

Cisco

Exam Questions 350-401

Implementing and Operating Cisco Enterprise Network Core Technologies



NEW QUESTION 1

- (Topic 4)

Which access control feature does MAB provide?

- A. user access based on IP address
- B. allows devices to bypass authenticate*
- C. network access based on the physical address of a device
- D. simultaneous user and device authentication

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?

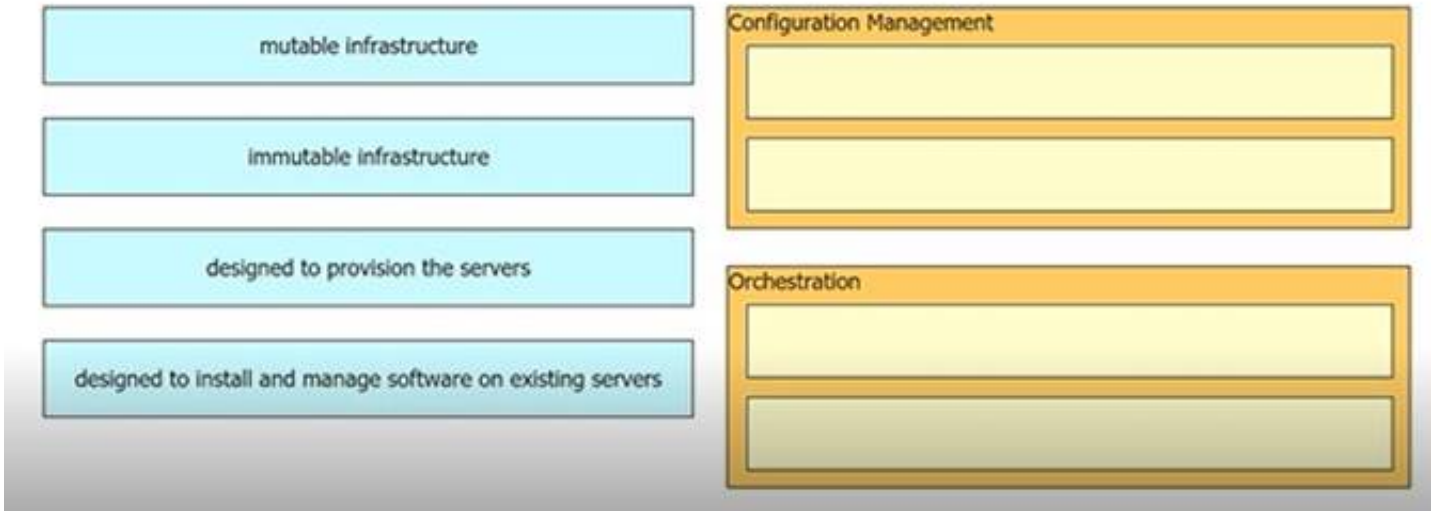
- A. Configure channel-group 1 mode active on GVO and G1 1 of SW2.
- B. Configure trunksport trunk encapsulation dot1q on SW1 and SW2.
- C. Configure channel-group 1 mode active on GI'O and GM of SW1 .
- D. Configure switchport mode dynamic desirable on SW1 and SW2

Answer: C

NEW QUESTION 3

DRAG DROP - (Topic 4)

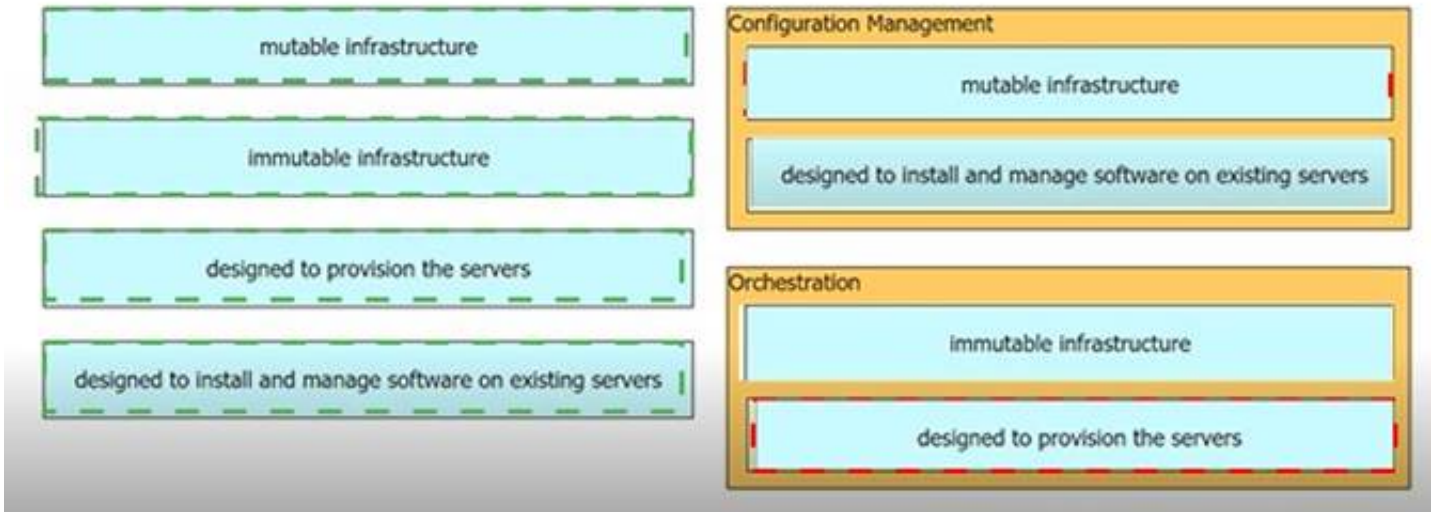
Drag and drop the characteristics from the left onto the orchestration tool classifications on the right.



