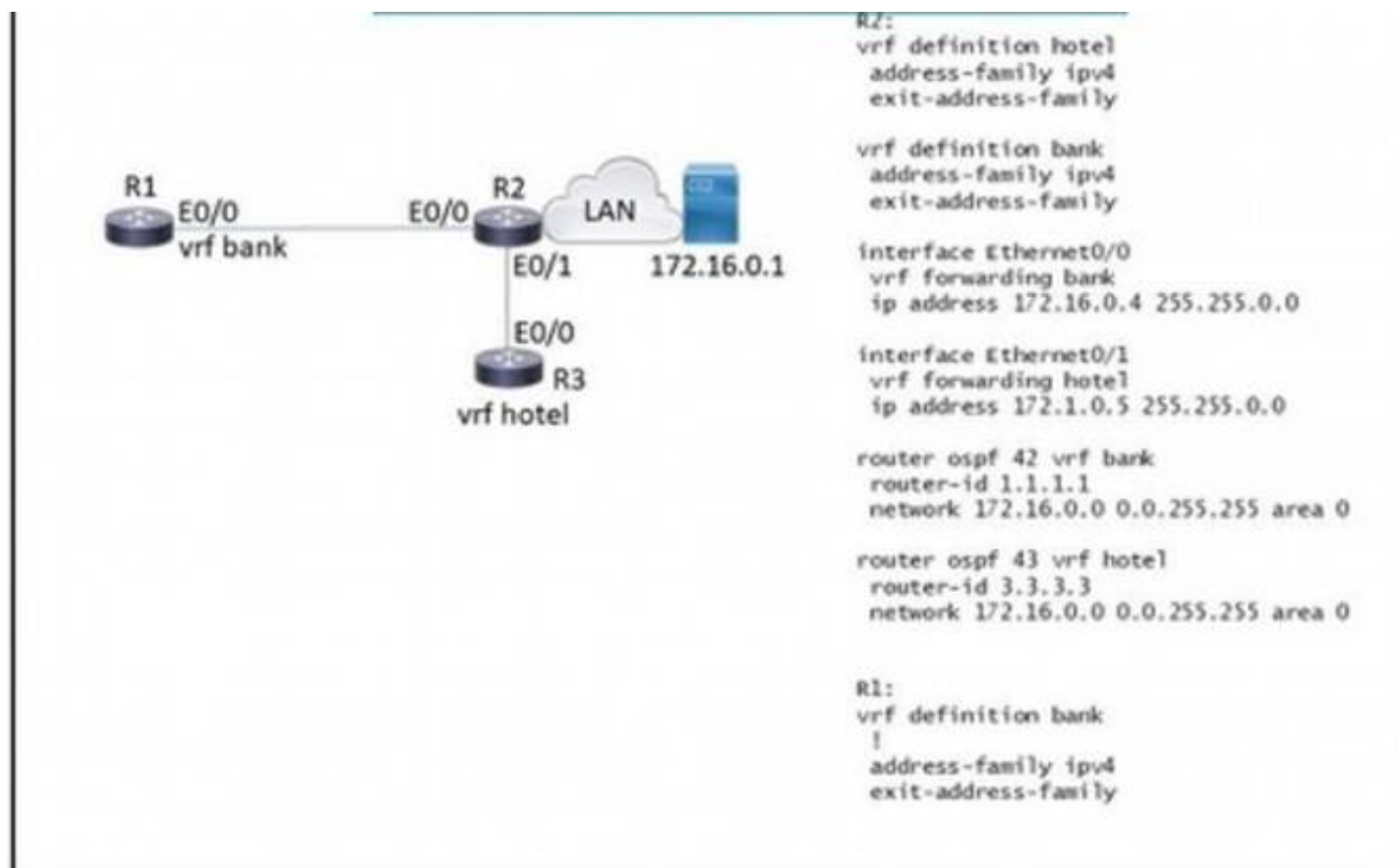
An engineer attempts to establish BGP peering between router CORP and two ISP routers. What is the root cause for the failure between CORP and ISP#2?

- A. Router ISP#2 is configured to use SHA-1 authentication.
- B. There is a password mismatch between router CORP and router ISP#2.
- C. Router CORP is configured with an extended access control list.
- D. MD5 authorization is configured incorrectly on router ISP#2.

**Answer: B**

#### NEW QUESTION 166

- (Topic 2)



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 169

DRAG DROP - (Topic 2)

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

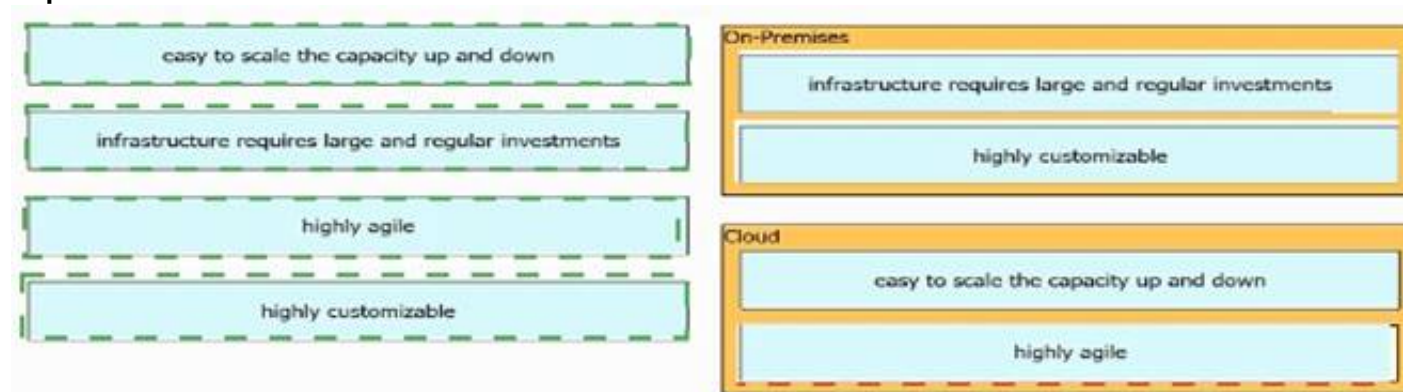




- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



#### NEW QUESTION 173

- (Topic 2)

Which two actions, when applied in the LAN network segment, will facilitate Layer 3 CAPWAP discovery for lightweight AP? (Choose two.)

- A. Utilize DHCP option 17.
- B. Configure WLC IP address on LAN switch.
- C. Utilize DHCP option 43.
- D. Configure an ip helper-address on the router interface
- E. Enable port security on the switch port

**Answer:** CE

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/119286-lap-notjoin-wlc-tshoot.html>

#### NEW QUESTION 175

- (Topic 2)

What is one primary REST security design principle?

- A. fail-safe defaults
- B. password hash
- C. adding a timestamp in requests
- D. OAuth

**Answer:** A

**Explanation:**

Reference: <https://yurisubach.com/2017/04/04/restful-api-security-principles/> "Fail-safe defaults Access to any resource (like API endpoint) should be denied by default. Access granted only in case of specific permission.

#### NEW QUESTION 176

- (Topic 2)

Which protocol infers that a YANG data model is being used?

- A. SNMP
- B. NX-API
- C. REST
- D. RESTCONF

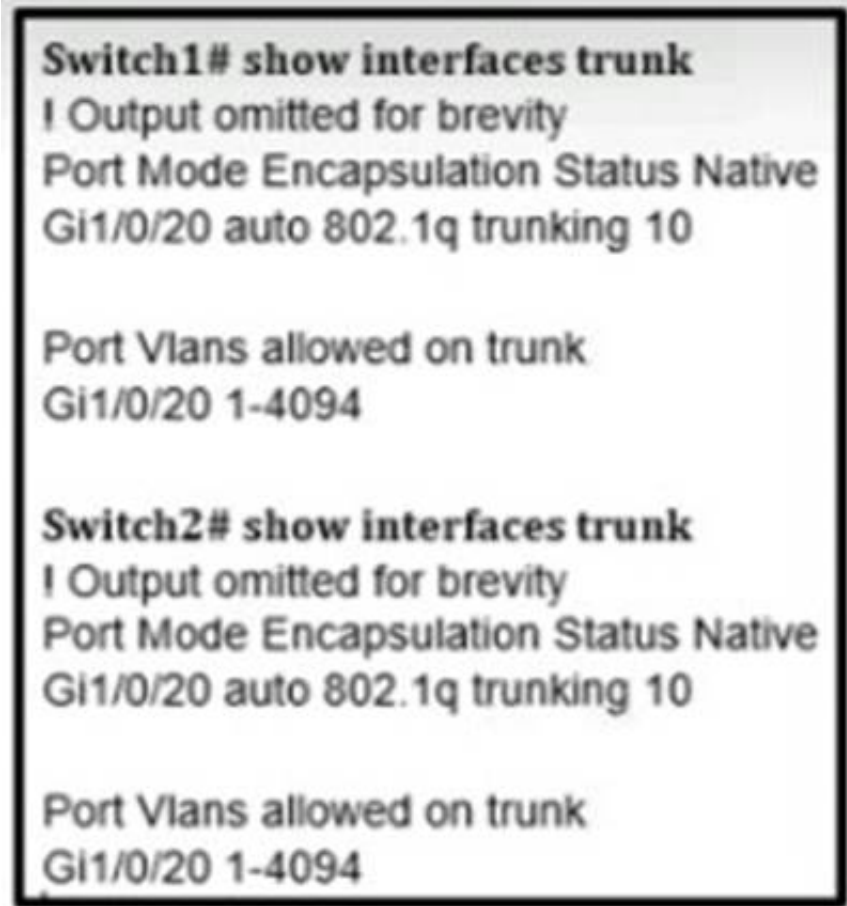
**Answer:** D

**Explanation:**

YANG (Yet another Next Generation) is a data modeling language for the definition of data sent over network management protocols such as the NETCONF and RESTCONF.

NEW QUESTION 180

- (Topic 2)  
Refer to the exhibit.



The trunk does not work over the back-to-back link between Switch1 interface Gi1/0/20 and Switch2 interface Gig1/0/20. Which configuration fixes the problem?

- A)  
Switch1(config)#interface gig1/0/20  
Switch1(config-if)#switchport mode dynamic auto
- B)  
Switch2(config)#interface gig1/0/20  
Switch2(config-if)#switchport mode dynamic desirable
- C)  
Switch1(config)#interface gig1/0/20  
Switch1(config-if)#switchport trunk native vlan 1  
Switch2(config)#interface gig1/0/20  
Switch2(config-if)#switchport trunk native vlan 1
- D)  
Switch2(config)#interface gig1/0/20  
Switch2(config-if)#switchport mode dynamic auto

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

Answer: B

NEW QUESTION 182

DRAG DROP - (Topic 2)  
Drag and drop the characteristics from the left onto the deployment models on the right.

long implementation timeframe

on-demand self-service

offers complex customization

Cloud

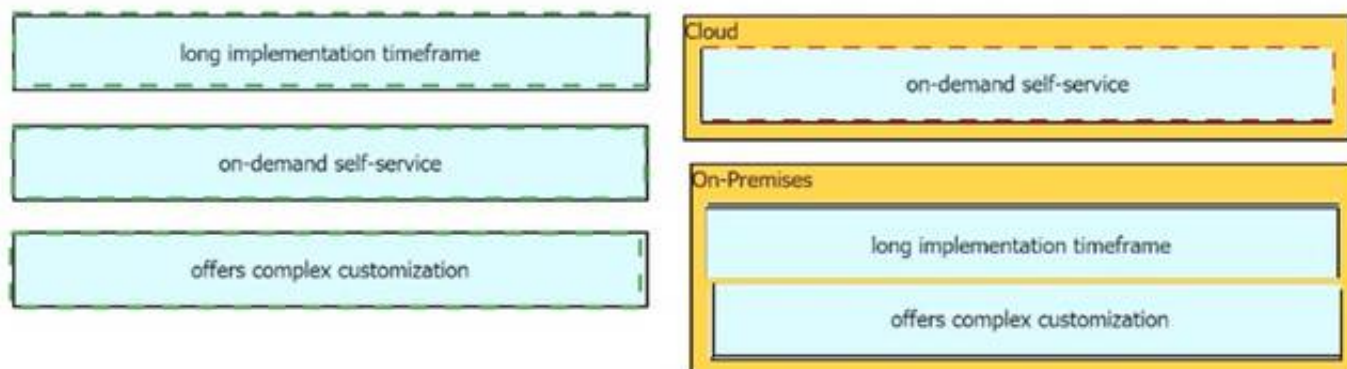
On-Premises



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



#### NEW QUESTION 187

- (Topic 2)

An engineer must create an EEM applet that sends a syslog message in the event a change happens in the network due to trouble with an OSPF process. Which action should the engineer use?

**event manager applet LogMessage**  
**event routing network 172.30.197.0/24 type all**

- A. action 1 syslog msg "OSPF ROUTING ERROR"
- B. action 1 syslog send "OSPF ROUTING ERROR"
- C. action 1 syslog pattern "OSPF ROUTING ERROR"
- D. action 1 syslog write "OSPF ROUTING ERROR"

**Answer:** C

#### NEW QUESTION 189

- (Topic 2)

Refer to the exhibit.

```
>>> netconf_data["GigabitEthernet"][0]["enabled"]  
u'false'  
>>> netconf_data["GigabitEthernet"][1]["enabled"]  
u'true'  
>>> netconf_data["GigabitEthernet"][2]["enabled"]  
u'false'  
>>> netconf_data["GigabitEthernet"][0]["description"]  
u'my description'
```

Which Python code snippet prints the descriptions of disabled interfaces only?

A)

```
for interface in netconf_data["GigabitEthernet"]:  
    if interface["disabled"] != 'true':  
        print(interface["description"])
```

B)

```
for interface in netconf_data["GigabitEthernet"]:  
    print(interface["enabled"])  
    print(interface["description"])
```

C)

```
for interface in netconf_data["GigabitEthernet"]:  
    if interface["enabled"] != 'false':  
        print(interface["description"])
```

D)

```
for interface in netconf_data["GigabitEthernet"]:  
    if interface["enabled"] != 'true':  
        print(interface["description"])
```

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

**Answer:** D

#### NEW QUESTION 194

- (Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 195

- (Topic 2)

Which two GRE features are configured to prevent fragmentation? (Choose two.)

- A. TCP MSS
- B. PMTUD
- C. DF bit Clear
- D. MTU ignore
- E. IP MTU
- F. TCP window size

**Answer:** AE

#### Explanation:

The **ip tcp adjust-mss** only affects TCP streams. Other kinds of IP traffic – UDP, SCTP, DCCP, ICMP, ESP, AH, to name just a few – won't be influenced by the **ip tcp adjust-mss** command, and so their datagrams must be fragmented at the IP layer. That's why it is necessary to properly **configure the ip mtu** command to let the router know how large the fragments of non-TCP-carrying IP packets can be.

#### NEW QUESTION 200

- (Topic 2)

Refer to the exhibit.

```
R1# sh run | begin line con
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  password 7 045802150C2E
  login
line vty 5 15
  password 7 045802150C2E
  login
!
end

R1# sh run | include aaa | enable
no aaa new-model
R1#
```

Which privilege level is assigned to VTY users?

- A. 1
- B. 7
- C. 13
- D. 15

**Answer:** A

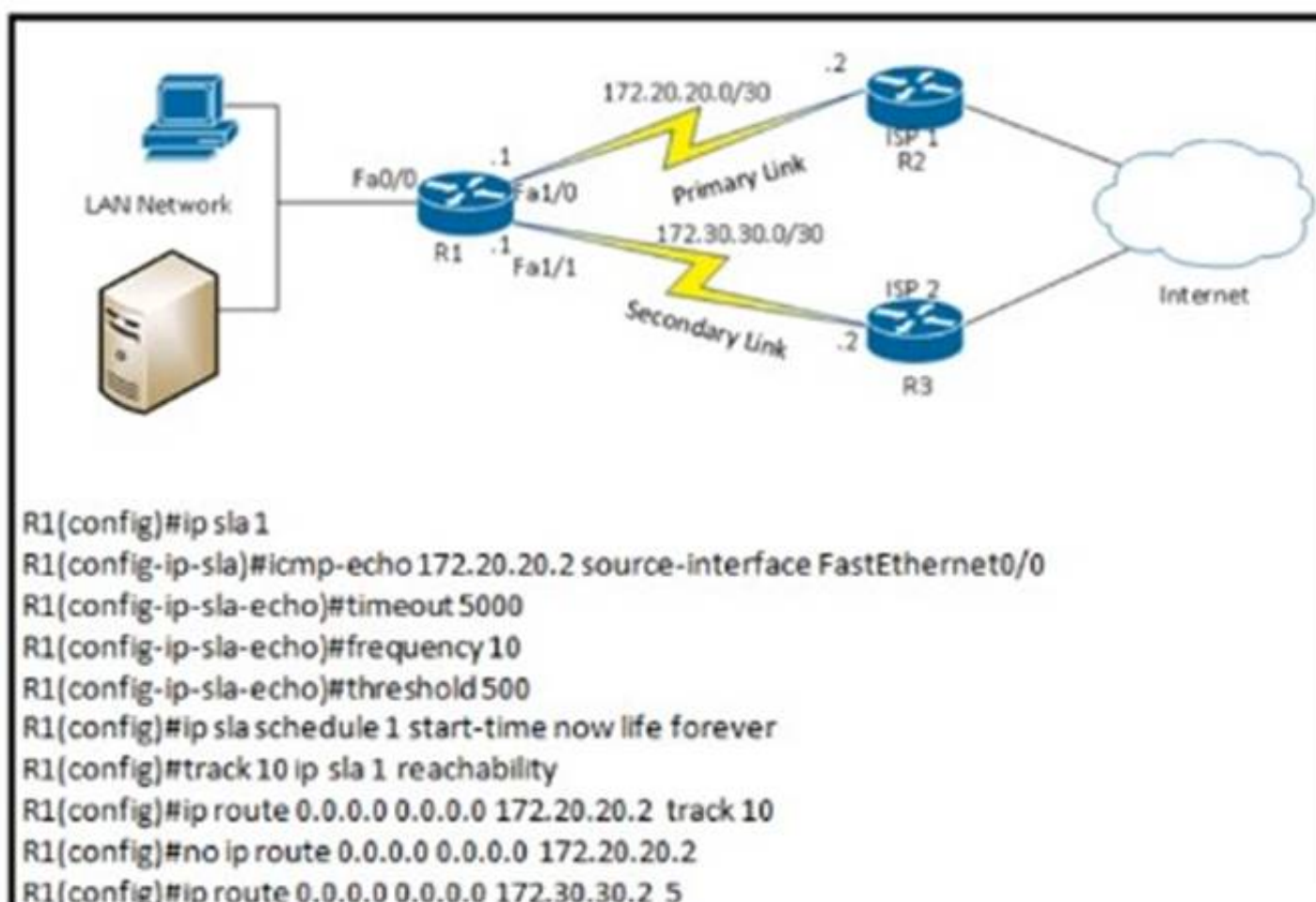
**Explanation:**

Lines (CON, AUX, VTY) default to level 1 privileges.

**NEW QUESTION 204**

- (Topic 2)

Refer to the exhibit.



What are two reasons for IP SLA tracking failure? (Choose two )

- A. The destination must be 172 30 30 2 for icmp-echo
- B. A route back to the R1 LAN network is missing in R2.
- C. The source-interface is configured incorrectly.
- D. The default route has the wrong next hop IP address
- E. The threshold value is wrong

**Answer:** BE

#### NEW QUESTION 207

- (Topic 2)

A customer wants to use a single SSID to authenticate IoT devices using different passwords. Which Layer 2 security type must be configured in conjunction with Cisco ISE to achieve this requirement?

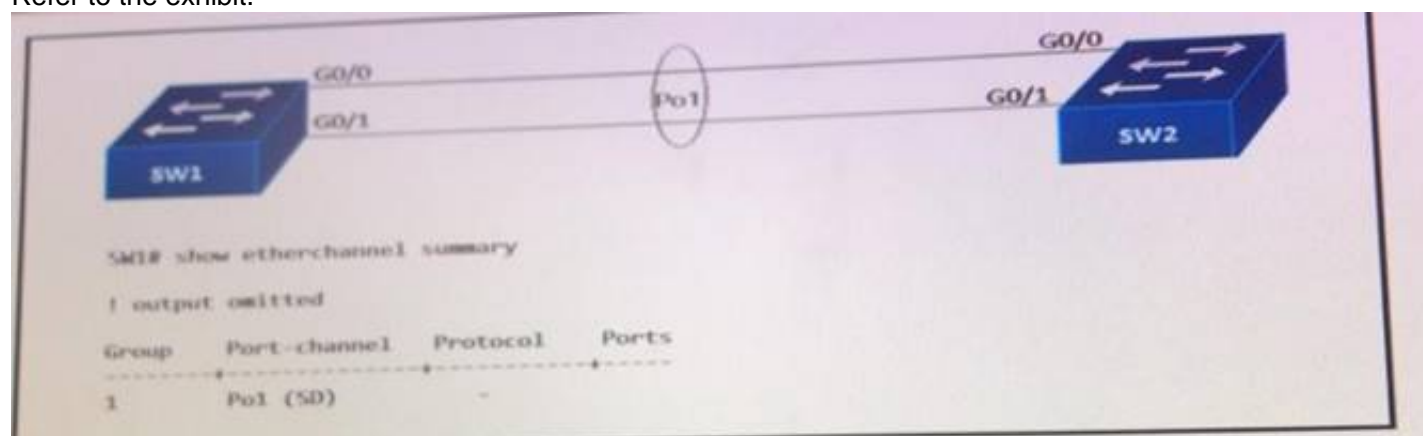
- A. Fast Transition
- B. Central Web Authentication
- C. Cisco Centralized Key Management
- D. Identity PSK

**Answer:** D

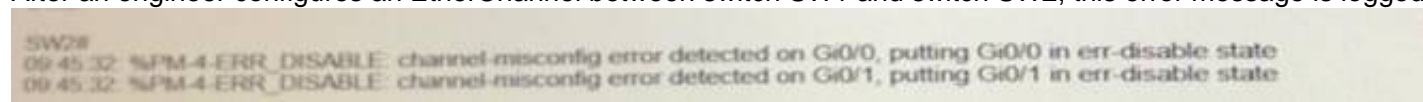
#### NEW QUESTION 211

- (Topic 2)

Refer to the exhibit.



After an engineer configures an EtherChannel between switch SW1 and switch SW2, this error message is logged on switch SW2.



Based on the output from SW1 and the log message received on Switch SW2, what action should the engineer take to resolve this issue?

- A. Configure the same protocol on the EtherChannel on switch SW1 and SW2.
- B. Connect the configuration error on interface Gi0/1 on switch SW1.
- C. Define the correct port members on the EtherChannel on switch SW1.
- D. Correct the configuration error on interface Gi0/0 switch SW1.

**Answer:** A

#### Explanation:

In this case, we are using your EtherChannel without a negotiation protocol. As a result, if the opposite switch is not also configured for EtherChannel operation on the respective ports, there is a danger of a switching loop. The EtherChannel Misconfiguration Guard tries to prevent that loop from occurring by disabling all the ports bundled in the EtherChannel.

#### NEW QUESTION 216

- (Topic 2)

What do Cisco DNA southbound APIs provide?

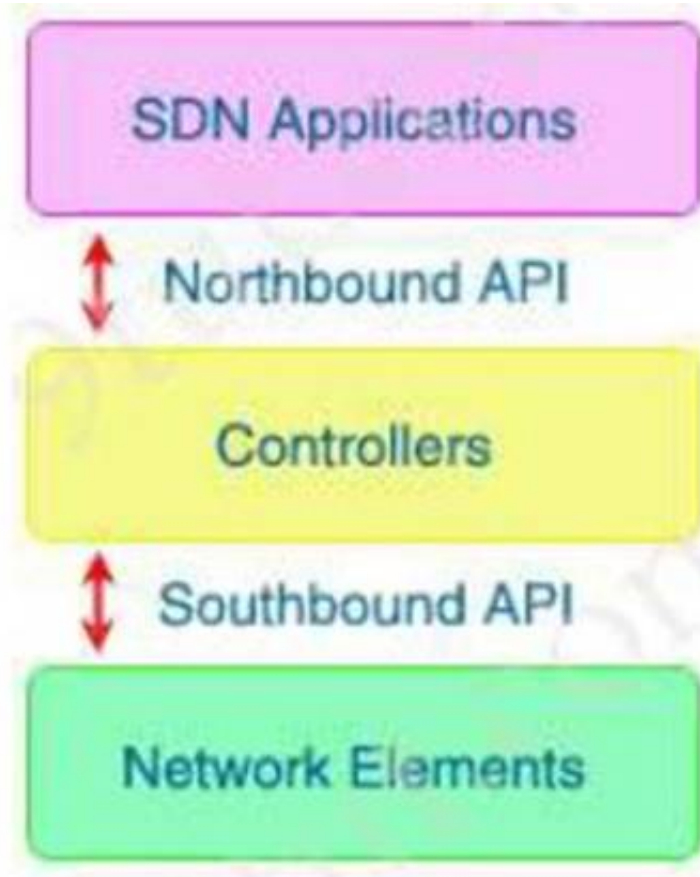
- A. Interface between the controller and the network devices
- B. NETCONF API interface for orchestration communication
- C. RESful API interface for orchestrator communication
- D. Interface between the controller and the consumer

**Answer:** A

#### Explanation:

The Southbound API is used to communicate with network devices.





#### NEW QUESTION 217

- (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 221

- (Topic 2)

Refer to the exhibit.

```

Hello due in 00:00:07
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/2/2, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 1 msec, maximum is 1 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
  
```

An engineer configures OSPF and wants to verify the configuration Which configuration is applied to this device?

A)  
**R1(config)#router ospf 1**  
**R1(config-router)#network 192.168.50.0 0.0.0.255 area 0**

B)  
**R1(config)#router ospf 1**  
**R1(config-router)#network 0.0.0.0 0.0.0.0 area 0**  
**R1(config-router)#no passive-interface Gi0/1**

C)  
**R1(config)#interface Gi0/1**  
**R1(config-if)#ip ospf enable**  
**R1(config-if)#ip ospf network broadcast**  
**R1(config-if)#no shutdown**

D)

```
R1(config)#interface Gi0/1
R1(config-if)#ip ospf 1 area 0
R1(config-if)#no shutdown
```

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

**Answer:** C

#### NEW QUESTION 224

- (Topic 2)

Which antenna type should be used for a site-to-site wireless connection?

- A. Omnidirectional
- B. dipole
- C. patch
- D. Yagi

**Answer:** D

**Explanation:**

Yagi Antenna

- Used to communicate in one direction (unidirectional)
- They have a longer range in comparison to Omni Antennas
- Typically only communicate with one other radio, however can talk to multiple
- More common to see used in remote locations

Graphical user interface, text Description automatically generated

#### NEW QUESTION 228

- (Topic 2)

A network monitoring system uses SNMP polling to record the statistics of router interfaces The SNMP queries work as expected until an engineer installs a new interface and reloads the router After this action, all SNMP queries for the router fail What is the cause of this issue?

- A. The SNMP community is configured incorrectly
- B. The SNMP interface index changed after reboot.
- C. The SNMP server traps are disabled for the interface index
- D. The SNMP server traps are disabled for the link state.

**Answer:** B

#### NEW QUESTION 232

- (Topic 2)

Refer to the exhibit.

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

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

Which JSON syntax is derived from this data?

- A)  
 {{{('First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': ['Running', 'Video games']), ('First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': ['Napping', 'Reading'])}}}
- B)  
 {'Person': [{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': 'Running', 'Video games'}, ('First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': 'Napping', 'Reading')]]}
- C)  
 {{{('First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': 'Running', 'Hobbies': 'Video games'), ('First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': 'Napping', 'Hobbies': 'Reading')}}}
- D)  
 {'Person': [{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': ['Running', 'Video games']}, ('First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': ['Napping', 'Reading'])]]}

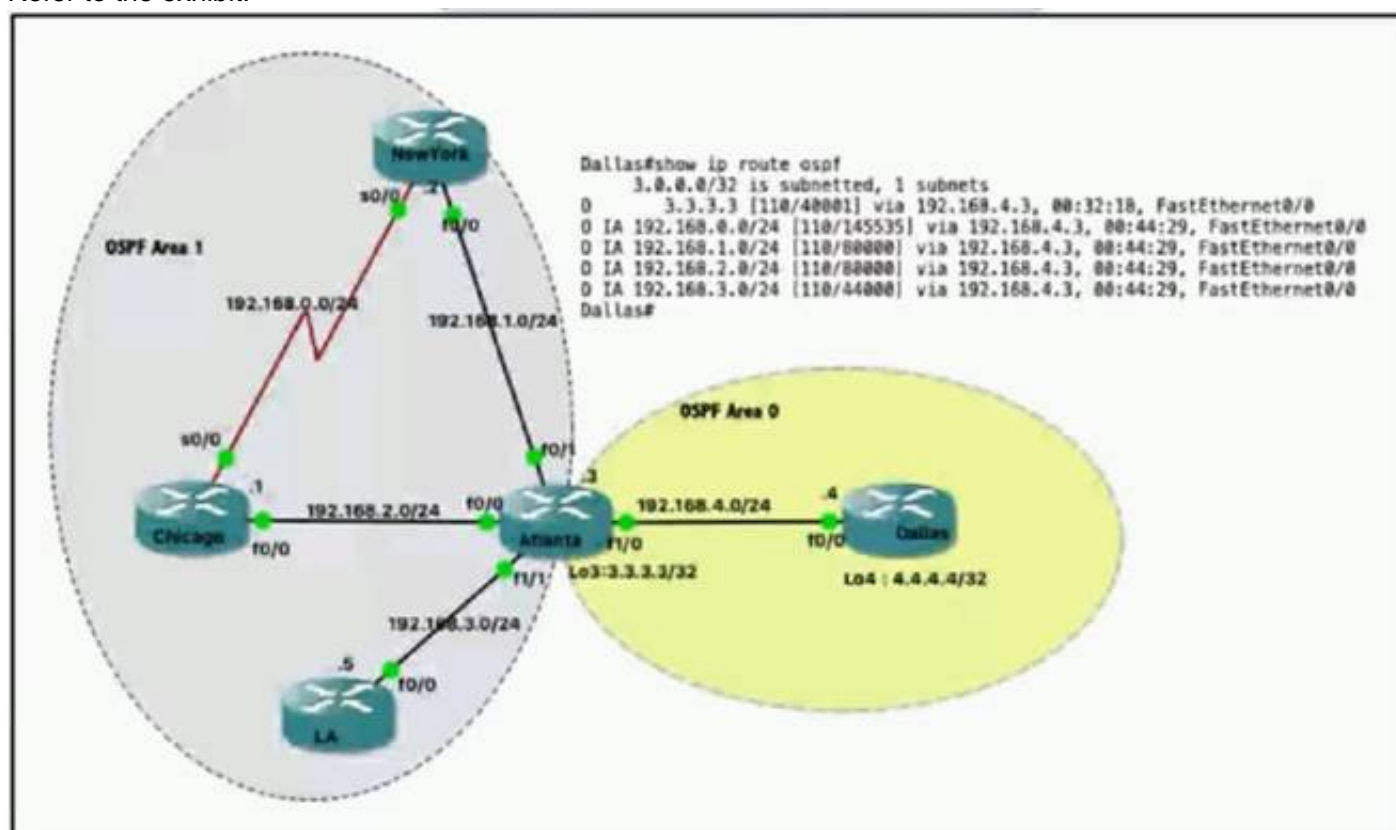
- A. Option A  
 B. Option B  
 C. Option C  
 D. Option D

**Answer: D**

#### NEW QUESTION 237

- (Topic 2)

Refer to the exhibit.



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

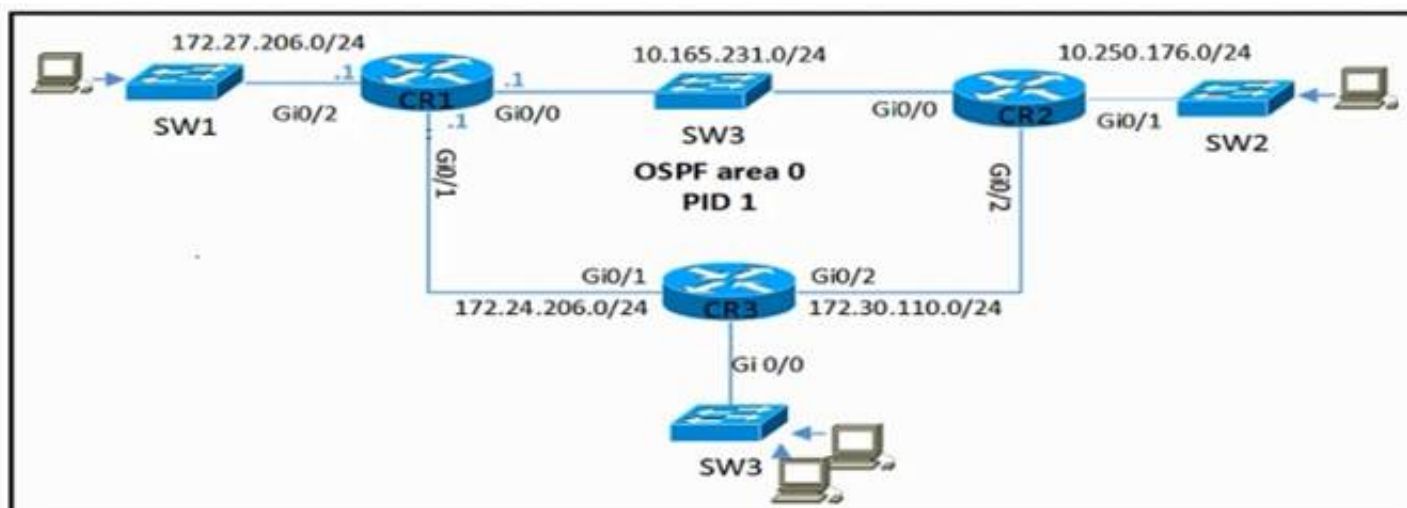
- A. Atlanta(config-route)#area 0 range 192.168.0.0 255.255.248.0  
 B. Atlanta(config-route)#area 0 range 192.168.0.0 255.255.252.0  
 C. Atlanta(config-route)#area 1 range 192.168.0.0 255.255.252.0  
 D. Atlanta(config-route)#area 1 range 192.168.0.0 255.255.248.0

**Answer: C**

#### NEW QUESTION 238

- (Topic 2)

Refer to the exhibit.



CR2 and CR3 are configured with OSPF. Which configuration, when applied to CR1, allows CR1 to exchange OSPF information with CR2 and CR3 but not with other network devices or on new interfaces that are added to CR1?

- A)



```
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
passive-interface GigabitEthernet0/2
```

B)

```
router ospf 1
network 10.165.231.0 0.0.0.255 area 0
network 172.27.206.0 0.0.0.255 area 0
network 172.24.206.0 0.0.0.255 area 0
```

C)

```
interface Gi0/2
ip ospf 1 area 0

router ospf 1
passive-interface GigabitEthernet0/2
```

D)

```
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
network 172.16.0.0 0.15.255.255 area 0
passive-interface GigabitEthernet0/2
```

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

**Answer:** D

**NEW QUESTION 242**

DRAG DROP - (Topic 2)

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

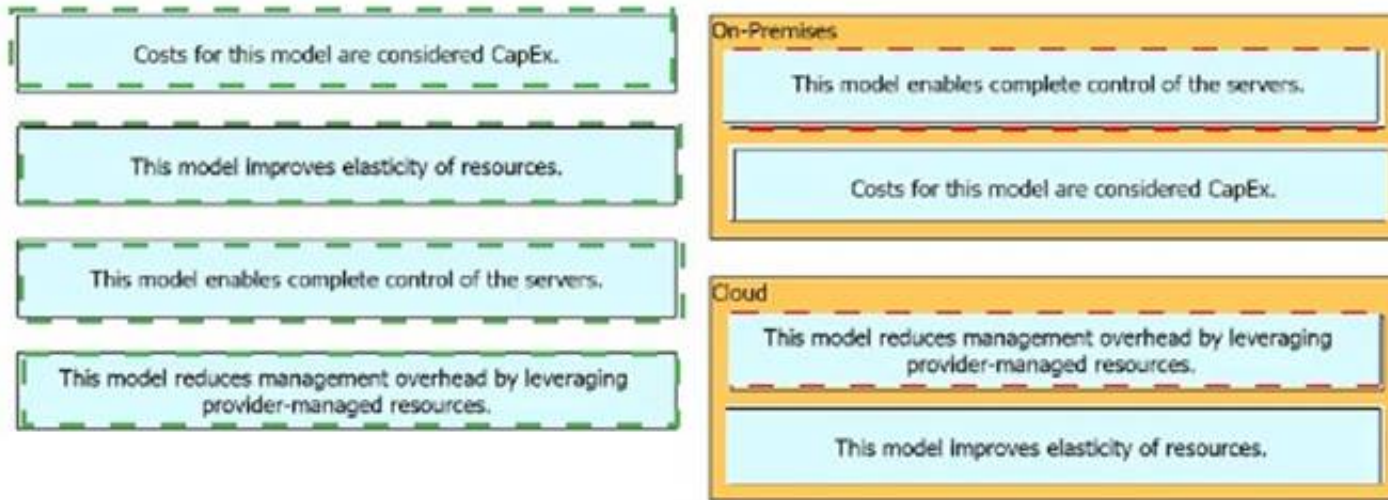
Costs for this model are considered CapEx.	<b>On-Premises</b> <div></div> <div></div>
This model improves elasticity of resources.	
This model enables complete control of the servers.	<b>Cloud</b> <div></div> <div></div>
This model reduces management overhead by leveraging provider-managed resources.	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**