- A. Mastered
- B. Not Mastered

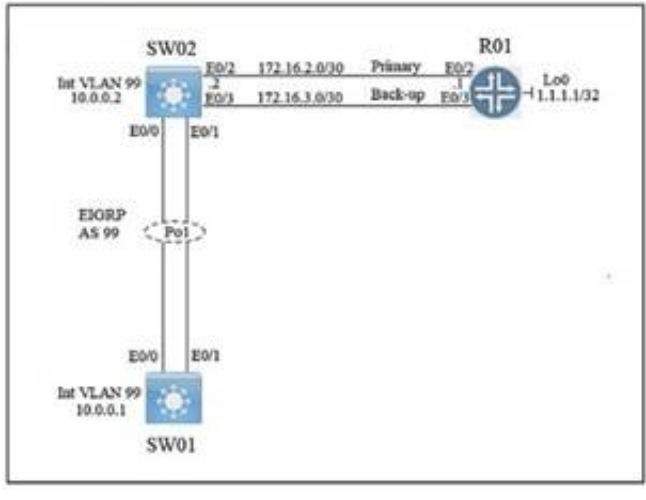
Answer: A

Explanation:



NEW QUESTION 4
SIMULATION - (Topic 4)
Simulation 07

GuidelinesTopologyTasks



GuidelinesTopologyTasks

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.

Submit feedback about this item

R01SW01SW02

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 5

- (Topic 4)

An engineer must implement a configuration to allow a network administrator to connect to the console port of a router and authenticate over the network. Which command set should the engineer use?

- A. aaa new-modelaaa authentication login default enable
- B. aaa new-modelaaa authentication login console local
- C. aaa new-model aaa authentication login console group radius
- D. aaa new-modelaaa authentication enable default

Answer: B

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)

Which activity requires access to Cisco DNA Center CLI?

- A. provisioning a wireless LAN controller
- B. creating a configuration template
- C. upgrading the Cisco DNA Center software
- D. graceful shutdown of Cisco DNA Center

Answer: D

NEW QUESTION 8

- (Topic 4)

An engineer must configure a router to allow users to run specific configuration commands by validating the user against the router database. Which configuration must be applied?

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

Answer: C

NEW QUESTION 9

- (Topic 4)

Which security measure mitigates a man-in-the-middle attack of a REST API?

- A. SSL certificates
- B. biometric authentication
- C. password hash
- D. non repudiation feature

Answer: A

NEW QUESTION 10

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 10

- (Topic 4)

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

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

Answer: A

Explanation:

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

NEW QUESTION 13

- (Topic 4)

S1# show etherchannel summary

Flags: D - down P - bundled in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3 S - Layer2

U - in use f - failed to allocate aggregator

M - not in use, minimum links not met

u - unsuitable for bundling

w - waiting to be aggregated

d - default port

Number of channel-groups in use: 1

Number of aggregators: 1

Group Port-channel Protocol Ports

-----+-----+-----+-----

1 Pol (SD) - Fa0/1 (D) Fa0/2 (D)

S1# show run | begin interface port-channel

interface Port-channel1

switchport mode trunk

|

interface FastEthernet0/1

switchport mode trunk

channel-group 1 mode on

|

interface FastEthernet0/2

switchport mode trunk

channel-group 1 mode on

|

<Output omitted>

S2# show run | begin interface port-channel

interface Port-channel1

switchport mode trunk

|

interface FastEthernet0/1

switchport mode trunk

channel-group 1 mode desirable

|

interface FastEthernet0/2

switchport mode trunk

channel-group 1 mode desirable

|

<Output omitted>

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

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

Answer: C

NEW QUESTION 14

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 19

- (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 21

- (Topic 4)

When does a Cisco StackWise primary switch lose its role?

- A. when a stack member fails
- B. when the stack primary is reset
- C. when a switch with a higher priority is added to the stack
- D. when the priority value of a stack member is changed to a higher value

Answer: C

NEW QUESTION 24

- (Topic 4)

An engineer is connected to a Cisco router through a Telnet session. Which command must be issued to view the logging messages from the current session as soon as they are generated by the router?