#### NEW QUESTION 246

##### DRAG DROP - (Topic 2)

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

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



- 192.168.1.1
- 192.168.1.2
- 65000
- 65001
- Client
- ISP

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
    <router>
      <ios-bgp:bgp>
        <ios-bgp:id> ISP /ios-bgp:id>
        <ios-bgp:neighbor>
          <ios-bgp:id> 192.168.1.1 </ios-bgp:id>
          <ios-bgp:remote-as> 65001 </ios-bgp:remote-as>
        </ios-bgp:neighbor>
        <ios-bgp:address-family>
          <ios-bgp:no-vrf>
          <ios-bgp:ipv4>
            <ios-bgp:af-name>unicast</ios-bgp:af-name>
            <ios-bgp:ipv4-unicast>
              <ios-bgp:neighbor>
                <ios-bgp:id> 65001 </ios-bgp:id>
                <ios-bgp:soft-reconfiguration>inbound</ios-bgp:soft-reconfiguration>
              </ios-bgp:neighbor>
            </ios-bgp:ipv4-unicast>
          </ios-bgp:ipv4>
        </ios-bgp:address-family>
      </ios-bgp:bgp>
    </router>
  </native>
</config>
```

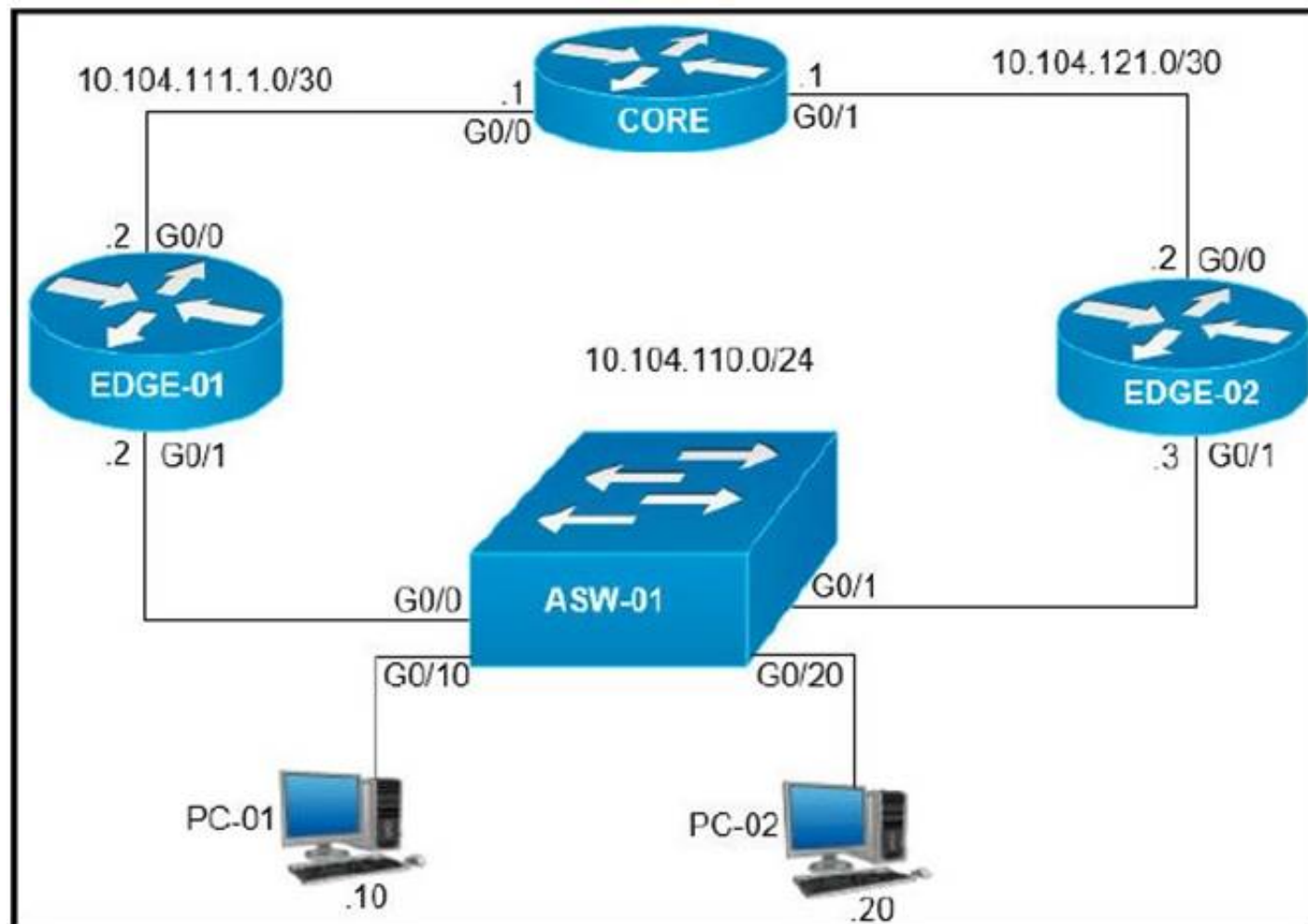


- 192.168.1.1
- 192.168.1.2
- 65000
- 65001
- Client
- ISP

#### NEW QUESTION 247

##### - (Topic 2)

Refer to the exhibit.



On which interfaces should VRRP commands be applied to provide first hop redundancy to PC-01 and PC-02?

- A. G0/0 and G0/1 on Core
- B. G0/0 on Edge-01 and G0/0 on Edge-02
- C. G0/1 on Edge-01 and G0/1 on Edge-02
- D. G0/0 and G0/1 on ASW-01

**Answer: C**

#### NEW QUESTION 251

- (Topic 2)

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

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

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

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

**Answer: C**

#### NEW QUESTION 252

- (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 254

- (Topic 2)

By default, which virtual MAC address does HSRP group 16 use?

- A. c0:41:43:64:13:10
- B. 00:00:0c 07:ac:10
- C. 00:05:5c:07:0c:16
- D. 05:00:0c:07:ac:16

**Answer:** B

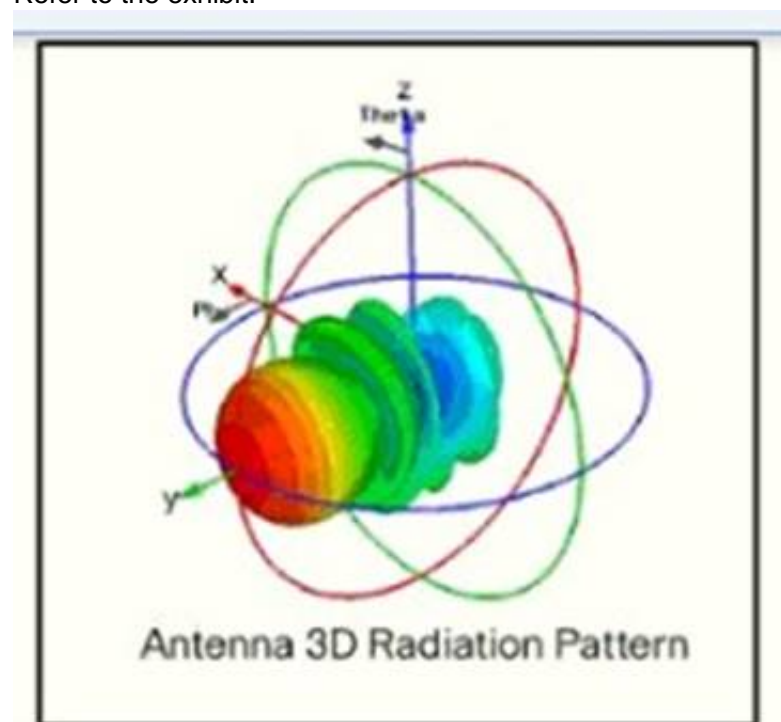
#### Explanation:

The last two-digit hex value in the MAC address presents the HSRP group number. In this case 16 in decimal is 10 in hexadecimal

#### NEW QUESTION 255

- (Topic 2)

Refer to the exhibit.



Which type of antenna does the radiation pattern represent?

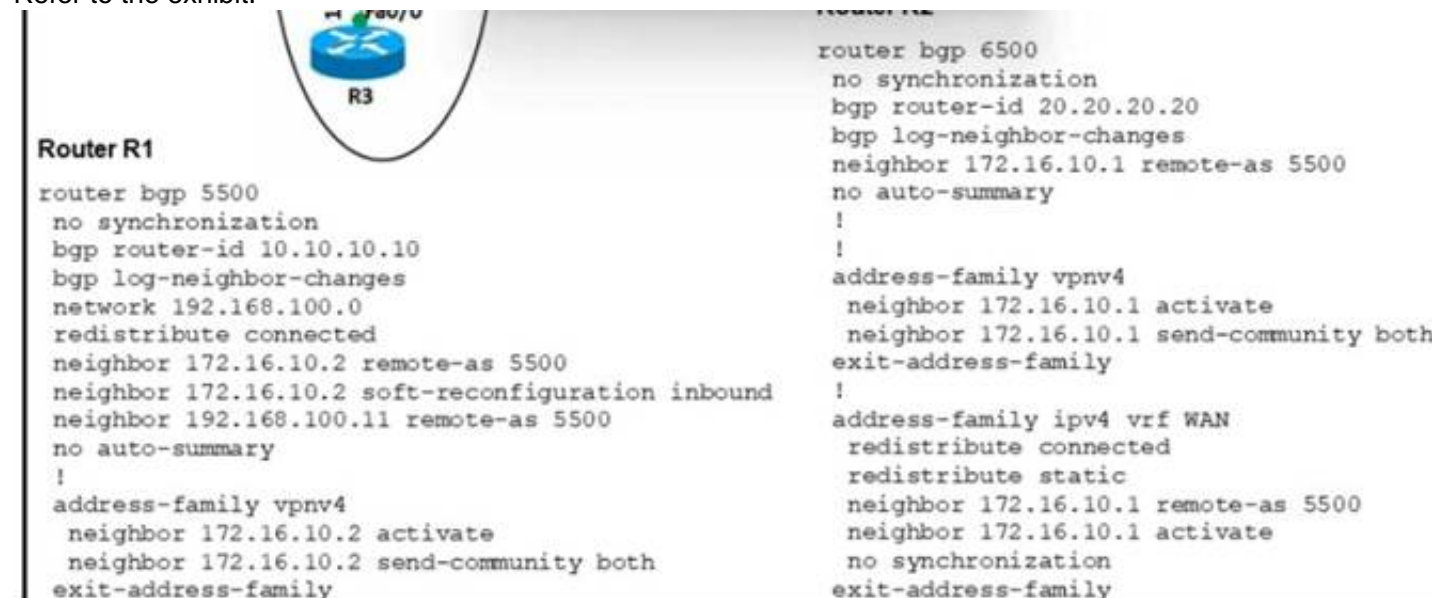
- A. Yagi
- B. multidirectional
- C. directional patch
- D. omnidirectional

**Answer:** A

#### NEW QUESTION 256

- (Topic 2)

Refer to the exhibit.



An engineer configures the BGP adjacency between R1 and R2, however, it fails to establish Which action resolves the issue?

- A. Change the network statement on R1 to 172.16 10.0
- B. Change the remote-as number for 192 168.100.11.
- C. Enable synchronization on R1 and R2



D. Change the remote-as number on R1 to 6500.

Answer: D

NEW QUESTION 260

- (Topic 2)

Refer to the Exhibit.

R1	R2
key chain cisco123 key 1 key-string Cisco123!	key chain cisco123 key 1 key-string cisco123!
Ethernet0/0 - Group 10 State is Active 8 state changes, last state change 00:02:49 Virtual IP address is 192.168.0.1 Active virtual MAC address is 0000.0c07.ac0a Local virtual MAC address is 0000.0c07.ac0a (vl default) Hello time 5 sec, hold time 15 sec Next hello sent in 2.880 secs Authentication MD5, key-chain "cisco123" Preemption enabled Active router is local Standby router is unknown Priority 255 (configured 255) Group name is "workstation-group" (cfgd)	Ethernet0/0 - Group 10 State is Active 17 state changes, last state change 00:02:17 Virtual IP address is 192.168.0.1 Active virtual MAC address is 0000.0c07.ac0a Local virtual MAC address is 0000.0c07.ac0a (vl default) Hello time 10 sec, hold time 30 sec Next hello sent in 6.720 secs Authentication MD5, key-chain "cisco123" Preemption disabled Active router is local Standby router is unknown Priority 200 (configured 200) Group name is "workstation-group" (cfgd)

An engineer is installing a new pair of routers in a redundant configuration. When checking on the standby status of each router the engineer notices that the routers are not functioning as expected. Which action will resolve the configuration error?

- A. configure matching hold and delay timers
- B. configure matching key-strings
- C. configure matching priority values
- D. configure unique virtual IP addresses

Answer: B

Explanation:

From the output exhibit, we notice that the key-string of R1 is Cisco123! (letter C is in capital) while that of R2 is cisco123!. This causes a mismatch in the authentication so we have to fix their key-strings.  
key-string [encryption-type] text-string: Configures the text string for the key. The text- string argument is alphanumeric, case-sensitive, and supports special characters. Reference: [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/security/configuration/guide/b\\_Cisco\\_Nexus\\_9000\\_Series\\_NX-OS\\_Security\\_Configuration\\_Guide/b\\_Cisco\\_Nexus\\_9000\\_Series\\_NX-OS\\_Security\\_Configuration\\_Guide\\_chapter\\_01111.pdf](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/security/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_chapter_01111.pdf)

NEW QUESTION 265

- (Topic 1)

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

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

Answer: B

NEW QUESTION 266

- (Topic 1)

A customer has several small branches and wants to deploy a WI-FI solution with local management using CAPWAP. Which deployment model meets this requirement?

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


Answer: B

NEW QUESTION 268

- (Topic 1)



London



New York

```

London(config)#interface range fa0/1-2
London(config-if-range)#switchp trunk encapsulation dot1q
London(config-if-range)#switchp mode trunk
London(config-if-range)#channel-group 1 mode active
London(config-if-range)#end
London#

NewYork#show etherchannel summary
Flags: D - down        P - 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
       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)        PAgP       Fa0/1(I) Fa0/2(D)
NewYork#
NewYork#show etherchannel port-channel
Channel-group listing:
-----
Group: 1
-----
Port-channels in the group:
-----
Port-channel: Po1
-----
Age of the Port-channel   = 00d:00h:14m:20s
Logical slot/port        = 2/1      Number of ports = 0
GC                        = 0x00000000 HotStandBy port = null
Port state                = Port-channel |
Protocol                  = PAgP
Port Security              = Disabled

```

Refer to the exhibit. Communication between London and New York is down. Which command set must be applied to the NewYork switch to resolve the issue?

A)

```

NewYork(config)#no interface po1
NewYork(config)#interface range fa0/1-2
NewYork(config-if)#channel-group 1 mode negotiate
NewYork(config-if)#end
NewYork#

```

B)

```

NewYork(config)#no interface po1
NewYork(config)#interface range fa0/1-2
NewYork(config-if)#channel-group 1 mode on
NewYork(config-if)#end
NewYork#

```

C)

```

NewYork(config)#no interface po1
NewYork(config)#interface range fa0/1-2
NewYork(config-if)#channel-group 1 mode auto
NewYork(config-if)#end
NewYork#

```

D)

```

NewYork(config)#no interface po1
NewYork(config)#interface range fa0/1-2
NewYork(config-if)#channel-group 1 mode passive
NewYork(config-if)#end
NewYork#

```

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

**Answer:** D

#### NEW QUESTION 272

- (Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 274

- (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 276

- (Topic 1)

Which method of account authentication does OAuth 2.0 within REST APIs?

- A. username/role combination
- B. access tokens
- C. cookie authentication
- D. basic signature workflow

**Answer:** B

#### Explanation:

The most common implementations of OAuth (OAuth 2.0) use one or both of these tokens:

+ access token: sent like an API key, it allows the application to access a user's data; optionally, access tokens can expire.

+ refresh token: optionally part of an OAuth flow, refresh tokens retrieve a new access token if they have expired. OAuth2 combines Authentication and Authorization to allow more sophisticated scope and validity control.

#### NEW QUESTION 281

- (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 285

- (Topic 1)

Which JSON syntax is valid?

A)

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

B)

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

C)

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

D)

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

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

**Answer:** C

**Explanation:**

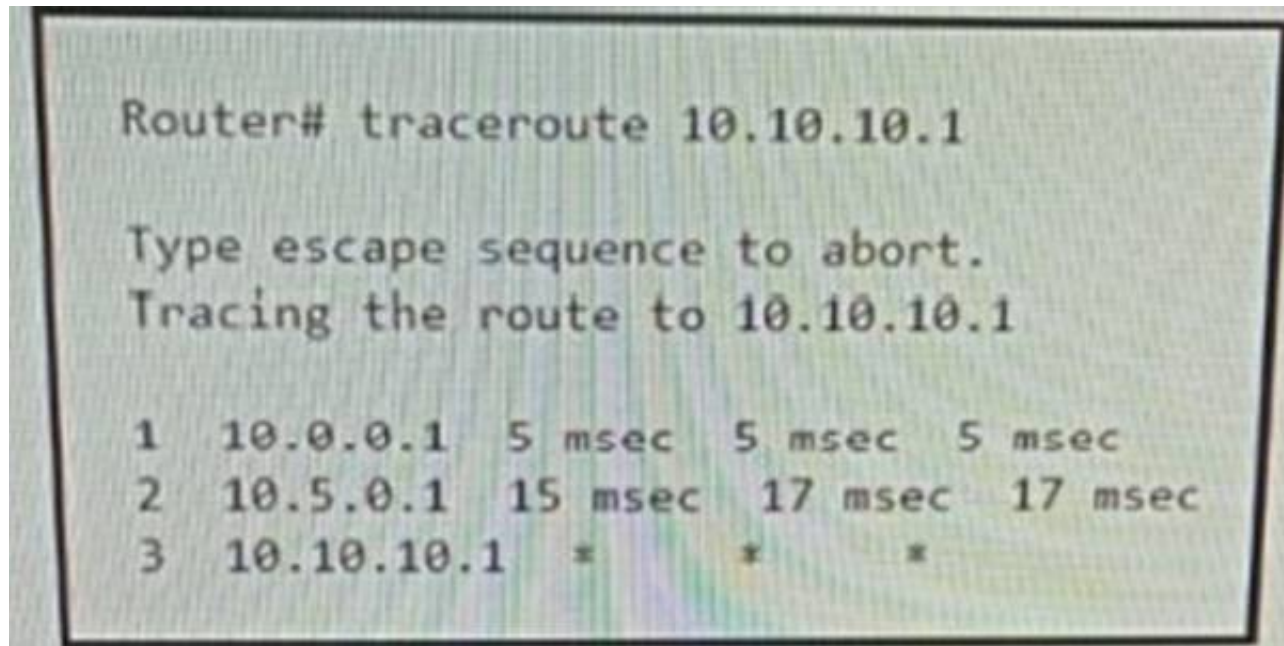
This JSON can be written as follows:

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

**NEW QUESTION 287**

- (Topic 1)

Refer to the exhibit.



An engineer is troubleshooting a connectivity issue and executes a traceoute. What does the result confirm?

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

**Answer:** D

**Explanation:**

In Cisco routers, the codes for a traceroute command reply are:

! — success\* — time outN — network unreachableH — host unreachableP — protocol unreachableA — admin deniedQ — source quench received (congestion)? — unknown (any other ICMP message)

In Cisco routers, the codes for a traceroute command reply are:

! — success\* — time outN — network unreachableH — host unreachableP — protocol unreachableA — admin deniedQ — source quench received (congestion)? — unknown (any other ICMP message)

**NEW QUESTION 288**

- (Topic 1)

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

```
import requests
import sys
import urllib3

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

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

if __name__ == "__main__":
    sys.exit(main())
```

Output

```
$ python get_token.py
<Response [405]>
Call failed! Review get_token ().
```



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

**Answer:** D

**Explanation:**

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Status>

**NEW QUESTION 292**

- (Topic 1)

In a wireless Cisco SD-Access deployment, which roaming method is used when a user moves from one access point to another on a different access switch using a single WLC?

- A. Layer 3
- B. inter-xTR
- C. auto anchor
- D. fast roam

**Answer:** B

**Explanation:**

A fabric edge node provides onboarding and mobility services for wired users and devices (including fabric-enabled WLCs and APs) connected to the fabric. It is a LISP tunnel router (xTR) that also provides the anycast gateway, endpoint authentication, and assignment to overlay host pools (static or DHCP), as well as group-based policy enforcement (for traffic to fabric endpoints).

From Cisco's guide, under SDA roaming - When a client on a fabric enabled WLAN, roams from an access point to another access point on a different access-switch, it is called Inter- xTR, like a highway. Intra is within intra is between. Like interstate highways. That's how I remember. [https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b\\_wl\\_16\\_10\\_cg/mobility.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/mobility.html)

**NEW QUESTION 293**

- (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 294**

- (Topic 1)

Which design principle states that a user has no access by default to any resource, and unless a resource is explicitly granted, it should be denied?

- A. least privilege
- B. fail-safe defaults
- C. economy of mechanism
- D. complete mediation

**Answer:** B

**NEW QUESTION 297**

- (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 299**

- (Topic 1)

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



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

**Answer:** C

**Explanation:**

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

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/vxlan/configuration/guide/b\\_Cisco\\_Nexus\\_9000\\_Series\\_NX-OS\\_VXLAN\\_Configuration\\_Guide\\_7x/b\\_Cisco\\_Nexus\\_9000\\_Series\\_NX-OS\\_VXLAN\\_Configuration\\_Guide\\_7x\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/vxlan/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_7x_chapter_010.html)

**NEW QUESTION 303**

- (Topic 1)

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

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

**Answer:** D

**NEW QUESTION 308**

- (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 309**

- (Topic 1)

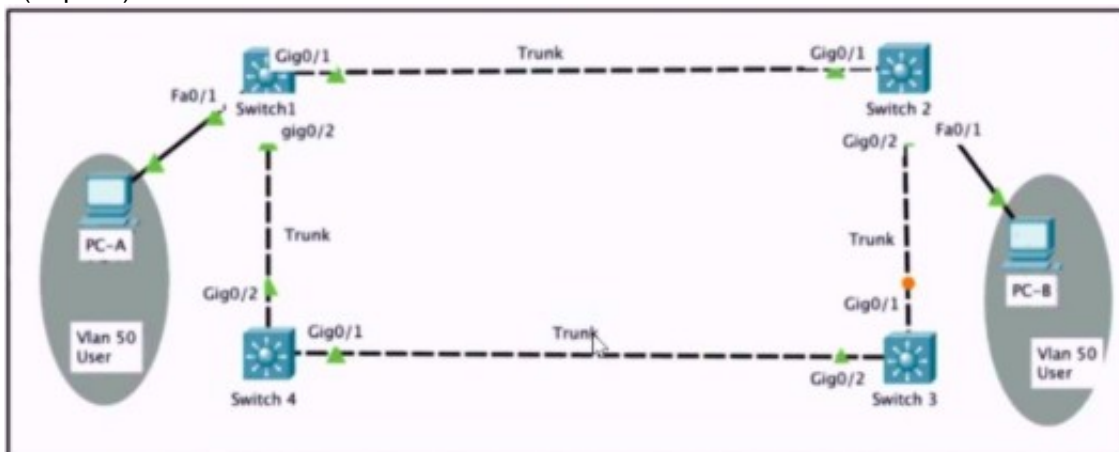
which entity is a Type 1 hypervisor?

- A. Oracle VM VirtualBox
- B. VMware server
- C. Citrix XenServer
- D. Microsoft Virtual PC

**Answer:** C

**NEW QUESTION 312**

- (Topic 1)



Refer to the exhibit. Rapid PVST+ is enabled on all switches. Which command set must be configured on switch1 to achieve the following results on port fa0/1?

- When a device is connected, the port transitions immediately to a forwarding state.
- The interface should not send or receive BPDUs.
- If a BPDU is received, it continues operating normally.

- A)  
Switch1(config)# **interface f0/1**  
Switch1(config-if)# **spanning-tree portfast**
- B)  
Switch1(config)# **spanning-tree portfast bpdufilter default**  
Switch1(config)# **Interface f0/1**  
Switch1(config-if)# **spanning-tree portfast**
- C)  
Switch1(config)# **spanning-tree portfast bpduguard default**  
Switch1(config)# **interface f0/1**  
Switch1(config-if)# **spanning-tree portfast**
- D)  
Switch1(config)# **interface f0/1**  
Switch1(config-if)# **spanning-tree portfast**  
Switch1(config-if)# **spanning-tree bpduguard enable**

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

Answer: D

NEW QUESTION 313

DRAG DROP - (Topic 1)

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

supports unequal path load balancing

link state routing protocol

distance vector routing protocol

metric is based on delay and bandwidth by default

makes it easy to segment the network logically

constructs three tables as part of its operation: neighbor table, topology table, and routing table

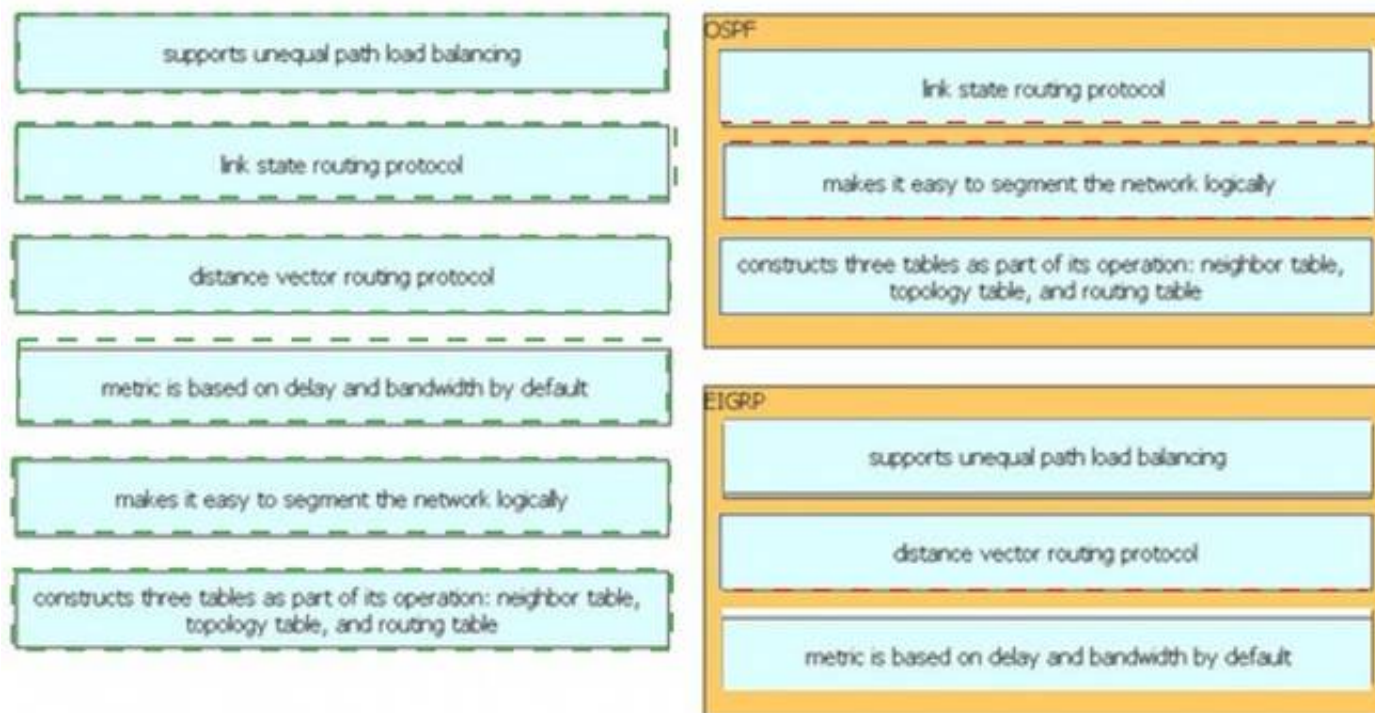
OSPF

EIGRP

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:



### NEW QUESTION 317

- (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 net-work redesign.

### NEW QUESTION 318

- (Topic 1)

When a wireless client roams between two different wireless controllers, a network connectivity outage is experience 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 319

DRAG DROP - (Topic 1)

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

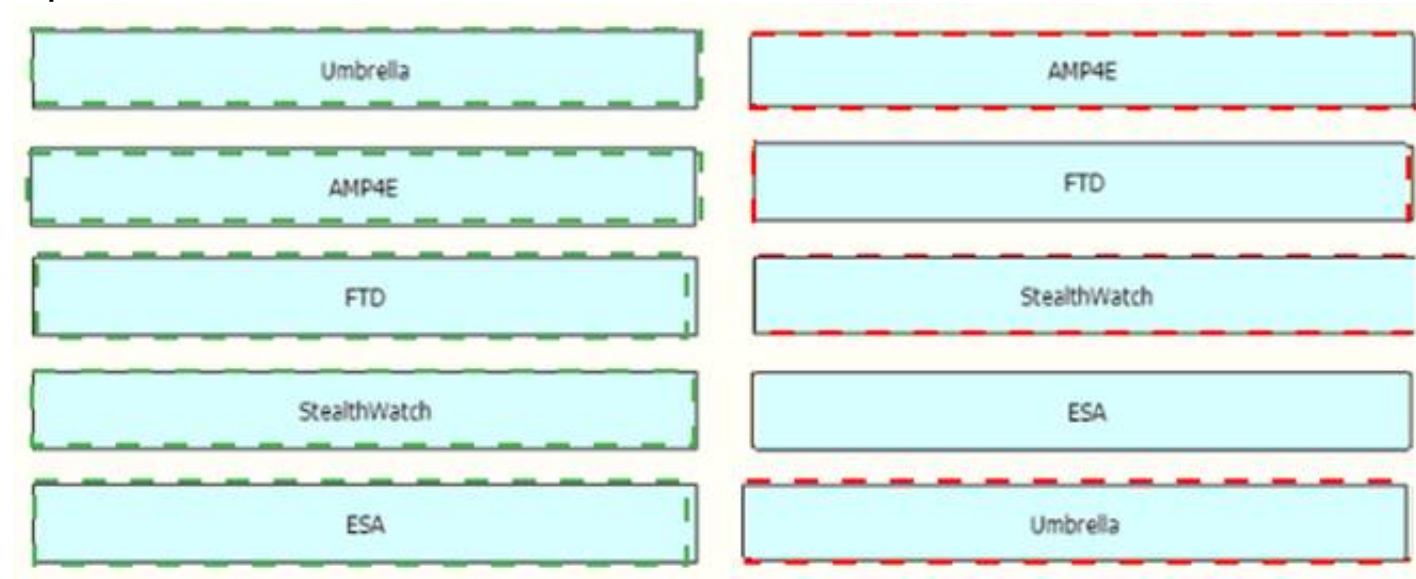


- A. Mastered
- B. Not Mastered

**Answer: A**



**Explanation:**



**NEW QUESTION 322**

- (Topic 1)

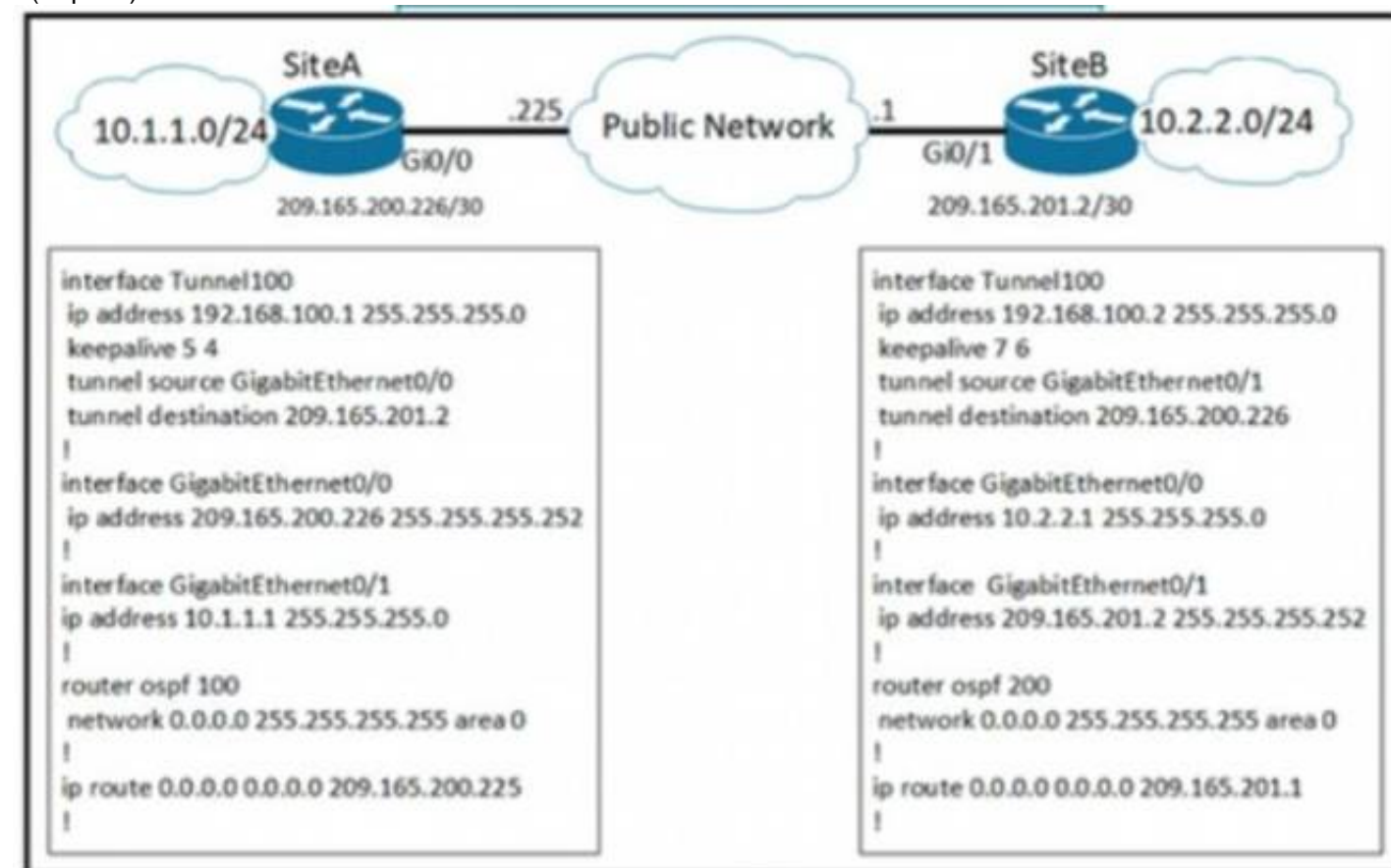
How does EIGRP differ from OSPF?

- A. EIGRP is more prone to routing loops than OSPF
- B. EIGRP supports equal or unequal path cost, and OSPF supports only equal path cost.
- C. EIGRP has a full map of the topology, and OSPF only knows directly connected neighbors
- D. EIGRP uses more CPU and memory than OSPF

**Answer:** B

**NEW QUESTION 327**

- (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 332**

- (Topic 1)

Refer to the exhibit.

```
Router#sh run | b vty
line vty 0 4
  session-timeout 30
  exec-timeout 120 0
  session-limit 30
  login local
line vty 5 15
  session-timeout 30
  exec-timeout 30 0
  session-limit 30
  login local
```

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

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

**Answer: C**

#### NEW QUESTION 333

- (Topic 1)

Which action is the vSmart controller responsible for in an SD-WAN deployment?

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

**Answer: B**

#### NEW QUESTION 337

- (Topic 1)

Which outbound access list, applied to the WAN interface of a router, permits all traffic except for http traffic sourced from the workstation with IP address 10.10.10.1?

A)

```
ip access-list extended 100
deny tcp host 10.10.10.1 any eq 80
permit ip any any
```

B)

```
ip access-list extended 200
deny tcp host 10.10.10.1 eq 80 any
permit ip any any
```

C)

```
ip access-list extended NO_HTTP
deny tcp host 10.10.10.1 any eq 80
```

D)

```
ip access-list extended 10
deny tcp host 10.10.10.1 any eq 80
permit ip any any
```

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

Answer: A

#### NEW QUESTION 338

- (Topic 1)

Refer to the exhibit.

```
PYTHON CODE:
import requests
import json

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

myheaders={'content-type':'application/json'}
payload={
  "ins_api": {
    "version": "1.0",
    "type": "cli_show",
    "chunk": "0",
    "sid": "1",
    "input": "show version",
    "output_format": "json"
  }
}
response = requests.post(url,data=json.dumps(payload), headers=myheaders,auth=(switchuser,switchpassword)) json()
print(response[ins_api][outputs][output][body][kickstart_ver_str])

HTTP JSON Response:
{
  "ins_api": {
    "type": "cli_show",
    "version": "1.0",
    "sid": "eoc",
    "outputs": {
      "output": {
        "input": "show version",
        "msg": "Success",
        "code": "200",
        "body": {
          "bios_ver_str": "07.61",
          "kickstart_ver_str": "7.0(3)I7(4)",
          "bios_cmpl_time": "04/06/2017",
          "kick_file_name": "bootflash:/nxos.7.0.3.i7.4.bin",
          "kick_cmpl_time": "6/14/1970 2:00:00",
          "kick_tmstamp": "06/14/1970 09:49:04",
          "chassis_id": "Nexus6000 93180YC-EX chassis",
          "cpu_name": "Intel(R) Xeon(R) CPU @ 1.80GHz",
          "memory": 24633488,
          "mem_type": "kB",
          "n_uscs": 134703,
          "n_ctime": "Sun Mar 10 15:41:46 2019",
          "rr_reason": "Reset Requested by CLI command reload",
          "rr_sys_ver": "7.0(3)I7(4)",
          "rr_service": "-",
          "manufacturer": "Cisco Systems, Inc.",
          "TABLE_package_inf": {
            "ROW_package_inf": {
              "package_id": 0
            }
          }
        }
      }
    }
  }
}
```

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 340

- (Topic 1)

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

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

Answer: AB

#### NEW QUESTION 343

- (Topic 1)

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

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

Answer: BE

#### NEW QUESTION 345

- (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 348

- (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 353**

DRAG DROP - (Topic 1)

Drag and drop the characteristics from the left onto the protocols they apply to on the right?

uses Dijkstra's Shortest Path First algorithm	OSPF
uses Diffused Update Algorithm	
uses bandwidth, delay, reliability, and load for routing metric	EIGRP
uses an election process	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

uses Dijkstra's Shortest Path First algorithm	OSPF
uses an election process	
uses Diffused Update Algorithm	EIGRP
uses bandwidth, delay, reliability, and load for routing metric	

**NEW QUESTION 358**

- (Topic 1)

When is an external antenna used inside a building?

- A. only when using Mobility Express
- B. when it provides the required coverage
- C. only when using 2.4 GHz
- D. only when using 5 GHz

**Answer:** B

**NEW QUESTION 361**

- (Topic 1)

Which HTTP code must be returned to prevent the script from exiting?

```
def get_token () :
    device_uri = "https://192.168.1.1/dna/system/api/v1/auth/token"
    http_result = requests.post(device_uri, auth = ("test", "test3988104361"))
    if http_result.status_code != requests.codes.ok:
        print ("Call failed! Review get_token () . ")
        sys.exit ()
    return (http_result.json () ["Token"])
```

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

Answer: A

NEW QUESTION 363

- (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 367

DRAG DROP - (Topic 1)  
Drag and drop the characteristics from the left onto the appropriate infrastructure deployment types on the right.

customizable hardware, purpose-built systems

easy to scale and upgrade

more suitable for companies with specific regulatory or security requirements

resources can be over or underutilized as requirements vary

requires a strong and stable internet connection

built-in, automated data backups and recovery

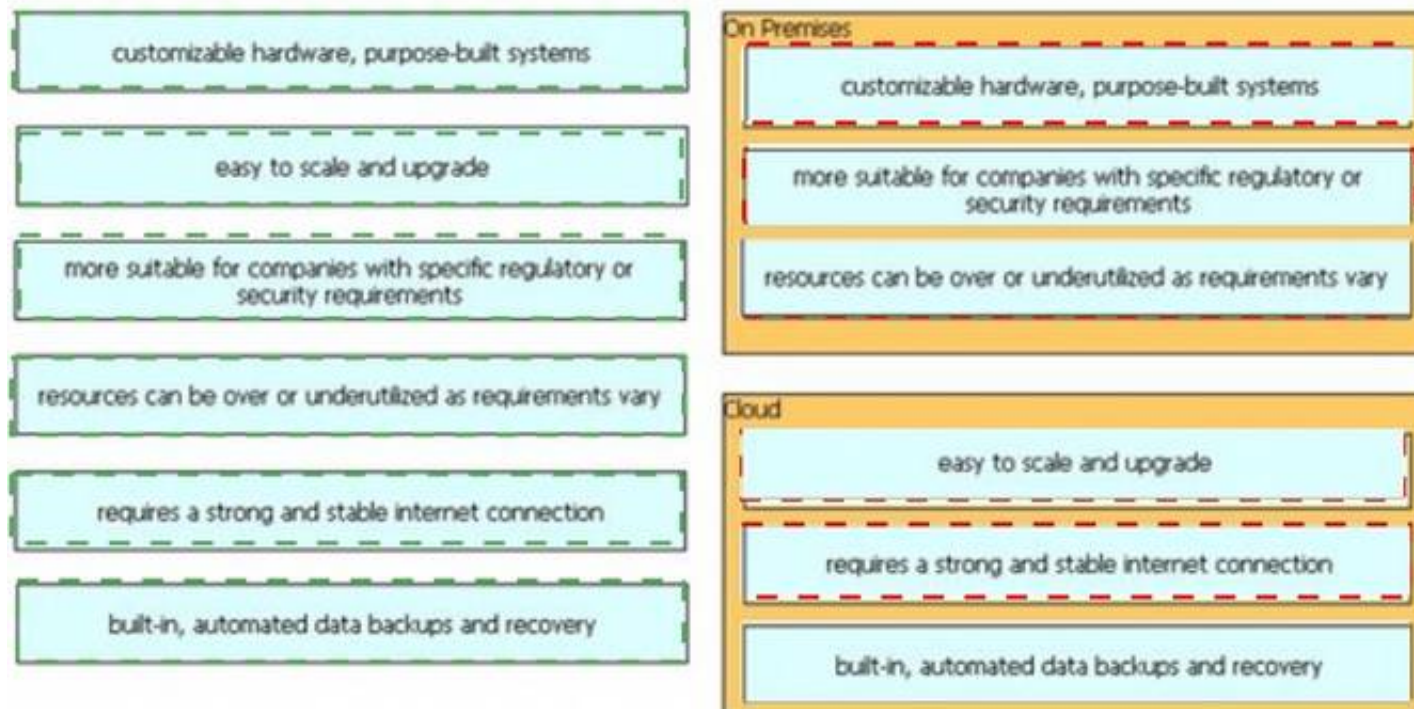
On Premises

Cloud

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



### NEW QUESTION 368

- (Topic 1)

Refer to the exhibit.

```

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

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

Which action resolves the EtherChannel issue between SW2 and SW3?

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

**Answer: D**

### NEW QUESTION 370

- (Topic 1)

What is the purpose of the LISP routing and addressing architecture?

- A. It creates two entries for each network node, one for its identity and another for its location on the network.
- B. It allows LISP to be applied as a network visualization overlay though encapsulation.
- C. It allows multiple Instances of a routing table to co-exist within the same router.
- D. It creates head-end replication used to deliver broadcast and multicast frames to the entire network.

**Answer: A**

### NEW QUESTION 375

- (Topic 1)



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

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

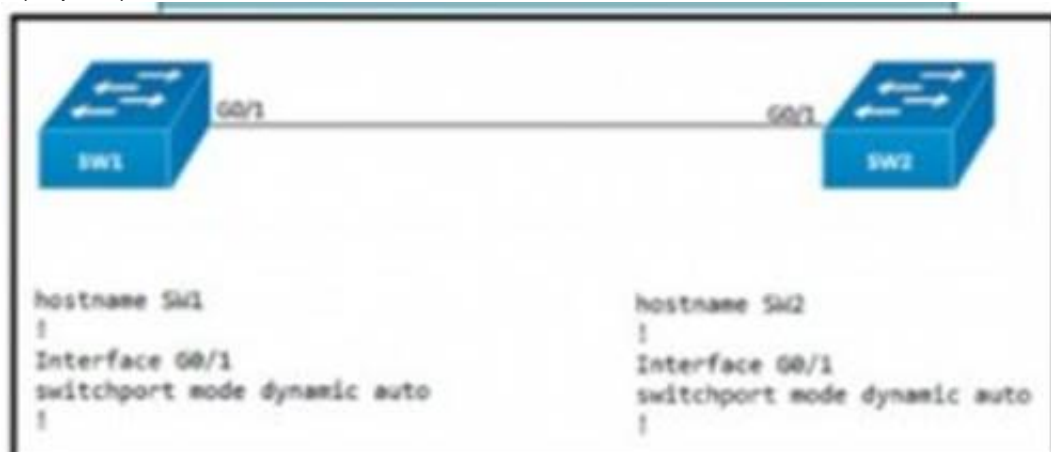
**Answer: C**

**Explanation:**

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

**NEW QUESTION 378**

- (Topic 1)



Refer to the exhibit. An engineer attempts to configure a trunk between switch sw1 and switch SW2 using DTP, but the trunk does not form. Which command should the engineer apply to switch SW2 to resolve this issue?

- A. switchport mode dynamic desirable
- B. switchport nonegotiate
- C. no switchport
- D. switchport mode access

**Answer: A**

**NEW QUESTION 381**

- (Topic 1)