- A. logging buffer
- B. service timestamps log uptime
- C. logging host
- D. terminal monitor

Answer: D

NEW QUESTION 27

- (Topic 4)

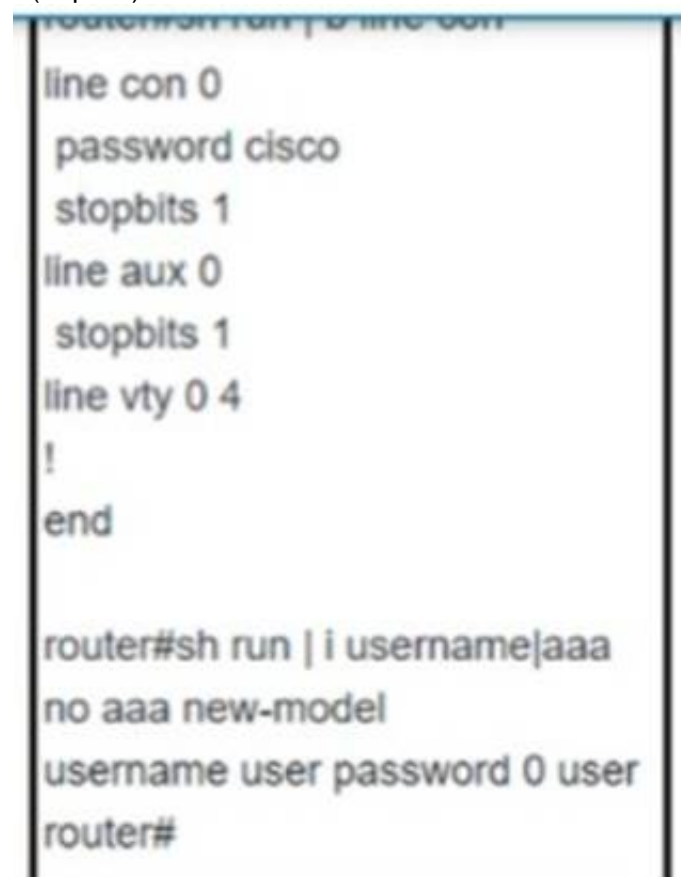
How is a data modelling language used?

- A. To enable data to be easily structured, grouped, validated, and replicated.
- B. To represent finite and well-defined network elements that cannot be changed.
- C. To model the flows of unstructured data within the infrastructure
- D. To provide human readability to scripting languages

Answer: A

NEW QUESTION 32

- (Topic 4)



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

A)

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

B)

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

C)

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

D)

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

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

Answer: B

NEW QUESTION 37

- (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 41

- (Topic 4)

Where in Cisco DNA Center is documentation of each API call, organized by its functional area?

- A. Developer Toolkit
- B. platform management
- C. platform bundles
- D. Runtime Dashboard

Answer: A

Explanation:

<https://developer.cisco.com/docs/dna-center/#!api-quick-start/cisco-dna-center-platform-api-overview>

NEW QUESTION 45

- (Topic 1)

What is used to perform OoS packet classification?

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

Answer: D

Explanation:

Type of service, when we talk about PACKET, means layer 3

NEW QUESTION 50

- (Topic 2)

Refer to the exhibit.


```
DSW2#sh spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    4106
            Address     0018.7363.4300
            This bridge is the root
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4106 (priority 4096 sys-id-ext 20)
            Address     0018.7363.4300
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  300

Interface                Role Sts Cost      Prio.Nbr Type
-----
Fa1/0/7                  Desg FWD 2        128.9   P2p Peer (STP)
Fa1/0/10                 Desg FWD 4        128.12  P2p Peer (STP)
Fa1/0/11                 Desg FWD 2        128.13  P2p Peer (STP)
Fa1/0/12                 Desg FWD 2        128.14  P2p Peer (STP)
```

What is the result when a switch that is running PVST+ is added to this network?

- A. DSW2 operates in Rapid PVST+ and the new switch operates in PVST+
- B. Both switches operate in the PVST+ mode
- C. Spanning tree is disabled automatically on the network
- D. Both switches operate in the Rapid PVST+ mode.

Answer: A

Explanation:

From the output we see DSW2 is running in RSTP mode (in fact Rapid PVST+ mode as Cisco does not support RSTP alone). When a new switch running PVST+ mode is added to the topology, they keep running the old STP instances as RSTP (in fact Rapid PVST+) is compatible with PVST+.

NEW QUESTION 51

- (Topic 2)

Refer to the exhibit.



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

A)

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

B)

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

C)

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

D)

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

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

Answer: B

NEW QUESTION 52

DRAG DROP - (Topic 2)