Refer to the exhibit.

```

ip sla 10

icmp-echo 192.168.10.20

timeout 500

frequency 3

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

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

- A. event manager applet EEM\_IP\_SLA event track 10 state down
- B. event manager applet EEM\_IP\_SLA event track 10 state unreachable
- C. event manager applet EEM\_IP\_SLA event sla 10 state unreachable
- D. event manager applet EEM\_IP\_SLA event sla 10 state down

**Answer: A**

**Explanation:**

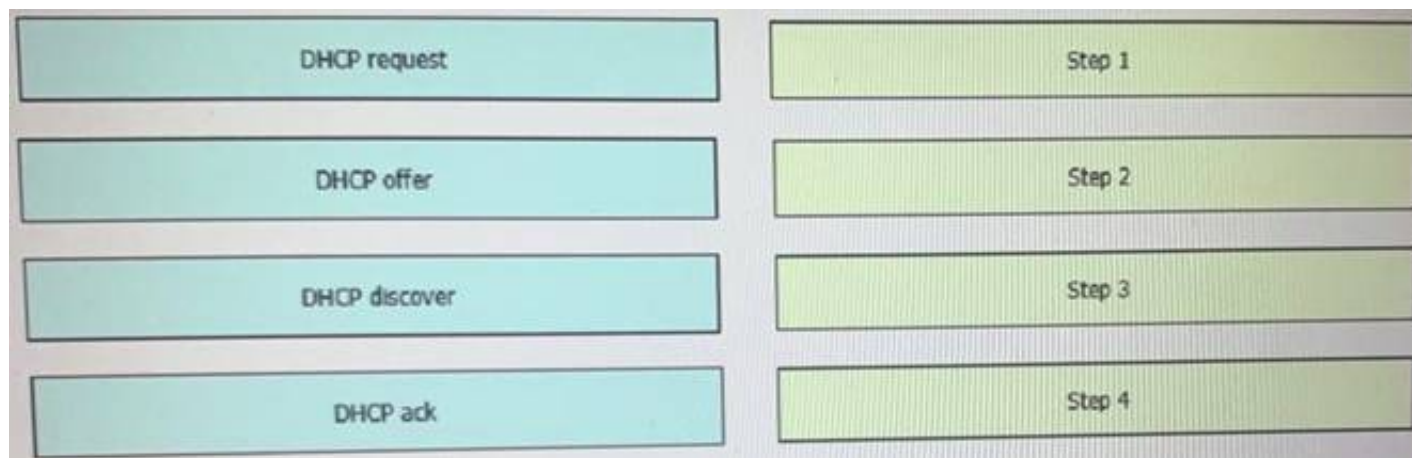
The ip sla 10 will ping the IP 192.168.10.20 every 3 seconds to make sure the connection is still up. We can configure an EEM applet if there is any problem with this IP SLA via the command event track 10 state down.

Reference: <https://www.theroutingtable.com/ip-sla-and-cisco-eem/>

**NEW QUESTION 383**

DRAG DROP - (Topic 1)

Drag and drop the DHCP messages that are exchanged between a client and an AP into the order they are exchanged on the right.



- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

There are four messages sent between the DHCP Client and DHCP Server: DHCPD ISCOVER, DHCPOFFER, DHCPrequest and DHCPACKNOWLEDGEMENT.

This process is often abbreviated as DORA (for Discover, Offer, Request, Acknowledgement).

**NEW QUESTION 386**

- (Topic 1)

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

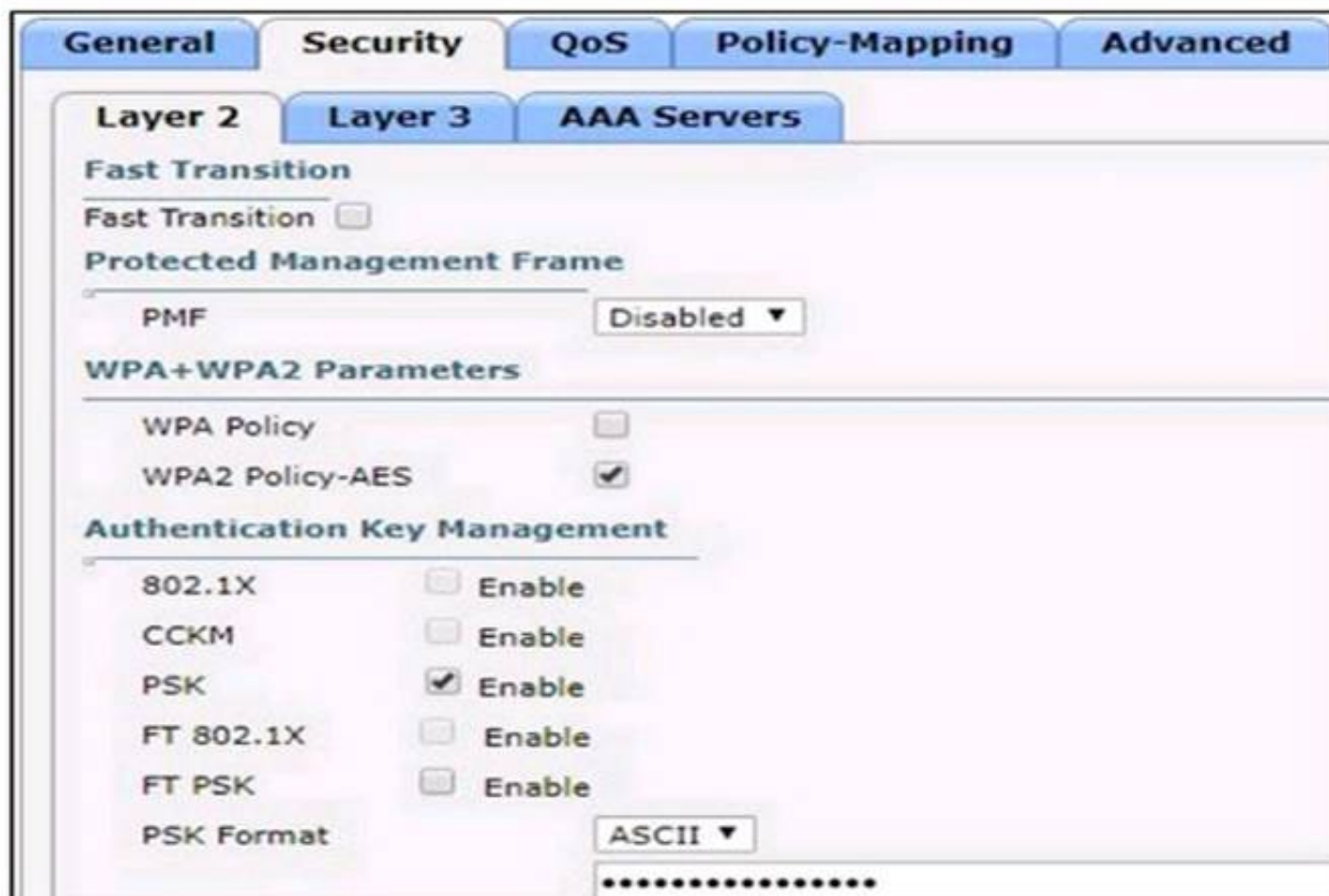
- A. The FIB is derived from the data plane, and the RIB is derived from the FIB.  
B. The RIB is a database of routing prefixes, and the FIB is the Information used to choose the egress interface for each packet.  
C. FIB is a database of routing prefixes, and the RIB is the information used to choose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

**Answer:** BE

**NEW QUESTION 389**

- (Topic 1)

Refer to the exhibit.



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

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

**Answer:** A

**NEW QUESTION 394**

- (Topic 1)

What is the function of the LISP map resolver?

- A. to send traffic to non-LISP sites when connected to a service provider that does not accept nonroutable EIDs as packet sources
- B. to connect a site to the LISP-capable part of a core network publish the EID-to-RLOC mappings for the site, and respond to map-request messages
- C. to decapsulate map-request messages from ITRs and forward the messages to the MS.
- D. to advertise routable non-LISP traffic from one address family to LISP sites in a different address family

**Answer: C**

**Explanation:**

Map resolver (MR): The MR performs the following functions: Receives MAP requests, which are encapsulated by ITRs. Provides a service interface to the ALT router, de-encapsulates MAP requests, and forwards on the ALT topology.

**NEW QUESTION 397**

- (Topic 1)

What are two benefits of virtual switching when compared to hardware switching? (Choose two.)

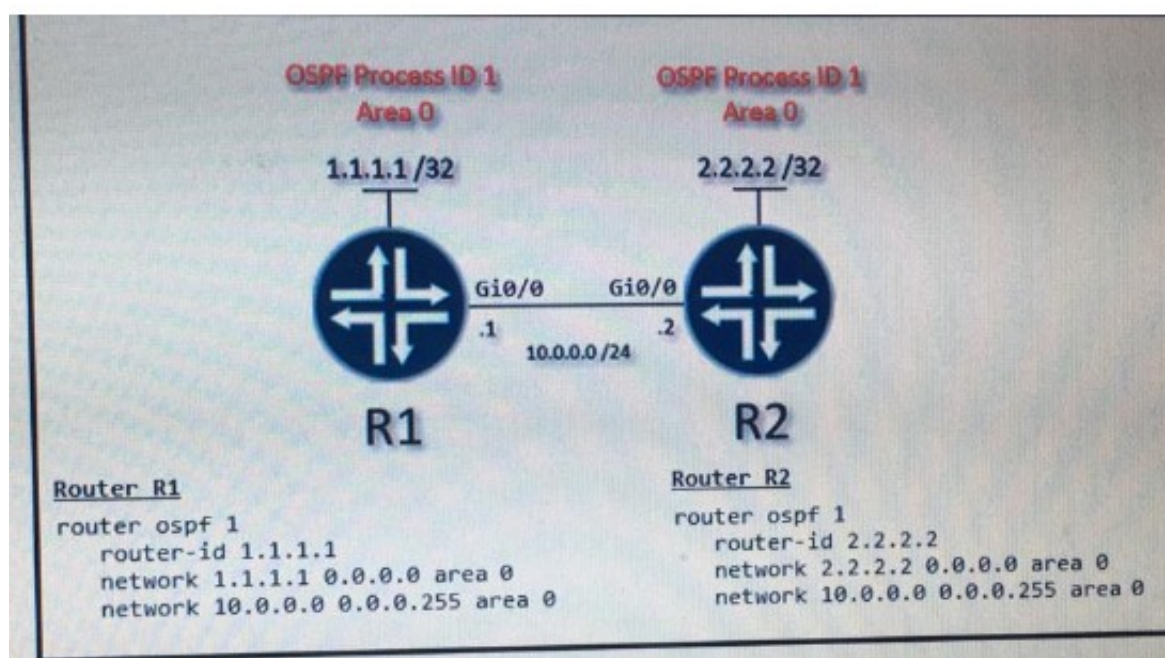
- A. increased MTU size
- B. hardware independence
- C. VM-level isolation
- D. increased flexibility
- E. extended 802.1Q VLAN range

**Answer: CD**

**NEW QUESTION 398**

- (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)

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

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

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

**Answer:** A

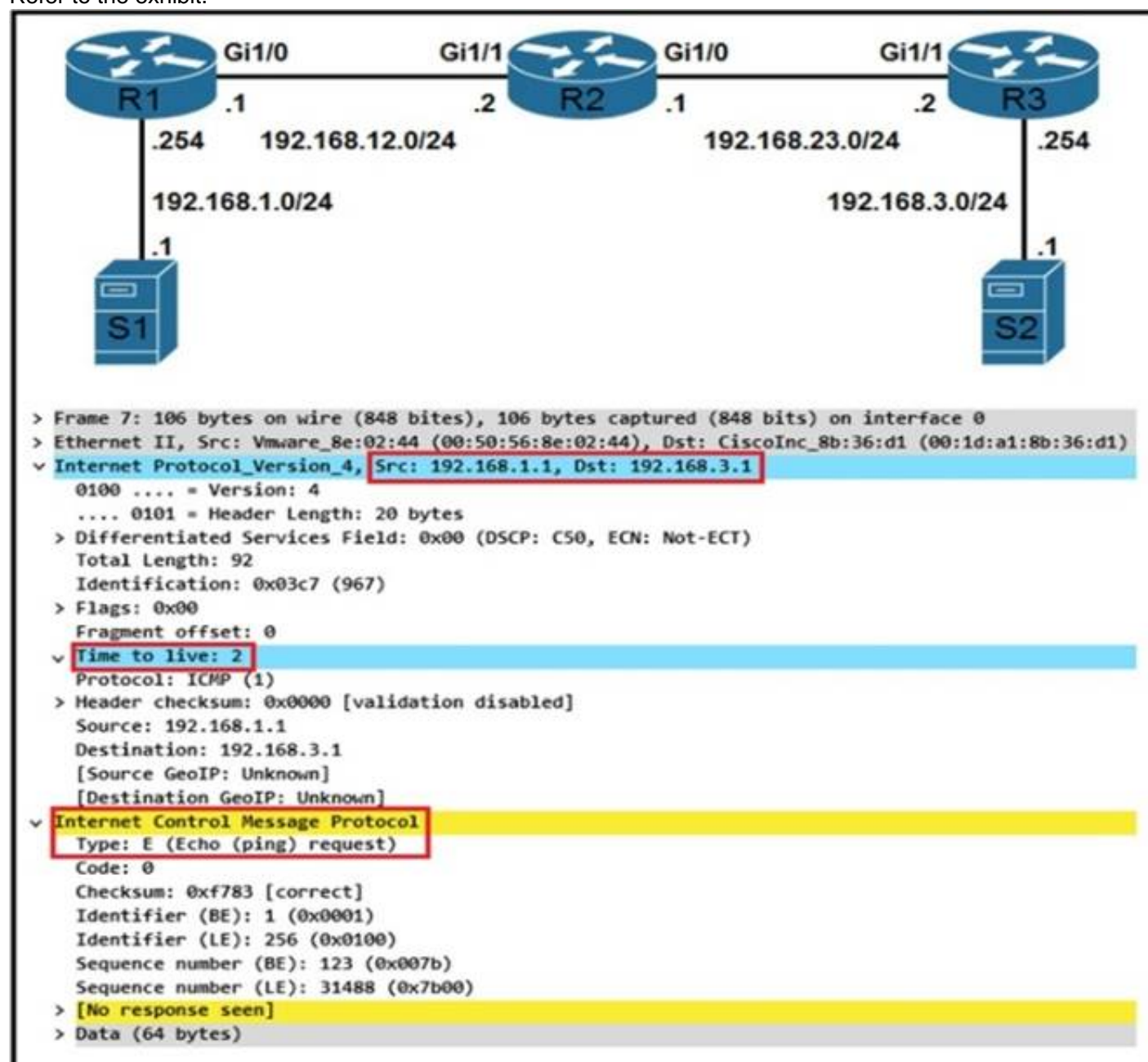
**Explanation:**

Broadcast and Non-Broadcast networks elect DR/BDR while Point-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 401**

- (Topic 1)

Refer to the exhibit.



Which troubleshooting a routing issue, an engineer issues a ping from S1 to S2. When two actions from the initial value of the TTL? (Choose two.)

- A. The packet reaches R3, and the TTL expires
- B. R2 replies with a TTL exceeded message
- C. R3 replies with a TTL exceeded message.

- D. The packet reaches R2 and the TTL expires
- E. R1 replies with a TTL exceeded message
- F. The packet reaches R1 and the TTL expires.

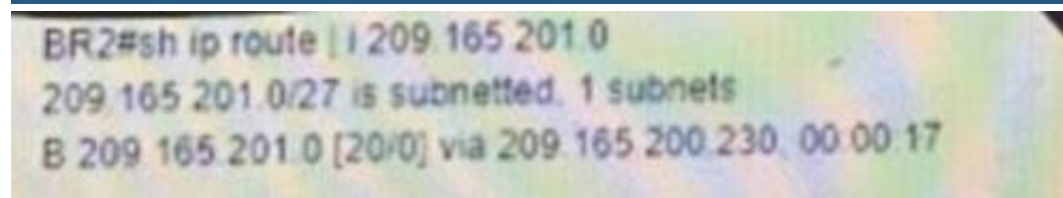
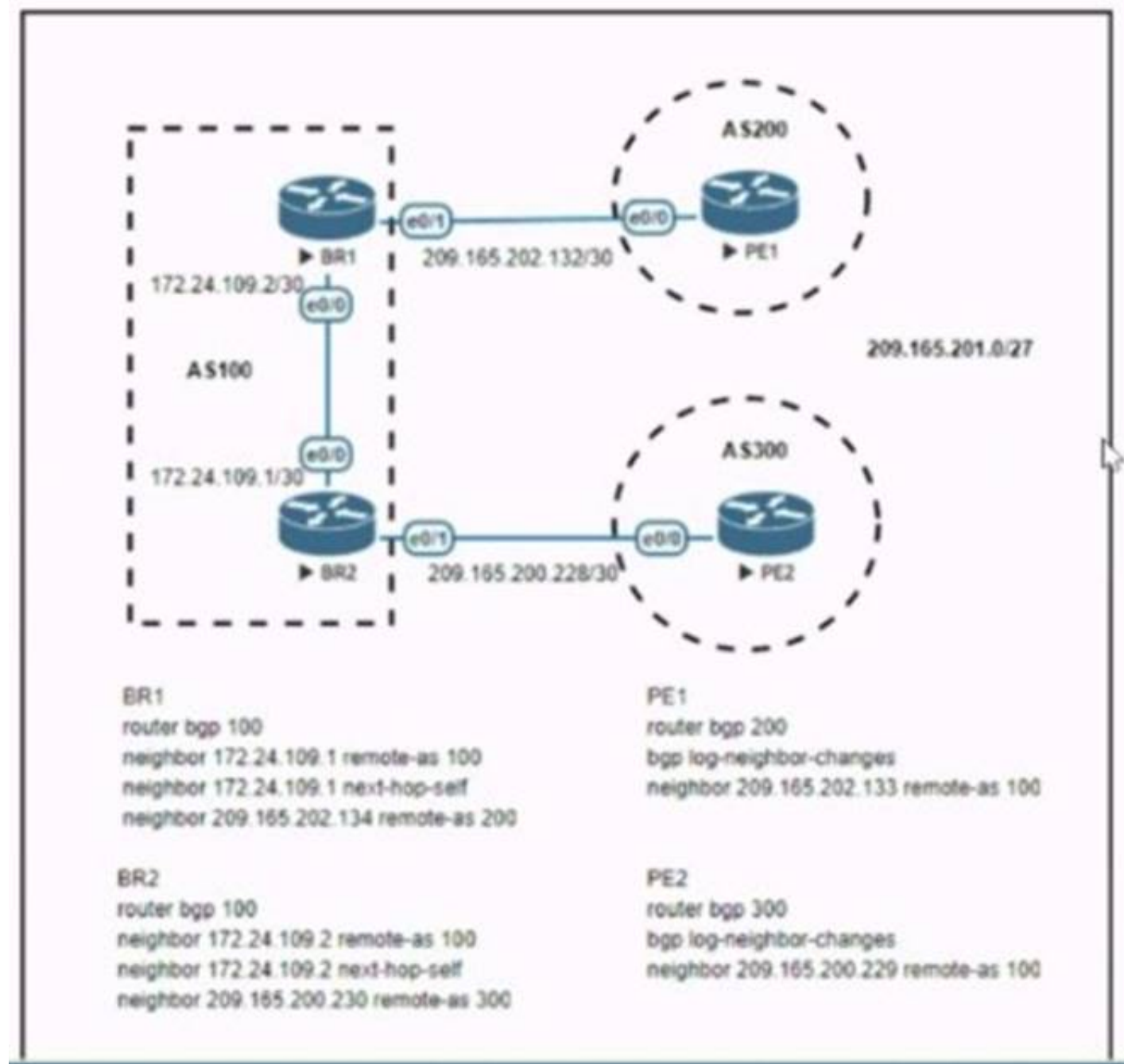
**Answer:** AD

**Explanation:**

Source MAC in the capture is VMWare, MAC is Cisco. Routers first check the TTL before any further process, subtract 1 at R1. Send to R2, subtract and you have ZERO. Discard packet and reply with ICMP Time Exceeded message from that point, don't even bother checking the Route table for further processing.

**NEW QUESTION 406**

- (Topic 1)



Refer to the exhibit. Which configuration change will force BR2 to reach 209 165 201 0/27 via BR1?

- A. Set the weight attribute to 65.535 on BR1 toward PE1.
- B. Set the local preference to 150 on PE1 toward BR1 outbound
- C. Set the MED to 1 on PE2 toward BR2 outbound.
- D. Set the origin to igp on BR2 toward PE2 inbound.

**Answer:** C

**Explanation:**

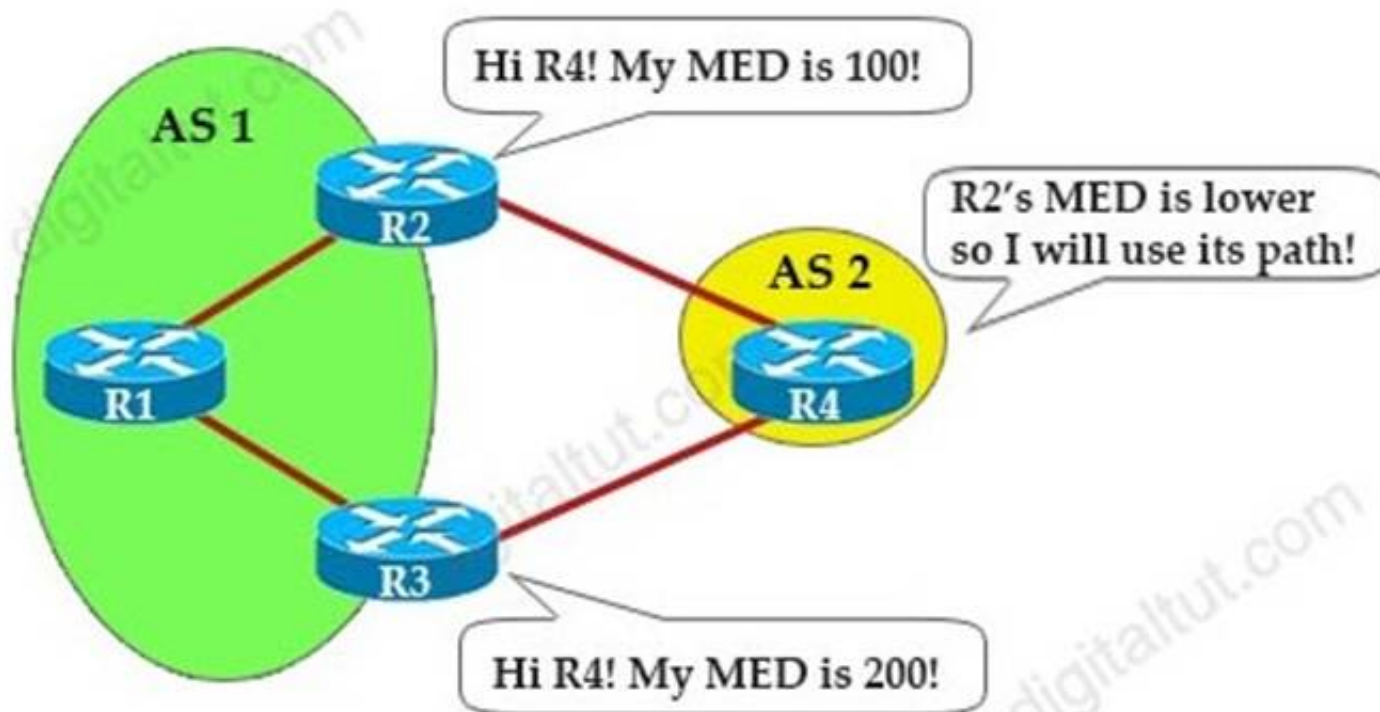


Diagrama Descripción generada automáticamente  
**MED Attribute:**  
 + Optional nontransitive attribute  
 (nontransitive means that we can only advertise MED to routers that are one AS away)  
 + Sent through ASes to external BGP neighbors  
 + Lower value is preferred  
 (it can be considered the external metric of a route)  
 + Default value is 0

#### NEW QUESTION 409

- (Topic 1)

Refer to the exhibit.

```
aaa new-model
aaa authentication login default local-case enable
aaa authentication login ADMIN local-case
username CCNP secret Str0ngP@ssw0rd!
line 0 4
  login authentication ADMIN
```

An engineer must create a configuration that executes the show run command and then terminates the session when user CCNP logs in. Which configuration change is required?

- A. Add the access-class keyword to the username command
- B. Add the access-class keyword to the aaa authentication command
- C. Add the autocommand keyword to the username command
- D. Add the autocommand keyword to the aaa authentication command

**Answer: C**

#### Explanation:

The autocommand causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and can contain embedded spaces, commands using the autocommand keyword must be the last option on the line. In this specific question, we have to enter this line username CCNP autocommand show running-config.

#### NEW QUESTION 412

- (Topic 1)

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

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

**Answer: A**

#### NEW QUESTION 414

- (Topic 1)

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

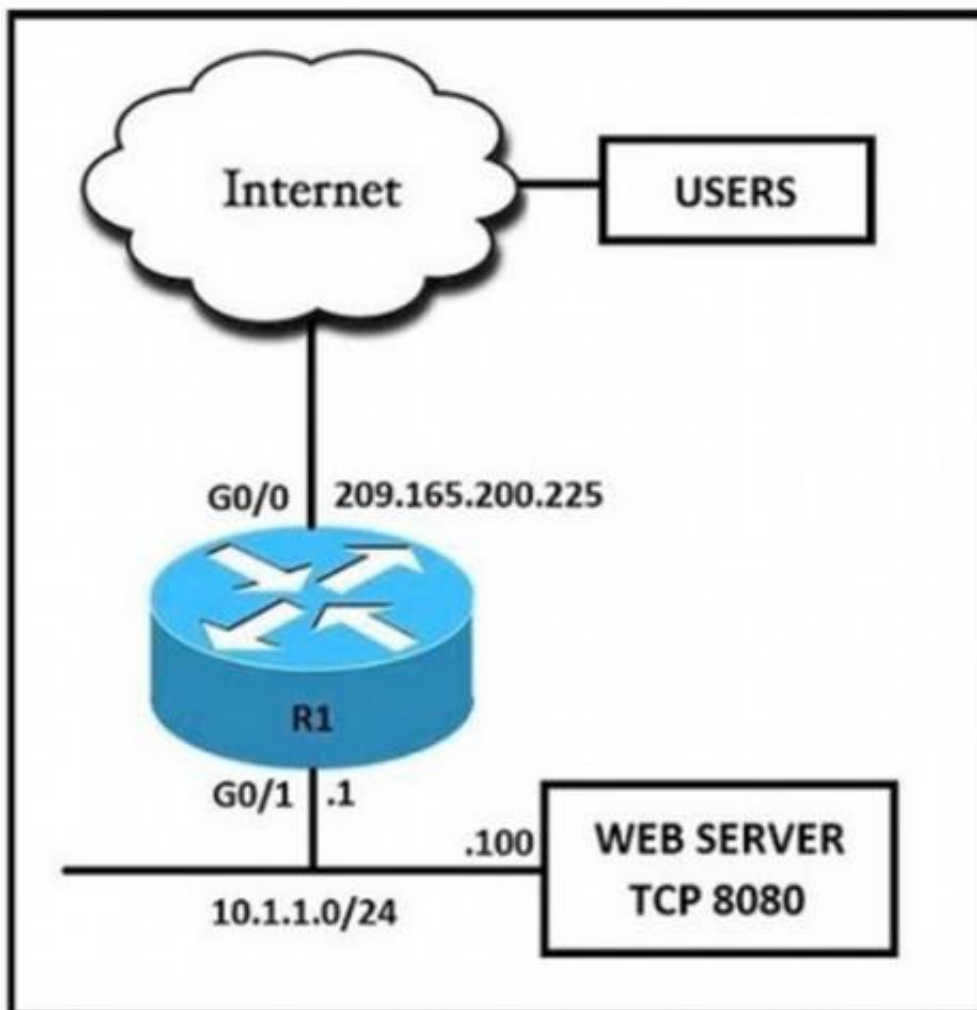
- A. The access point is part of the fabric underlay
- B. The WLC is part of the fabric underlay
- C. The access point is part the fabric overlay
- D. The wireless client is part of the fabric overlay

**Answer: C**

#### NEW QUESTION 417



- (Topic 1)



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

A)

```

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

```

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

```

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

B)

```

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

```

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

```

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

C)

```

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

D)

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

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

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

**Answer:** B

#### NEW QUESTION 421

- (Topic 1)

Refer to the exhibit.

```
Extended IP access list EGRESS
10 permit ip 10.0.0.0 0.0.0.255 any
|
<Output Omitted>
|
interface GigabitEthernet0/0
ip address 209.165.200.225 255.255.255.0
ip access-group EGRESS out
duplex auto
speed auto
media-type rj45
|
```

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

- A. Access control lists that are applied outbound to a router interface do not affect traffic that is sourced from the router.
- B. Only standard access control lists can block traffic from a source IP address.
- C. After an access control list is applied to an interface, that interface must be shut and no shut for the access control list to take effect.
- D. The access control list must contain an explicit deny to block traffic from the router.

**Answer:** A

#### NEW QUESTION 424

- (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 428

- (Topic 1)

How does an on-premises infrastructure compare to a cloud infrastructure?

- A. On-premises can increase compute power faster than cloud
- B. On-premises requires less power and cooling resources than cloud
- C. On-premises offers faster deployment than cloud
- D. On-premises offers lower latency for physically adjacent systems than cloud.

**Answer:** D

#### NEW QUESTION 429

- (Topic 1)

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

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

**Answer:** D

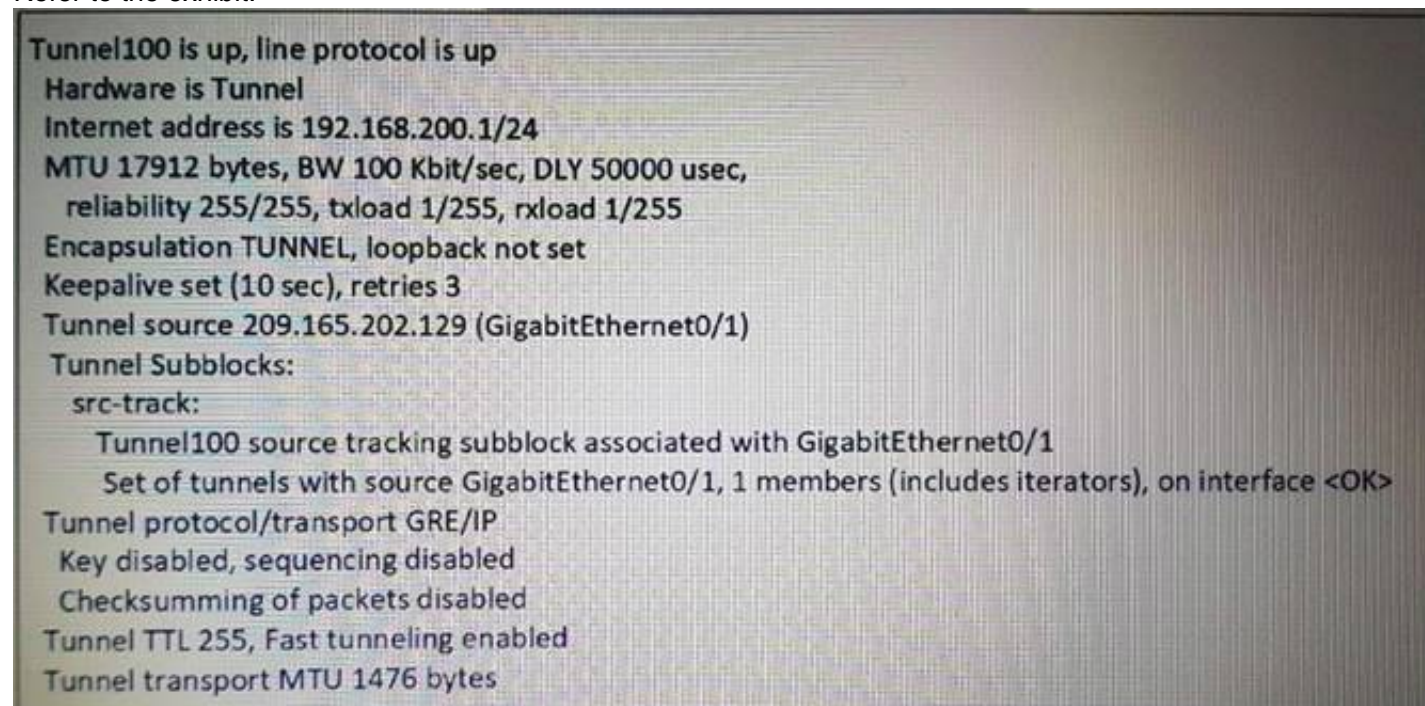
#### Explanation:

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

#### NEW QUESTION 431

- (Topic 1)

Refer to the exhibit.



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

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

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

**Answer:** C

#### NEW QUESTION 435

- (Topic 1)

A customer has recently implemented a new wireless infrastructure using WLC-5520 at a site directly next to a large commercial airport. Users report that they intermittently lose Wi-Fi connectivity, and troubleshooting reveals it is due to frequent channel changes. Which two actions fix this issue? (Choose two)

- A. Remove UNII-2 and Extended UNII-2 channels from the 5 Ghz channel list
- B. Restore the DCA default settings because this automatically avoids channel interference.
- C. Configure channels on the UNII-2 and the Extended UNII-2 sub-bands of the 5 Ghz band only
- D. Enable DFS channels because they are immune to radar interference.
- E. Disable DFS channels to prevent interference with Doppler radar

**Answer:** AE

#### NEW QUESTION 440

- (Topic 1)

What is the output of this code?



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

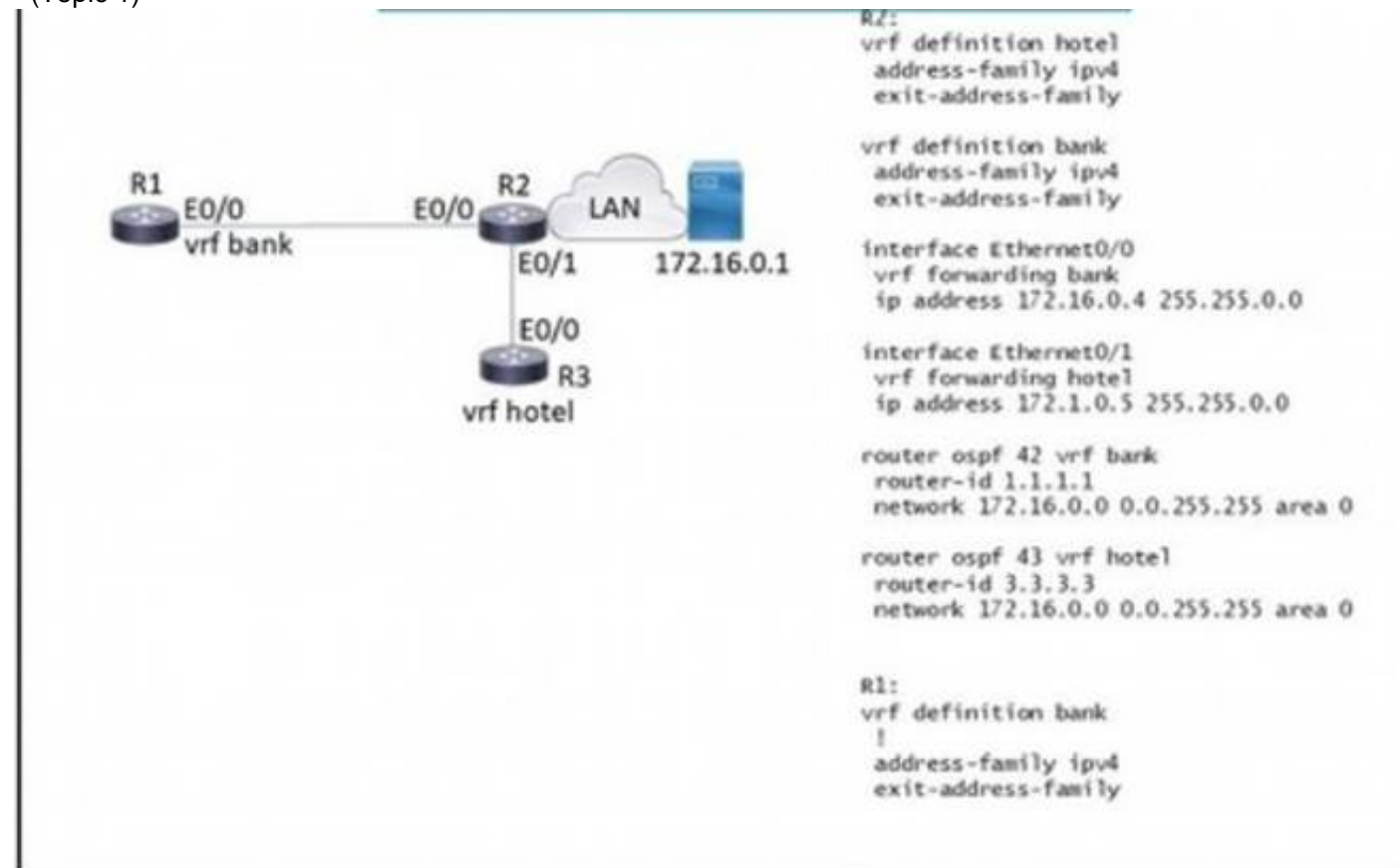
print(get_credentials())
```

- A. username Cisco
- B. get\_credentials
- C. username
- D. CISCO

Answer: D

#### NEW QUESTION 444

- (Topic 1)



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

A)

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

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

B)

```
interface Ethernet0/0
ip address 172.16.0.7 255.255.0.0

router ospf 44 vrf hotel
network 172.16.0.0 255.255.0.0
```

C)

```
interface Ethernet0/0
ip address 172.16.0.7 255.255.0.0

router ospf 44 vrf bank
network 172.16.0.0 255.255.0.0
```

D)

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

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

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

**Answer:** D

#### NEW QUESTION 449

- (Topic 1)

Which encryption hashing algorithm does NTP use for authentication?

- A. SSL
- B. MD5
- C. AES128
- D. AES256

**Answer:** B

#### Explanation:

An example of configuring NTP authentication is shown below: Router1(config)#ntp authentication-key 2 md5 itexamanswersRouter1(config)#ntp authenticateRouter1(config)#ntp trusted-key 2

#### NEW QUESTION 453

- (Topic 1)

A customer requests a network design that supports these requirements:

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

Which protocol does the design include?

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

**Answer:** D

#### NEW QUESTION 455

- (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:

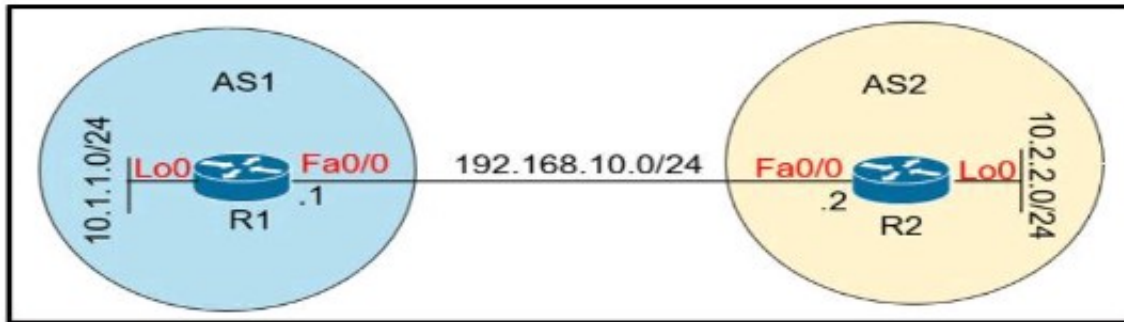
Support Virtual Switching System (VSS) to provide resiliency, and increased operational efficiency with a single point of management; VSS increases operational efficiency by simplifying the network, reducing switch management overhead by at least 50 percent. – Single configuration file and node to manage.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

#### NEW QUESTION 457

- (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 ebgp-multihop 2" on R2. 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



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.

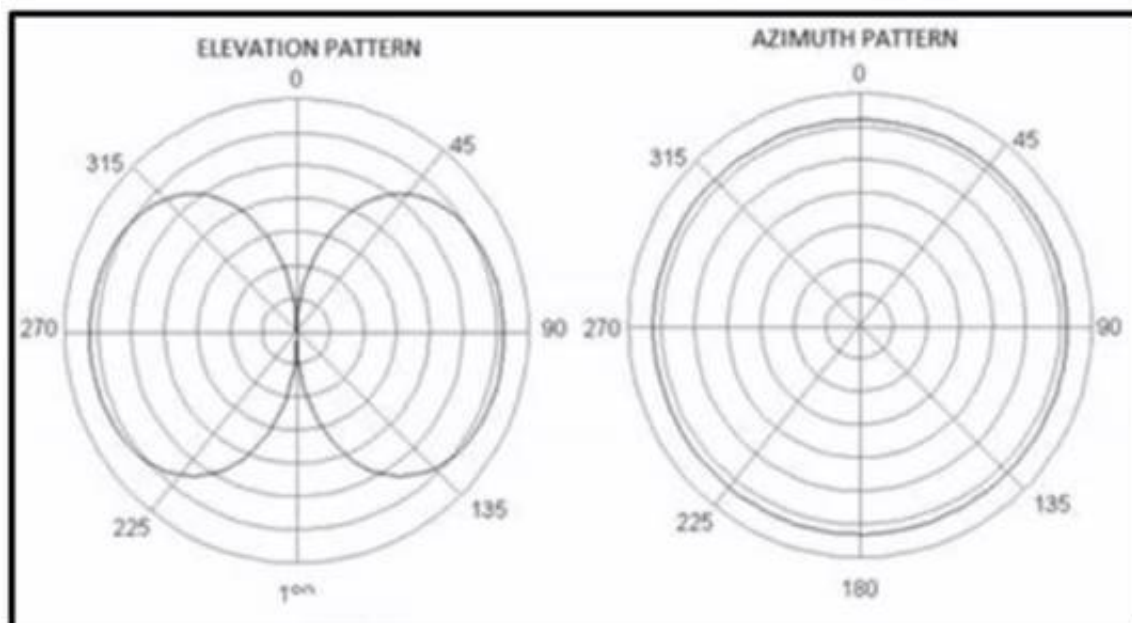
+ Bridge mode: bridge together the WLAN and the wired infrastructure together.

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 459

- (Topic 4)

Refer to the exhibit.



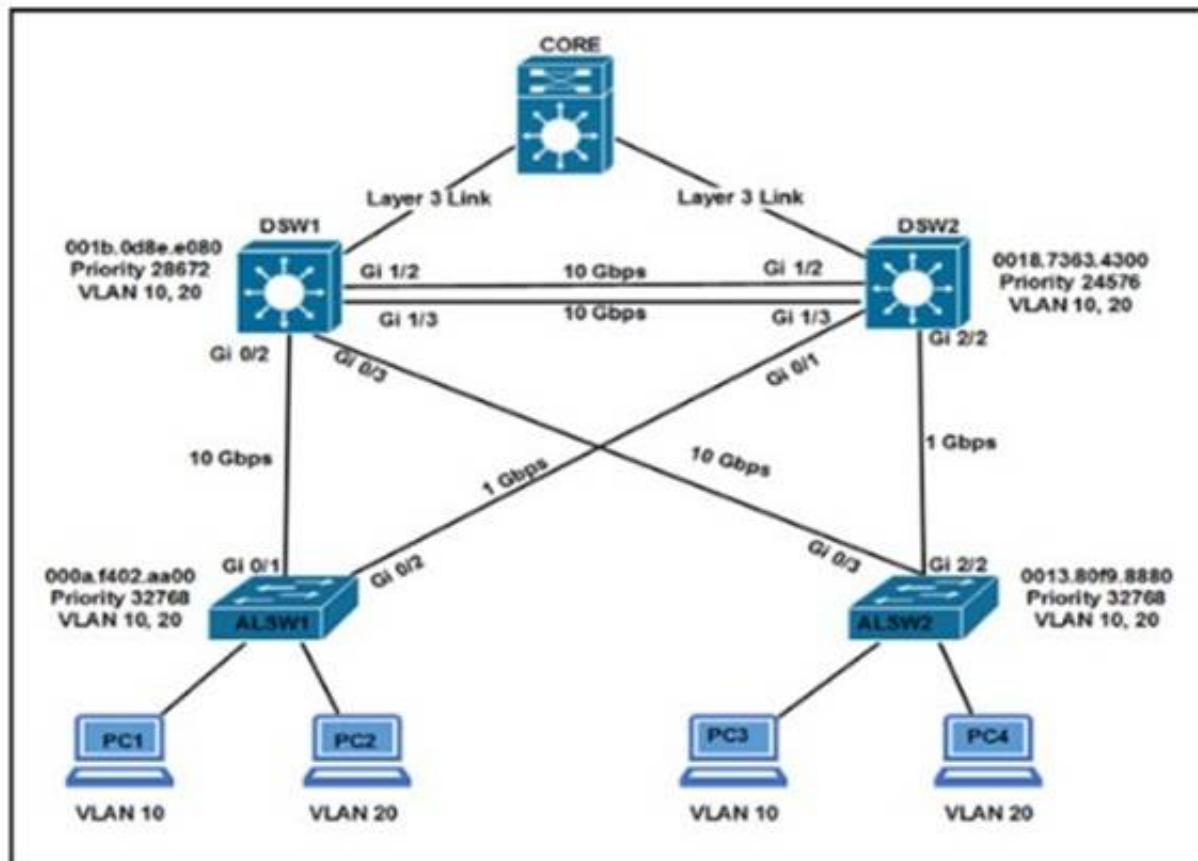
Which antenna emits this radiation pattern?

- A. omnidirectional
- B. Yagi
- C. RP-TNC
- D. dish

**Answer:** A

#### NEW QUESTION 464

- (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

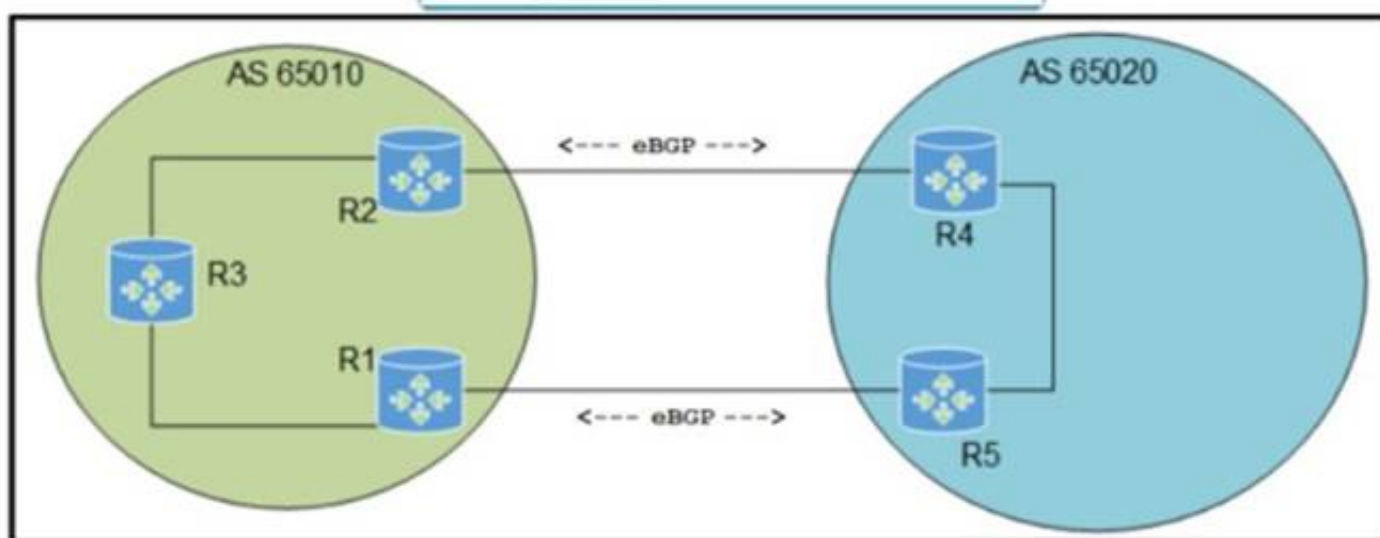
The bridge priority is a customizable value that can be used to influence which switch becomes the root bridge. The switch with the lowest priority, which implies the lowest BID, becomes the root bridge because a lower priority value takes precedence.

...

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 465**

- (Topic 4)



Refer to the exhibit. Which configuration must be applied to ensure that the preferred path for traffic from AS 65010 toward AS 65020 uses the R2 to R4 path?

A)