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

cost-based metric

Dual Diffusing Update algorithm

metrics are bandwidth, delay, reliability, load, and MTU

Dijkstra algorithm

EIGRP

OSPF

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

cost-based metric

Dual Diffusing Update algorithm

metrics are bandwidth, delay, reliability, load, and MTU

Dijkstra algorithm

EIGRP

metrics are bandwidth, delay, reliability, load, and MTU

Dual Diffusing Update algorithm

OSPF

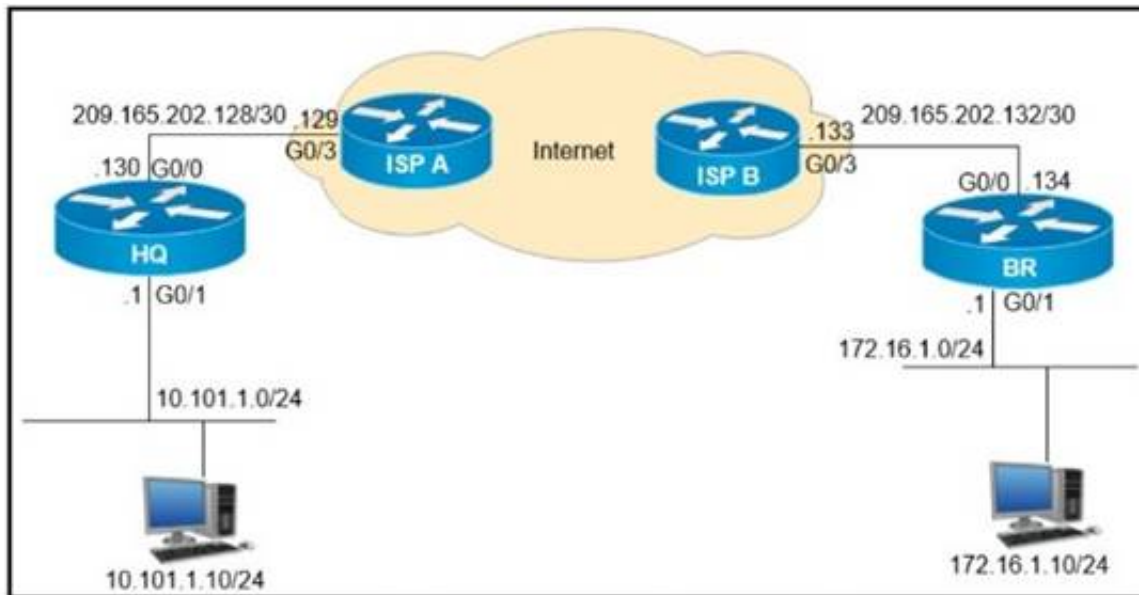
cost-based metric

Dijkstra algorithm

NEW QUESTION 56

- (Topic 2)

Refer to the exhibit.



```
> Frame 24: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
> Ethernet II, Src: 50:00:00:01:00:01 (50:00:00:01:00:01), Dst: 50:00:00:02:00:01 (50:00:00:02:00:01)
> Internet Protocol Version 4, Src: 209.165.202.130, Dst: 209.165.202.134
> Generic Routing Encapsulation (IP)
> Internet Protocol Version 4, Src: 10.111.111.1, Dst: 10.111.111.2
> Internet Control Message Protocol
```

A GRE tunnel has been created between HQ and BR routers. What is the tunnel IP on the HQ router?

- A. 10.111.111.1
- B. 10.111.111.2
- C. 209.165.202.130
- D. 209.165.202.134

Answer: A

NEW QUESTION 60

- (Topic 2)

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

Refer to the exhibit. Which command is required to verify NETCONF capability reply messages?

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

Answer: D

NEW QUESTION 63

- (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 68

- (Topic 2)

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

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

Answer: B

NEW QUESTION 70

- (Topic 2)

How cloud deployments differ from on-prem deployments?

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

Answer: C

NEW QUESTION 72

- (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 (= 2²⁴) VXLAN segments to coexist within the same infrastructure. This surely solve the small number of traditional VLANs.

NEW QUESTION 73

- (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 76

- (Topic 2)

When is the Design workflow used In Cisco DNA Center?

- A. in a greenfield deployment, with no existing infrastructure
- B. in a greenfield or brownfield deployment, to wipe out existing data
- C. in a brownfield deployment, to modify configuration of existing devices in the network
- D. in a brownfield deployment, to provision and onboard new network devices

Answer: A

Explanation:

The Design area is where you create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network. Use the Design workflow if you do not already have an existing infrastructure. If you have an existing infrastructure, use the Discovery feature.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/user_guide/b_cisco_dna_center_ug_2_1_2/b_cisco_dna_center_ug_2_1_1_chapter_0110.html

Reference: <https://synoptek.com/insights/it-blogs/greenfield-vs-brownfield-software-development/> "Greenfield development refers to developing a system for a totally new environment and requires development from a clean slate – no legacy code around. It is an approach used when you're starting fresh and with no restrictions or dependencies."

NEW QUESTION 77

- (Topic 2)

An engineer is implementing a Cisco MPLS TE tunnel to improve the streaming experience for the clients of a video-on-demand server. Which action must the engineer perform to configure extended discovery to support the MPLS LDP session between the headend and tailend routers?

- A. Configure the interface bandwidth to handle TCP and UDP traffic between the LDP peers
- B. Configure a Cisco MPLS TE tunnel on both ends of the session
- C. Configure an access list on the interface to permit TCP and UDP traffic
- D. Configure a targeted neighbor session.

Answer: B

NEW QUESTION 78

- (Topic 2)

In a Cisco SD-WAN solution, how is the health of a data plane tunnel monitored?