```
R2(config)# router bgp 65010
R2(config-router)# bgp default local-preference 200
R1(config)# router bgp 65010
R1(config-router)# bgp default local-preference 300
```

B)

```
R4(config)# router bgp 65020
R4(config-router)# bgp default local-preference 200
R5(config)# router bgp 65020
R5(config-router)# bgp default local-preference 300
```

C)

```
R2(config)# router bgp 65010
R2(config-router)# bgp default local-preference 300
R1(config)# router bgp 65010
R1(config-router)# bgp default local-preference 200
```

D)

```
R4(config)# router bgp 65020
R4(config-router)# bgp default local-preference 300
R5(config)# router bgp 65020
R5(config-router)# bgp default local-preference 200
```

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

**Answer:** C

#### NEW QUESTION 467

- (Topic 4)

Which configuration protects the password for the VTY lines against over-the-shoulder attacks?

- A. username admin secret 7 6j809j23kpp43883500N7%e\$
- B. service password-encryption
- C. line vty 04 password \$25\$FpM7182!
- D. line vty 0 15password \$25\$FpM71f82!

**Answer:** B

#### NEW QUESTION 471

- (Topic 4)

What is a client who is running 802.1x for authentication referred to as?

- A. supplicant
- B. NAC device
- C. authenticator
- D. policy enforcement point

**Answer:** A

#### NEW QUESTION 476

- (Topic 4)

Which of the following security methods uses physical characteristics of a person to authorize access to a location?

- A. Access control vestibule
- B. Palm scanner
- C. PIN pad
- D. Digital card reader
- E. Photo ID

**Answer:** B

#### Explanation:

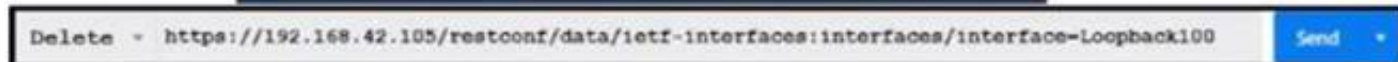
This is because a palm scanner is a type of biometric security method that uses the physical characteristics of a person's palm, such as the shape, size, and vein patterns, to authorize access to a location. A palm scanner is more reliable and secure than other methods, such as a PIN pad or a digital card reader, which can be easily stolen, lost, or shared. A palm scanner is also more hygienic and convenient than other biometric methods, such as a fingerprint scanner or a facial recognition system, which can be affected by dirt, oil, or lighting conditions. The source of this answer is the Cisco ENCOR v1.1 course, module 2, lesson 2.2: Implementing Device Access Control.

#### NEW QUESTION 480



- (Topic 4)

Refer to the exhibit.



What does the response "204 No Content mean for the REST API request?

- A. Interface toopback 100 is not removed from the configuration.
- B. Interface toopback 100 is not found in the configuration.
- C. Interface toopback 100 is removed from the configuration.
- D. The DELETE method is not supported.

**Answer: C**

**Explanation:**

This is because the response "204 No Content" means that the REST API request was successful, but there is no content to return. The request was a DELETE method, which is used to remove a resource from the server. The resource in this case was the interface loopback 100, which was deleted from the configuration of the device. The source of this answer is the Cisco ENCOR v1.1 course, module 8, lesson 8.4: Implementing REST API.

**NEW QUESTION 482**

- (Topic 4)

Which there application has the ability to make REST calls against Cisco DNA Center?

- A. API Explorer
- B. REST Explorer
- C. Postman
- D. Mozilla

**Answer: C**

**NEW QUESTION 485**

- (Topic 4)

An engineer is configuring RADIUS-Based Authentication with EAP MS-CHAPv2 is configured on a client device. Which outer method protocol must be configured on the ISE to support this authentication type?

- A. EAP-TLS
- B. PEAP
- C. LDAP
- D. EAP-FAST

**Answer: D**

**NEW QUESTION 488**

- (Topic 4)

Which device, in a LISP routing architecture, receives and de-encapsulates LISP traffic for endpoints within a LISP-capable site?

- A. MR
- B. ETR
- C. OMS
- D. ITR

**Answer: B**

**NEW QUESTION 493**

- (Topic 4)

An engineer applies this EEM applet to a router:

```
event manager applet Test
event timer watchdog time 600
action 1.0 cli command "enable"
action 2.0 cli command "term exec prompt timestamp"
action 3.0 cli command "term length 0"
action 4.0 cli command "show ip arp | in 0005.4210.0049"
action 5.0 regexp ".*(ARPA).*" $_cli_result
action 6.0 if $_regexp_result eq 1
action 7.0 syslog msg $_cli_result
action 8.0 end
```

What does the applet accomplish?

- A. It generates a syslog message every 600 seconds on the status of the specified MAC address.
- B. It checks the MAC address table every 600 seconds to see if the specified address has been learned.
- C. It compares syslog output to the MAC address table every 600 seconds and generates an event when there is a match.
- D. It compares syslog output to the MAC address table every 600 seconds and generates an event when no match is found.

**Answer: B**

**NEW QUESTION 494**

- (Topic 4)  
Which action limits the total amount of memory and CPU that is used by a collection of VMs?

- A. Place the collection of VMs in a resource pool.
- B. Place the collection of VMs in a vApp.
- C. Limit the amount of memory and CPU that is available to the cluster.
- D. Limit the amount of memory and CPU that is available to the individual VMs.

**Answer:** A

**NEW QUESTION 496**

- (Topic 4)  
Which two methods are used by an AP that is trying to discover a wireless LAN controller? (Choose two.)

- A. Cisco Discovery Protocol neighbour
- B. broadcasting on the local subnet
- C. DNS lookup cisco-DNA-PRIMARY.localdomain
- D. DHCP Option 43
- E. querying other APs

**Answer:** BD

**NEW QUESTION 499**

- (Topic 4)  
Why would a small or mid-size business choose a cloud solution over an on-premises solution?

- A. Cloud provides higher data security than on-premises.
- B. Cloud provides more control over the implementation process than on-premises.
- C. Cloud provides greater ability for customization than on-premises.
- D. Cloud provides lower upfront cost than on-premises.

**Answer:** C

**NEW QUESTION 501**

- (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 506**

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

link state routing protocol

distance vector routing protocol

metric is based on delay and bandwidth by default

makes it easy to segment the network logically

constructs three tables as part of its operation: neighbor table, topology table, and routing table

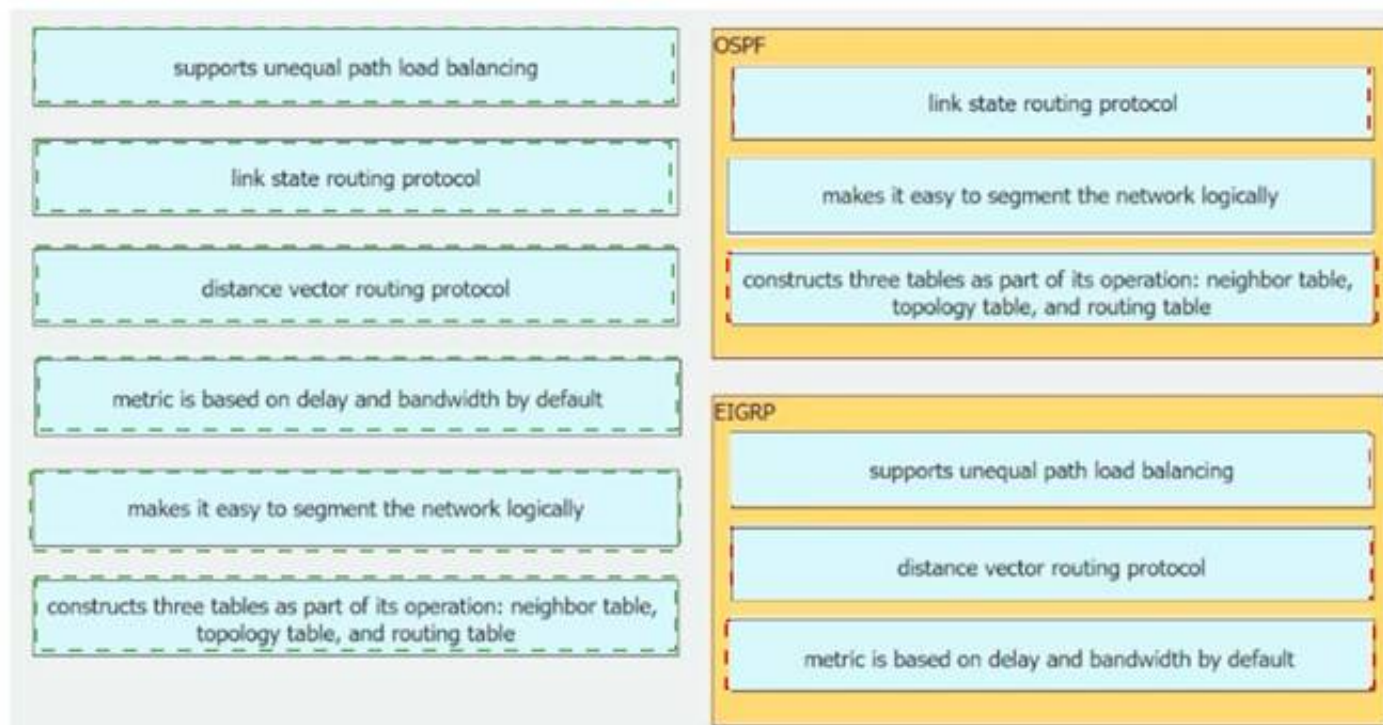
OSPF

EIGRP

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



#### NEW QUESTION 507

- (Topic 4)

Based on the router's API output In JSON format below, which Python code will display the value of the 'role' key?

```
{
  "response": [{
    "family": "Routers",
    "macAddress": "00:c8:8b:80:bb:00",
    "hostname": "BorderA",
    "role": "BORDER ROUTER",
    "lastUpdateTime": 1577420167054,
    "serialNumber": "FXS8799Q1SE",
    "softwareVersion": "16.3.2",
    "upTime": "5 days, 9:22:32:17",
    "lastUpdated": "2021-03-05 23:30:37"
  }]
}
```

- ☐ json\_data = json.loads(response.text)  
print(json\_data['response']['family']['role'])
- ☐ json\_data = response.json()  
print(json\_data['response'][family]['role'])
- ☐ json\_data = json.loads(response.text)  
print(json\_data[response][0][role])
- ☐ json\_data = response.json()  
print(json\_data['response'][0]['role'])

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

Answer: C

#### NEW QUESTION 512

- (Topic 4)

Which LISP infrastructure device provides connectivity between non-sites and LISP sites by receiving non-LISP traffic with a LISP site destination?

- A. PETR
- B. PITR
- C. map resolver
- D. map server

Answer: B



#### NEW QUESTION 517

- (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 f 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 521

DRAG DROP - (Topic 4)

An engineer must create a script to append and modify device entries in a JSON-formatted file. The script must work as follows:

? Until interrupted from the keyboard, the script reads in the hostname of a device, its management IP address, operating system type, and CLI remote access protocol.

? After being interrupted, the script displays the entered entries and adds them to

the JSON-formatted file, replacing existing entries whose hostname matches. The contents of the JSON-formatted file are as follows:

```
{
  "examplerouter": {
    "ip": "203.0.113.1",
    "os": "ios-xe",
    "protocol": "ssh"
  },
  ...
}
```

Drag and drop the statements onto the blanks within the code to complete the script. Not all options are used.

ChangedDevices = {}

try:

Name = input('\n\nDevice name: ')

IP = input('Address: ')

OS = input('Operating system: ')

Proto = input('CLI access protocol: ')

ChangedDevices.update({Name: {"ip": IP,

"os": OS, "protocol": Proto}})

(KeyboardInterrupt, EOFError):

pass

print("\n\n==> Entered device entries <==")

print(json.dumps(ChangedDevices, indent=4))

("devicesData.json", "r+")

Devices = json.load(File)

Devices.update(ChangedDevices)

File.seek(0)

json.dump(Devices, File, indent=4)

while True:

except

import json

File.open()

File.close()

File = open

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

```
import json
ChangedDevices = {}
try:
    while True:
        Name = input('\n\nDevice name: ')
        IP = input('Address: ')
        OS = input('Operating system: ')
        Proto = input('CLI access protocol: ')
        ChangedDevices.update({Name: {"ip": IP,
        "os": OS, "protocol": Proto}})
        File.close() (KeyboardInterrupt, EOFError):
        pass

    print("\n\n==> Entered device entries <==")
    print(json.dumps(ChangedDevices, indent=4))
    File.open() ("devicesData.json", "r+")
    Devices = json.load(File)
    Devices.update(ChangedDevices)
    File.seek(0)
    json.dump(Devices, File, indent=4)
    File = open
```

#### NEW QUESTION 526

- (Topic 4)

What are two characteristics of vManage APIs? (Choose two.)

- A. Southbound API is based on OMP and DTLS.
- B. Northbound API is RESTful, using JSON.
- C. Northbound API is based on RESTCONF and JSON.
- D. Southbound API is based on NETCONF and XML.
- E. Southbound API is based on RESTCONF and JSON.

**Answer:** BD

#### NEW QUESTION 529

- (Topic 4)

A technician is assisting a user who cannot connect to a website. The technician attempts to ping the default gateway and DNS server of the workstation. According to troubleshooting methodology, this is an example of:

- A. a divide-and-conquer approach.
- B. a bottom-up approach.
- C. a top-to-bottom approach.
- D. implementing a solution.

**Answer:** C

#### Explanation:

This is because a top-to-bottom approach is a troubleshooting methodology that starts from the highest layer of the OSI model and works its way down to the lowest layer. The technician is using this approach by first testing the network layer connectivity with the ping command, which uses the ICMP protocol. If the ping is successful, the technician can move on to the next layer, such as the transport layer or the application layer. If the ping fails, the technician can troubleshoot the lower layers, such as the data link layer or the physical layer. The source of this answer is the Cisco ENCOR v1.1 course, module 10, lesson 10.3: Applying Troubleshooting Methodologies.

#### NEW QUESTION 533

- (Topic 4)

Which authorization framework gives third-party applications limited access to HTTP services?

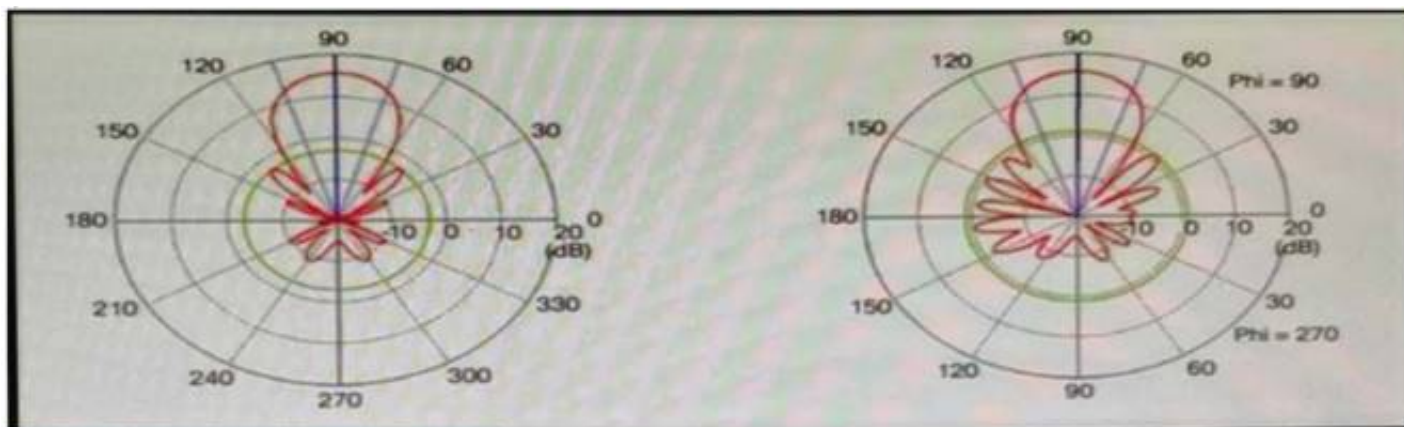
- A. IPsec
- B. Basic Auth
- C. GRE
- D. OAuth 2.0

**Answer:** D

#### NEW QUESTION 535

- (Topic 4)

Refer to the exhibit.



Which type of antenna is shown on the radiation patterns?

- A. Yagi
- B. dipole
- C. patch
- D. omnidirectional

**Answer:** A

#### NEW QUESTION 540

- (Topic 4)

What is difference between TCAM and the MAC address table?

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

**Answer:** D

#### NEW QUESTION 543

- (Topic 4)

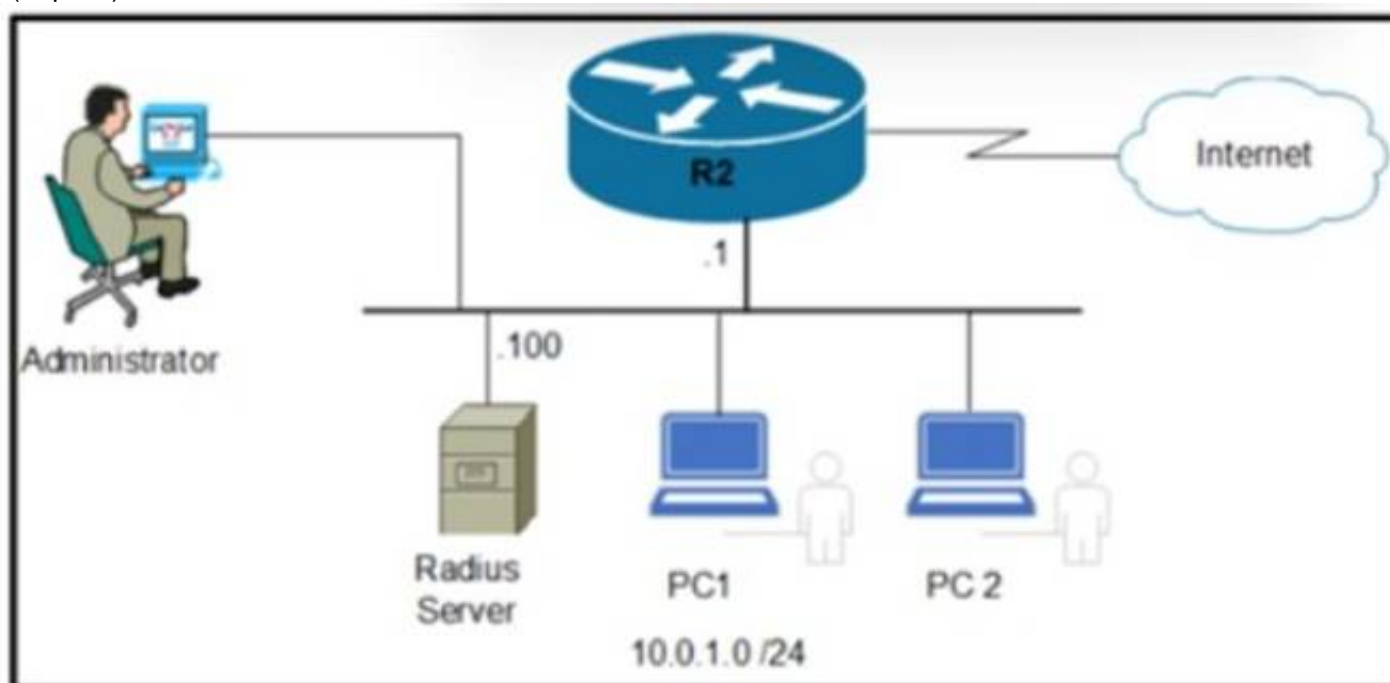
Which Cisco WLC feature allows a wireless device to perform a Layer 3 roam between two separate controllers without changing the client IP address?

- A. mobile IP
- B. mobility tunnel
- C. LWAPP tunnel
- D. GRE tunnel

**Answer:** B

#### NEW QUESTION 546

- (Topic 4)



Refer to the exhibit. Which command set enables router R2 to be configured via NETCONF?

- A)
 