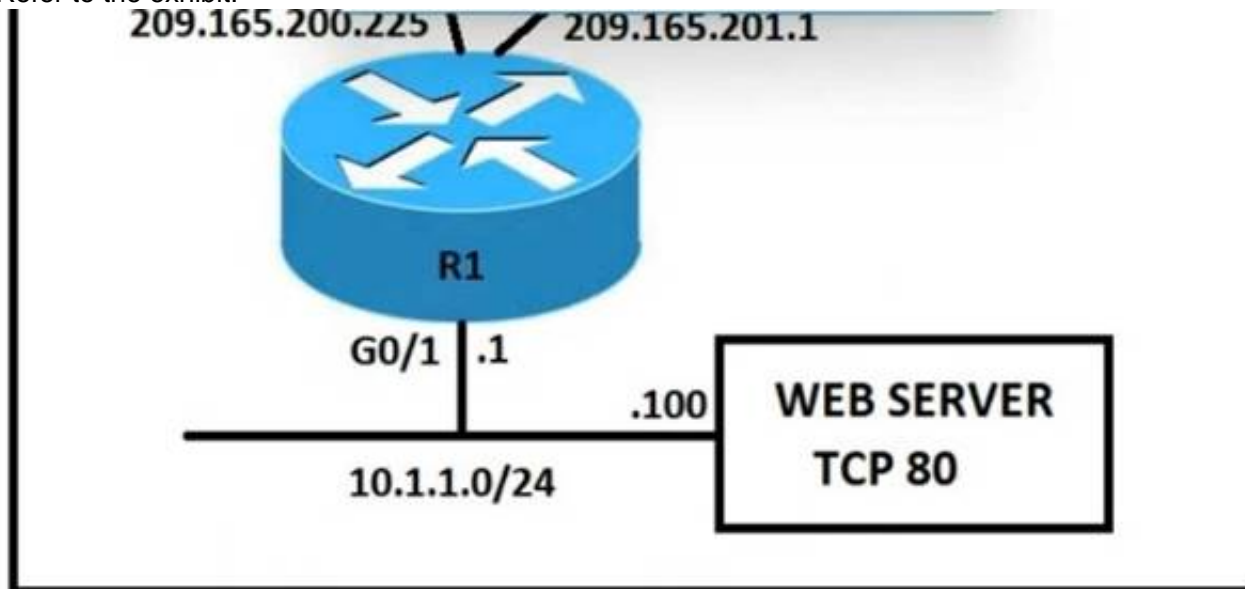
- A. with IP SLA
- B. ARP probing
- C. using BFD
- D. with OMP

Answer: C

NEW QUESTION 81

- (Topic 2)

Refer to the exhibit.



An engineer must configure static NAT on R1 to allow users HTTP access to the web server on TCP port 80. The web server must be reachable through ISP 1 and ISP 2. Which command set should be applied to R1 to fulfill these requirements?

- A. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 extendable ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80 extendable
- B. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80
- C. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80
- D. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 no-alias ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80 no-alias

Answer: B

NEW QUESTION 84

- (Topic 2)

Refer to the exhibit.

```
R1#show run | b router ospf
router ospf 1
network 192.168.10.0 0.0.0.255 area 0

R1#show run | b interface loopback0
interface loopback0
ip address 192.168.10.50 255.255.255.0
```

R2 is the neighboring router of R1. R2 receives an advertisement for network 192.168.10.50/32. Which configuration should be applied for the subnet to be advertised with the original /24 netmask?

- A)


```
R1(config)#router ospf 1
R1(config-router)#network 192.168.10.0 255.255.255.0 area 0
```

- B)


```
R1(config)#interface loopback0
R1(config-if)#ip ospf 1 area 0
```

C)

```
R1(config)# interface loopback0
R1(config-if)# ip ospf network point-to-point
```

D)

```
R1(config)# interface loopback0
R1(config-if)# ip ospf network non-broadcast
```

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

Answer: C

NEW QUESTION 89

- (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 93

- (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 97

- (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 101

- (Topic 2)

Which method is used by an AP to join HA controllers and is configured in NVRAM?

- A. stored WLC information
- B. DNS
- C. IP Helper Addresses
- D. Primary/Secondary/Tertiary/Backup

Answer: A

Explanation:

An AP can be “primed” with up to three controllers—a primary, a secondary, and a tertiary. These are stored in nonvolatile memory so that the AP can remember them after a reboot or power failure.

NEW QUESTION 106

- (Topic 2)

Refer to the exhibit.

```
import ncclient

with ncclient.manager.connect(host='192.168.1.1', port=830, username='root',
                             password='teset123!', allow_agent=False) as m:
    print(m.get_config('running').data_xml)
```

After running the code in the exhibit. Which step reduces the amount of data that NETCONF server returns to the NETCONF client, to only the interface's configuration?

- A. Create an XML filter as a string and pass it to get_config() method as an argument
- B. Use the txml library to parse the data returned by the NETCONF server for the interface's configuration
- C. Create a JSON filter as a string and pass it to the get_config() method as an argument
- D. Use the JSON library to parse the data returned by the NETCONF server for the interface's configuration

Answer: D

NEW QUESTION 110

DRAG DROP - (Topic 2)

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

summaries can be created anywhere in the IGP topology

uses areas to segment a network

summaries can be created in specific parts of the IGP topology

OSPF

EIGRP

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

summaries can be created anywhere in the IGP topology

uses areas to segment a network

summaries can be created in specific parts of the IGP topology

OSPF

summaries can be created anywhere in the IGP topology

uses areas to segment a network

EIGRP

summaries can be created in specific parts of the IGP topology

NEW QUESTION 111

DRAG DROP - (Topic 2)