```
R1(config)# username Netconf privilege 15 password example_password
R1(config)# netconf-yang
R1(config)# netconf-yang feature candidate-datastore
```

- B)
 

```
R1(config)# snmp-server manager
R1(config)# snmp-server community ENCOR ro
```



C)

```
R1(config)# snmp-server manager
R1(config)# snmp-server community ENCOR rw
```

D)

```
R1(config)# netconf
R1(config)# ip http secure-server
```

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

**Answer:** A

#### NEW QUESTION 551

- (Topic 4)

Which QoS queuing method transmits packets out of the interface in the order the packets arrive?

- A. custom
- B. weighted- fair
- C. FIFO
- D. priority

**Answer:** C

#### NEW QUESTION 554

- (Topic 4)

Which two functions is an edge node responsible for? (Choose two.)

- A. provides multiple entry and exit points for fabric traffic
- B. provides the default exit point for fabric traffic
- C. provides the default entry point for fabric traffic
- D. provides a host database that maps endpoint IDs to a current location
- E. authenticates endpoints

**Answer:** AD

#### NEW QUESTION 555

- (Topic 4)

An engineer must configure GigabitEthernet 0/0 for VRRP group 65. The router must assume the primary role when it has the highest priority in the group. Which command set must be applied?

A)

```
interface GigabitEthernet0/0
ip address 10.10.10.1 255.255.255.0
vrrp 65 ip 10.10.10.1
standby 65 priority 100
standby 65 preempt
```

B)

```
interface GigabitEthernet0/0
ip address 10.10.10.2 255.255.255.0
standby 65 ip 10.10.10.1
standby 65 track 1 decrement 10
standby 65 preempt
```

C)

```
interface GigabitEthernet0/0
ip address 10.10.10.2 255.255.255.0
vrrp 65 ip 10.20.20.1
vrrp 65 track 1 decrement 100
vrrp 65 preempt
vrrp 65 authentication $2#442619822
```

D)

```
interface GigabitEthernet0/0
ip address 10.10.10.2 255.255.255.0
vrrp 65 ip 10.10.10.1
vrrp 65 priority 110
```

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

**Answer:** D

#### NEW QUESTION 559

- (Topic 4)

How is traffic classified when using Cisco TrustSec technology?

- A. with the VLAN
- B. with the MAC address
- C. with the IP address
- D. with the security group tag

**Answer:** D

#### NEW QUESTION 564

- (Topic 4)

What is a benefit of using segmentation with TrustSec?

- A. Packets sent between endpoints on a LAN are encrypted using symmetric key cryptography.
- B. Firewall rules are streamlined by using business-level profiles.
- C. Integrity checks prevent data from being modified in transit.
- D. Security group tags enable network segmentation.

**Answer:** B

#### NEW QUESTION 567

- (Topic 4)

Which two pieces of information are necessary to compute SNR? (Choose two.)

- A. transmit power
- B. noise floor
- C. EIRP
- D. antenna gain
- E. RSSI

**Answer:** BE

#### NEW QUESTION 570

- (Topic 4)

Which signal strength and noise values meet the minimum SNR for voice networks?

- A. signal strength -67 dBm, noise 91 dBm
- B. signal strength -69 dBm, noise 94 dBm
- C. signal strength -68 dBm, noise 89 dBm
- D. signal strength -66 dBm, noise 90 dBm

**Answer:** A

#### NEW QUESTION 575

- (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 peenng 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 579

- (Topic 4)

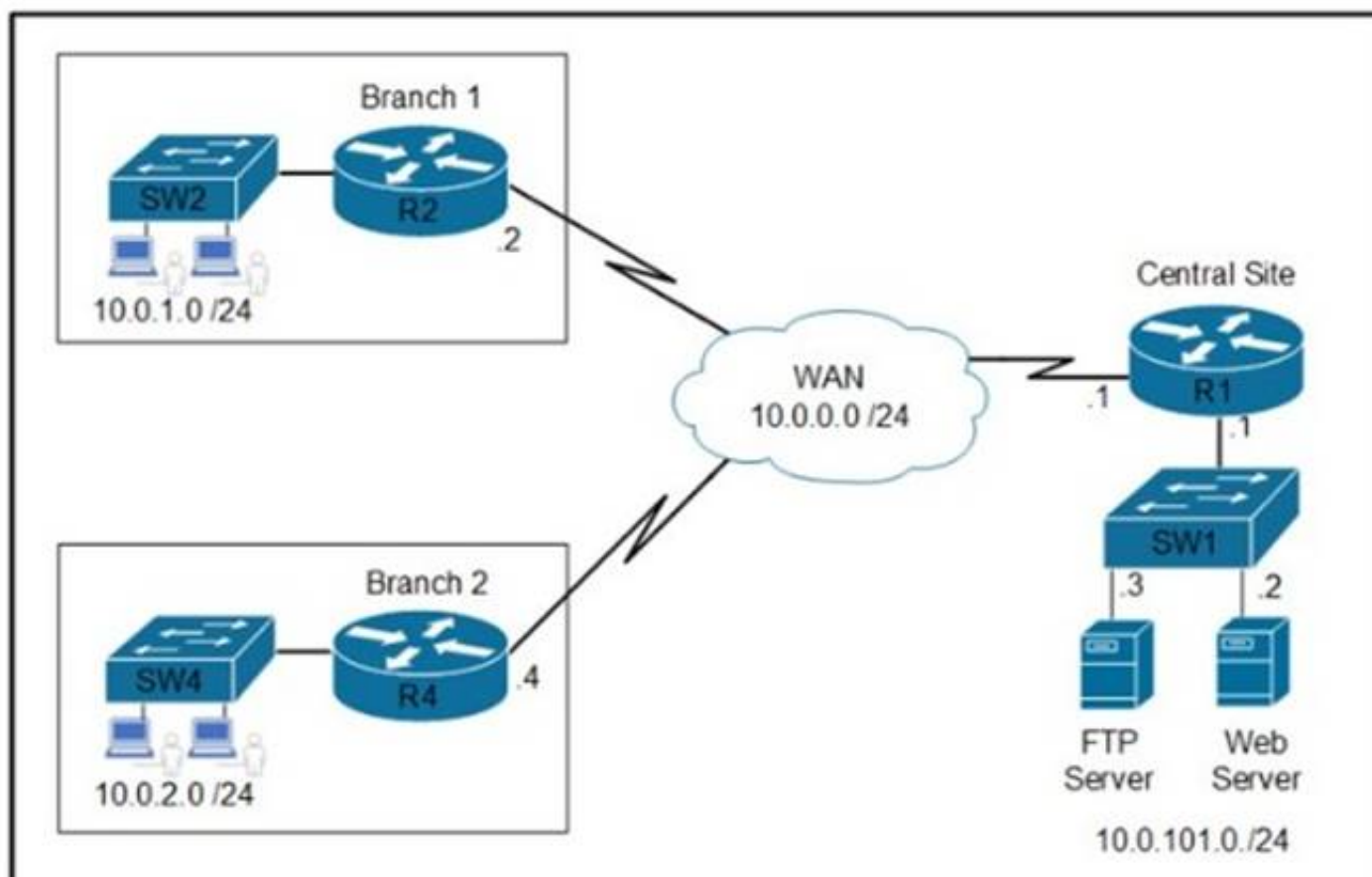
Which solution simplifies management ot secure access to network resources?

- 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 581

- (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 583

- (Topic 4)

```
event manager applet Config
event cli pattern "configure terminal"
action 1.0 cli command "enable"
```

Refer to the exhibit. An engineer constructs an EEM applet to prevent anyone from entering configuration mode on a switch. Which snippet is required to complete the EEM applet?

- A. sync yes skip yes
- B. sync no skip yes
- C. sync no skip no
- D. sync yes skip no

Answer: B

#### NEW QUESTION 586

- (Topic 4)

An engineer uses the Design workflow to create a new network infrastructure in Cisco DNA Center. How is the physical network device hierarchy structured?

- A. by organization
- B. by location
- C. by hostname naming convention
- D. by role

Answer: B

#### Explanation:

This is because the Design workflow in Cisco DNA Center allows the engineer to create a new network infrastructure by defining the physical network device hierarchy based on the location of the devices. The location hierarchy consists of four levels: global, area, building, and floor. The engineer can add, edit, or delete locations and assign devices to them. The location hierarchy helps to organize the network devices and apply policies and settings based on the location. The source of this answer is the Cisco ENCOR v1.1 course, module 8, lesson 8.6: Implementing Network Design Processes.

#### NEW QUESTION 589

- (Topic 4)

Which two steps are required for a complete Cisco DNA Center upgrade? (Choose two.)

- A. golden image selection
- B. automation backup
- C. proxy configuration
- D. application updates
- E. system update

Answer: DE

#### NEW QUESTION 592

- (Topic 4)

Which two methods are used to interconnect two Cisco SD-Access Fabric sites? (Choose two.)

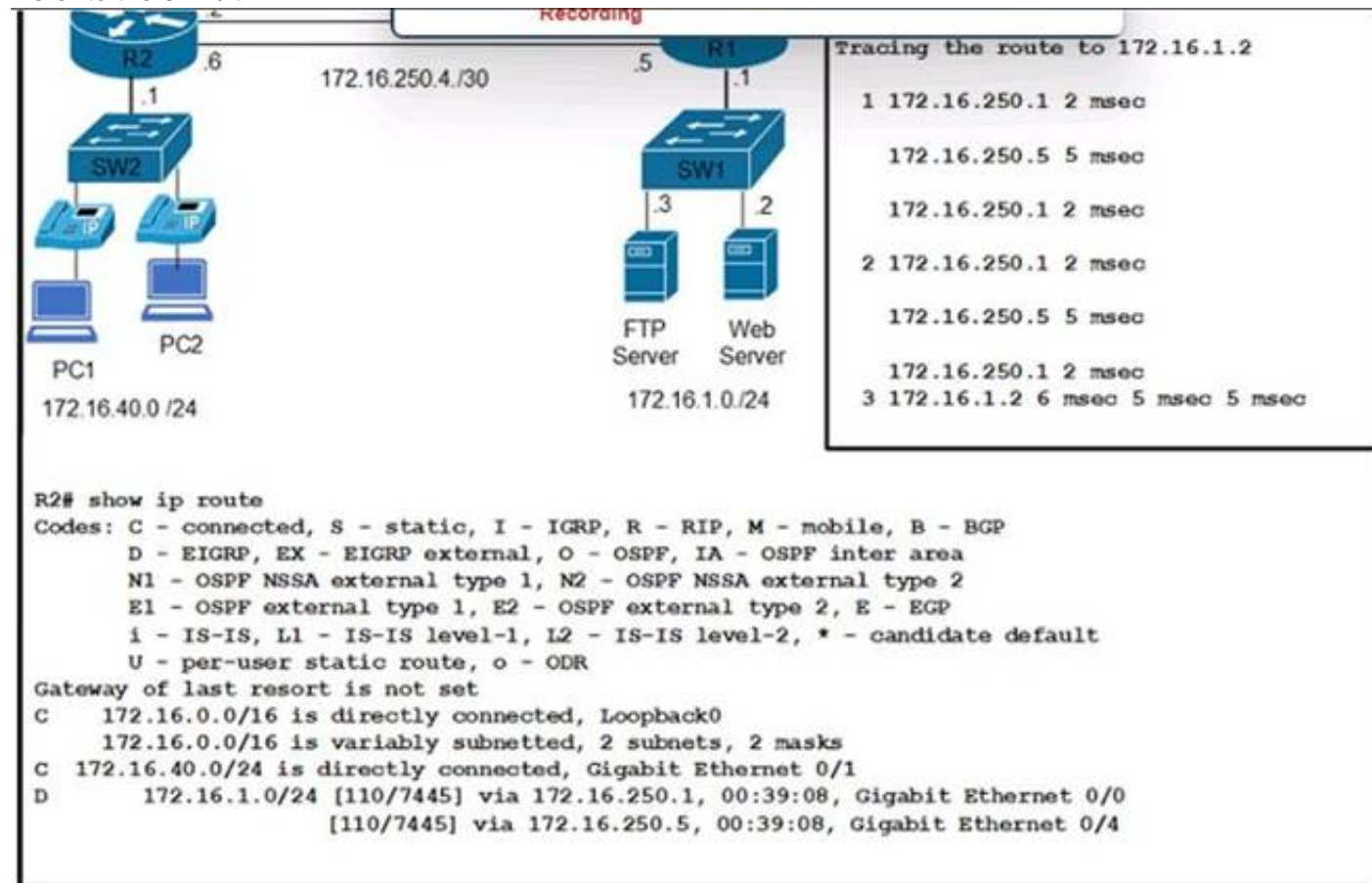
- A. SD-Access transit
- B. fabric interconnect
- C. wireless transit
- D. IP-based transit
- E. SAN transit

**Answer:** AD

#### NEW QUESTION 594

- (Topic 4)

Refer to the exhibit.



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.

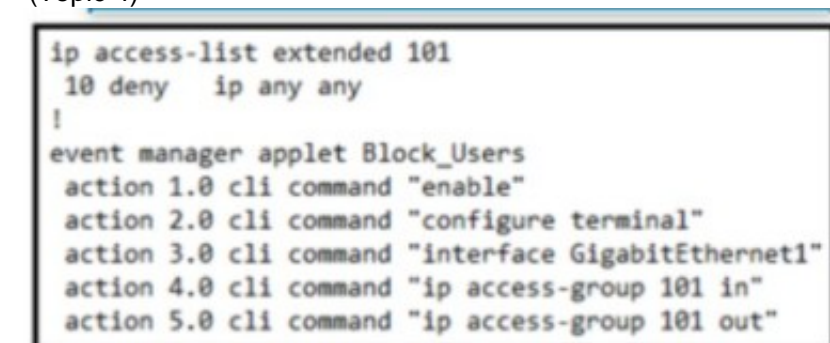
**Answer:** C

#### 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 595

- (Topic 4)



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 598

- (Topic 4)

Refer to the exhibit.

```
interface Ethernet0/0

 ipaddress 10.1.1.1 255.255.255.252

 ip natoutside

!

interface Ethernet0/0

 ipaddress 10.10.10.1 255.255.255.0

 ip natinside

!

ip nat inside source static 10.10.10.10 10.0.3.10
```

Which address type is 10.10.10.10 configured for?

- A. inside global
- B. outside local
- C. outside global
- D. inside local

**Answer:** D

#### NEW QUESTION 600

- (Topic 4)

Refer to the exhibit.



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 601

- (Topic 4)

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

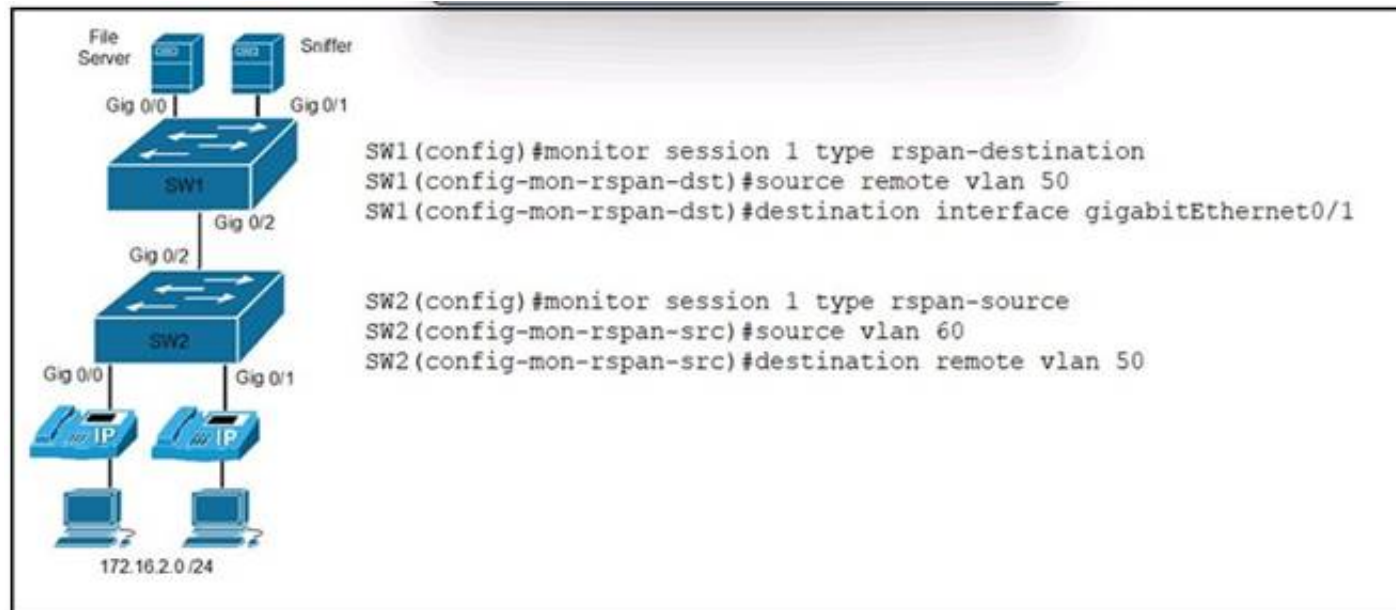
- A. RSSI
- B. dBI
- C. SNR
- D. EIRP

**Answer: B**

#### NEW QUESTION 603

- (Topic 4)

Refer to the exhibit.



An engineer must send the 172.16.2.0 /24 user traffic to a packet capture tool to troubleshoot an issue. Which action completes the configuration?

- A. Encrypt the traffic between the users and the monitoring servers.
- B. Disable the spanning tree protocol on the monitoring server VLAN.
- C. Enable the Cisco Discovery Protocol on the server interfaces.
- D. Define the remote span VLAN on SW1 and SW2.

**Answer: D**

#### Explanation:

This is because the remote span VLAN is used to transport the mirrored traffic from the source switch to the destination switch, where the monitoring server is connected. The remote span VLAN must be defined on both switches and must not be used for any other purpose. The source of this answer is the Cisco ENCOR v1.1 course, module 6, lesson 6.2: Implementing SPAN, RSPAN, and ERSPAN.

#### NEW QUESTION 608

- (Topic 4)

Which unit of measure is used to measure wireless RF SNR?

- A. mW
- B. bBm
- C. dB
- D. dBi

**Answer: C**

#### NEW QUESTION 609

DRAG DROP - (Topic 4)

Drag and drop the code snippets from the bottom onto the blanks in the code to construct a request that configures a deny rule on an access list?

```
{
  "ip": {
    "access-list": {
      "ios-acl:extended": {
        "ios-acl:name": "ato",
        "ios-acl:": {
          "ios-acl:sequence": "111111",
          "ios-acl:ace-rule": {
            "ios-acl:action": "",
            "ios-acl:protocol": "",
            "ios-acl:any": "",
            "ios-acl:": ""
          }
        }
      }
    }
  }
}
```

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

```
{
  "ip": {
    "access-list": {
      "ios-acl:extended": {
        "ios-acl:name": "ato",
        "ios-acl:dst-any": {
          "ios-acl:sequence": "111111",
          "ios-acl:ace-rule": {
            "ios-acl:action": "deny",
            "ios-acl:protocol": "ip",
            "ios-acl:any": "",
            "ios-acl:access-list-seq-rule": ""
          }
        }
      }
    }
  }
}
```

#### NEW QUESTION 610

- (Topic 4)  
Refer to the exhibit.

```
pl1=[
<get-config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <source>
    <running/>
  </source>
  <filter>
    <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
      <ip>
        <access-list>
          <extended xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-acf">
            <name>flp</name>
          </extended>
        </access-list>
      </ip>
    </native>
  </filter>
</get-config>
]
with manager.connect(host=10.1.1.1, port=830, username=cisco, password=cisco, timeout=90, hostkey_verify=False) as m:
    for rpc in pl1:
        r1= m.dispatch(et.fromstring(rpc))
        d1= xmldict.parse(r1.xml)['rpc-reply']['data']['native']['ip']['access-list']['extended']['access-list-seq-rule']
```

What is achieved by the XML code?

- A. It reads the access list sequence numbers from the output of the show ip access-list extended flp command into a dictionary list.
- B. It displays the output of the show ip access-list extended flp command on the terminal screen
- C. It displays the access list sequence numbers from the output of the show Ip access-list extended flp command on the terminal screen
- D. It reads the output of the show ip access-list extended flp command into a dictionary list.

**Answer:** A

#### NEW QUESTION 614

- (Topic 4)

A company recently rearranged some users' workspaces and moved several users to different desks. The network administrator receives a report that all of the users who were moved are having connectivity issues. Which of the following is the most likely reason?

- A. Ports are error disabled.
- B. Ports are administratively down.
- C. Ports are having an MDIX issue.
- D. Ports are trunk ports.

**Answer:** A

#### Explanation:

This is because ports can become error disabled when they detect certain errors or violations on the network, such as a loop, a security breach, or a duplex mismatch. When a port is error disabled, it shuts down and stops forwarding traffic until it is manually re-enabled by the administrator. The users who were moved to different desks may have plugged their devices into ports that were configured with different settings or security policies than their original ports, and this may have triggered the error disable state. The source of this answer is the Cisco ENCOR v1.1 course, module 3, lesson 3.3: Implementing EtherChannel.

#### NEW QUESTION 618

.....



## Relate Links

**100% Pass Your 350-401 Exam with ExamBible Prep Materials**

<https://www.exambible.com/350-401-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>