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

easy to scale the capacity up and down	On-Premises
infrastructure requires large and regular investments	
highly agile	Cloud
highly customizable	

- A. Mastered
 B. Not Mastered

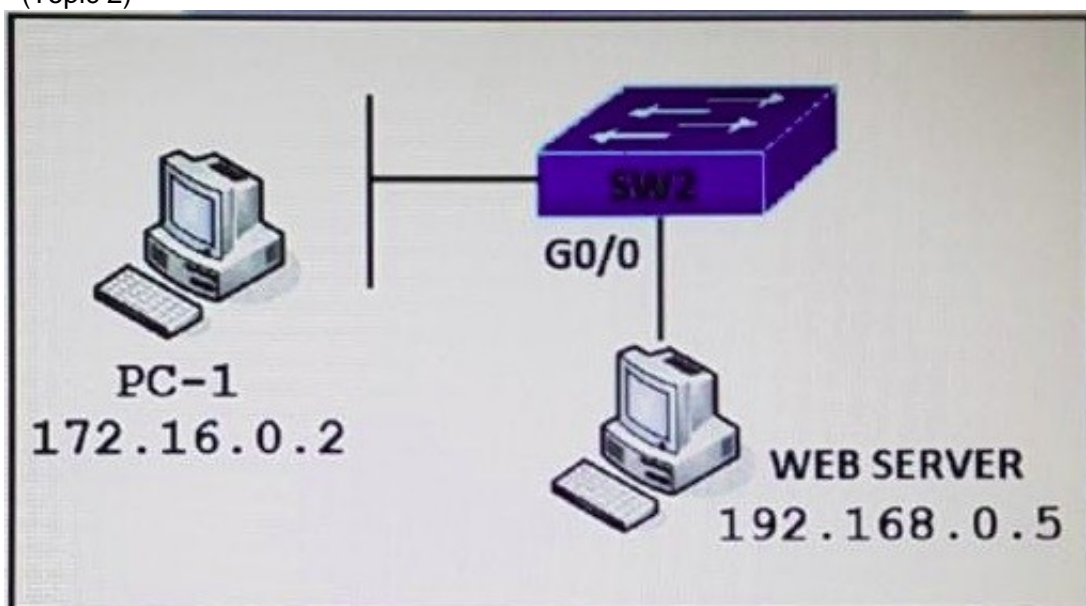
Answer: A

Explanation:

easy to scale the capacity up and down	On-Premises
infrastructure requires large and regular investments	
highly agile	Cloud
highly customizable	

NEW QUESTION 114

- (Topic 2)



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

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

Answer: C

Explanation:

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

NEW QUESTION 115

- (Topic 2)

Refer to the exhibit.


```
Switch1# show interfaces trunk
! Output omitted for brevity
Port Mode Encapsulation Status Native
Gi1/0/20 auto 802.1q trunking 10

Port Vlans allowed on trunk
Gi1/0/20 1-4094

Switch2# show interfaces trunk
! Output omitted for brevity
Port Mode Encapsulation Status Native
Gi1/0/20 auto 802.1q trunking 10

Port Vlans allowed on trunk
Gi1/0/20 1-4094
```

The trunk does not work over the back-to-back link between Switch1 interface Gig1/0/20 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 120

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

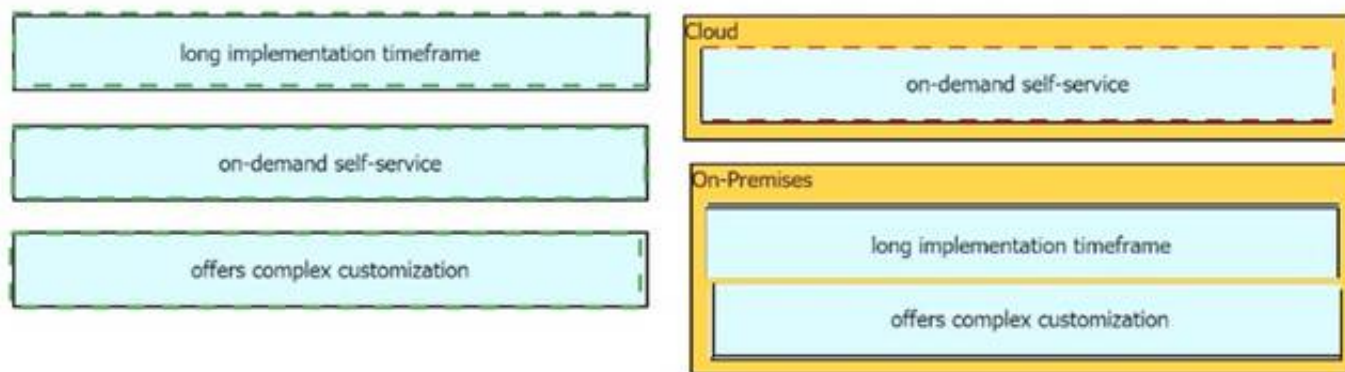
Cloud

On-Premises

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 124

- (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 128

- (Topic 2)

How are map-register messages sent in a LISP deployment?

- A. egress tunnel routers to map resolvers to determine the appropriate egress tunnel router
- B. ingress tunnel routers to map servers to determine the appropriate egress tunnel router
- C. egress tunnel routers to map servers to determine the appropriate egress tunnel router
- D. ingress tunnel routers to map resolvers to determine the appropriate egress tunnel router

Answer: C

Explanation:

During operation, an Egress Tunnel Router (ETR) sends periodic Map- Register messages to all its configured map servers.

NEW QUESTION 131

- (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 135

- (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 140

- (Topic 2)
Refer to the exhibit.

```
Switch1#show lacp internal
```

Flags: S - Device is requesting Slow LACPDUs
F - Device is requesting Fast LACPDUs
A - Device is in Active mode P - Device is in Passive mode

Channel group 1

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

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

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

Answer: D

NEW QUESTION 144

- (Topic 2)
Which two parameters are examples of a QoS traffic descriptor? (Choose two)

- A. MPLS EXP bits
- B. bandwidth
- C. DSCP
- D. ToS
- E. packet size

Answer: AC

NEW QUESTION 149

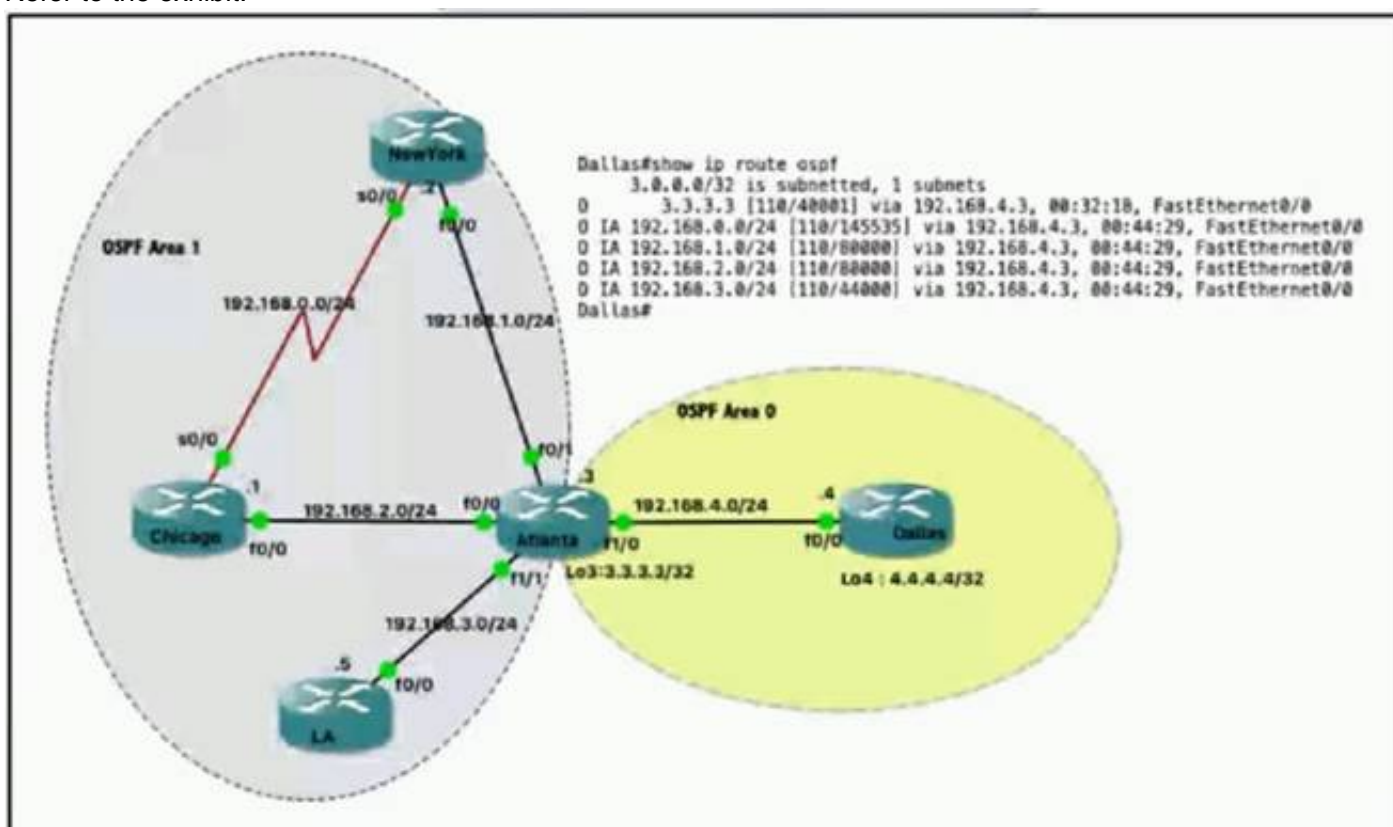
- (Topic 2)
A network monitoring system uses SNMP polling to record the statistics of router interfaces The SNMP queries work as expected until an engineer installs a new interface and reloads the router After this action, all SNMP queries for the router fail What is the cause of this issue?

- 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 151

- (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?

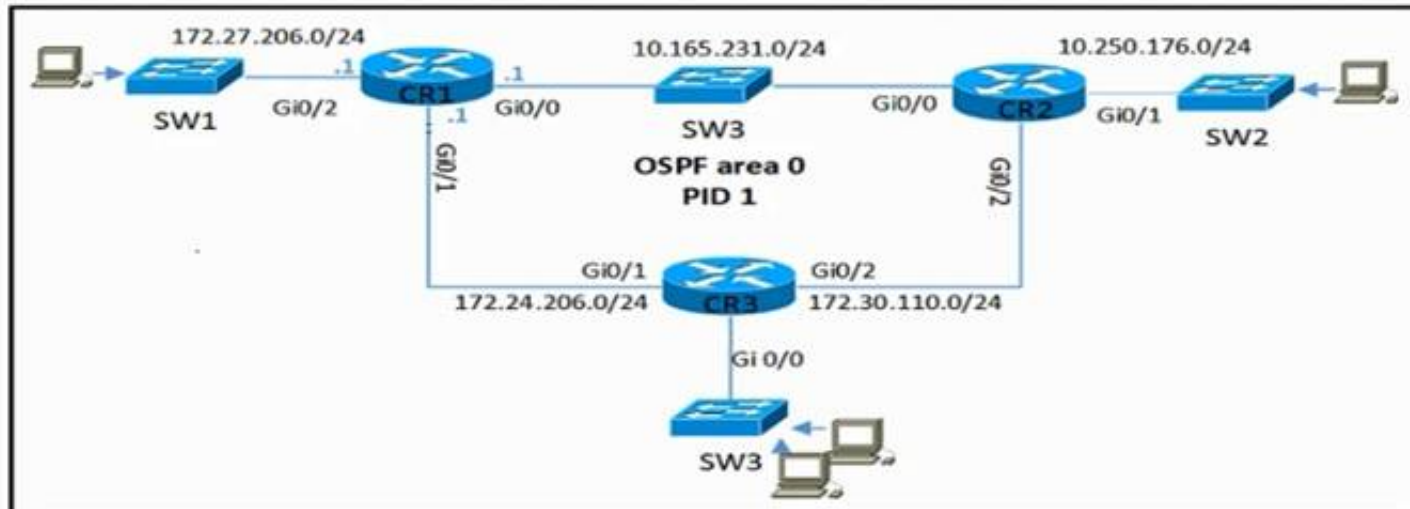
- A. Atlanta(config-route)#area 0 range 192.168.0.0 255.255.248.0
- B. Atlanta(config-route)#area 0 range 192.168.0.0 255.255.252.0
- C. Atlanta(config-route)#area 1 range 192.168.0.0 255.255.252.0
- D. Atlanta(config-route)#area 1 range 192.168.0.0 255.255.248.0

Answer: C

NEW QUESTION 152

- (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 153

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.	On-Premises
This model improves elasticity of resources.	
This model enables complete control of the servers.	Cloud
This model reduces management overhead by leveraging provider-managed resources.	

- A. Mastered
 B. Not Mastered

Answer: A

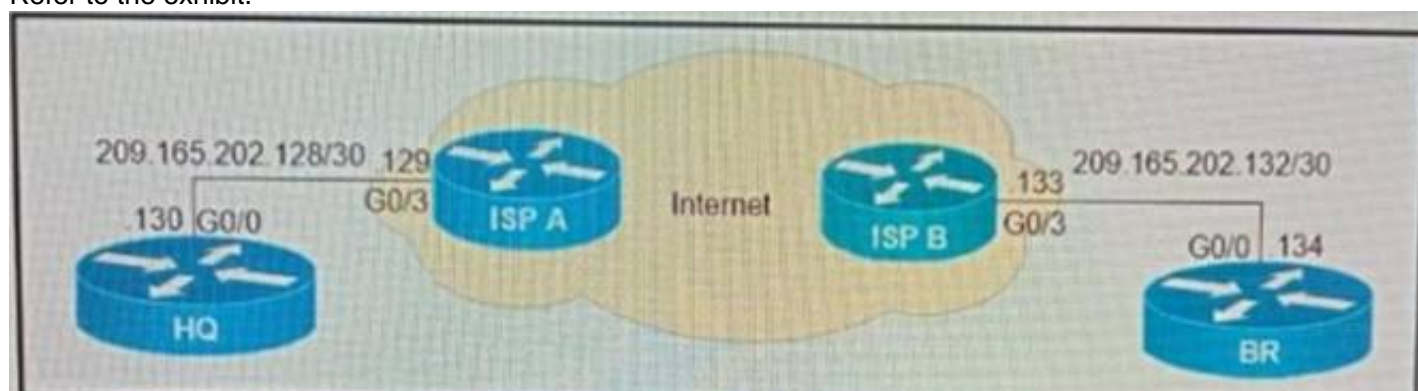
Explanation:

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

NEW QUESTION 156

- (Topic 2)

Refer to the exhibit.



What is the effect of these commands on the BR and HQ tunnel interfaces?

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

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

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

Answer: B

NEW QUESTION 160

- (Topic 2)

Which technology uses network traffic telemetry, contextual information, and file reputation to provide insight into cyber threats?

- A. threat defense
 B. security services
 C. security intelligence
 D. segmentation

Answer: C

NEW QUESTION 162

- (Topic 2)

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

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

Answer: C

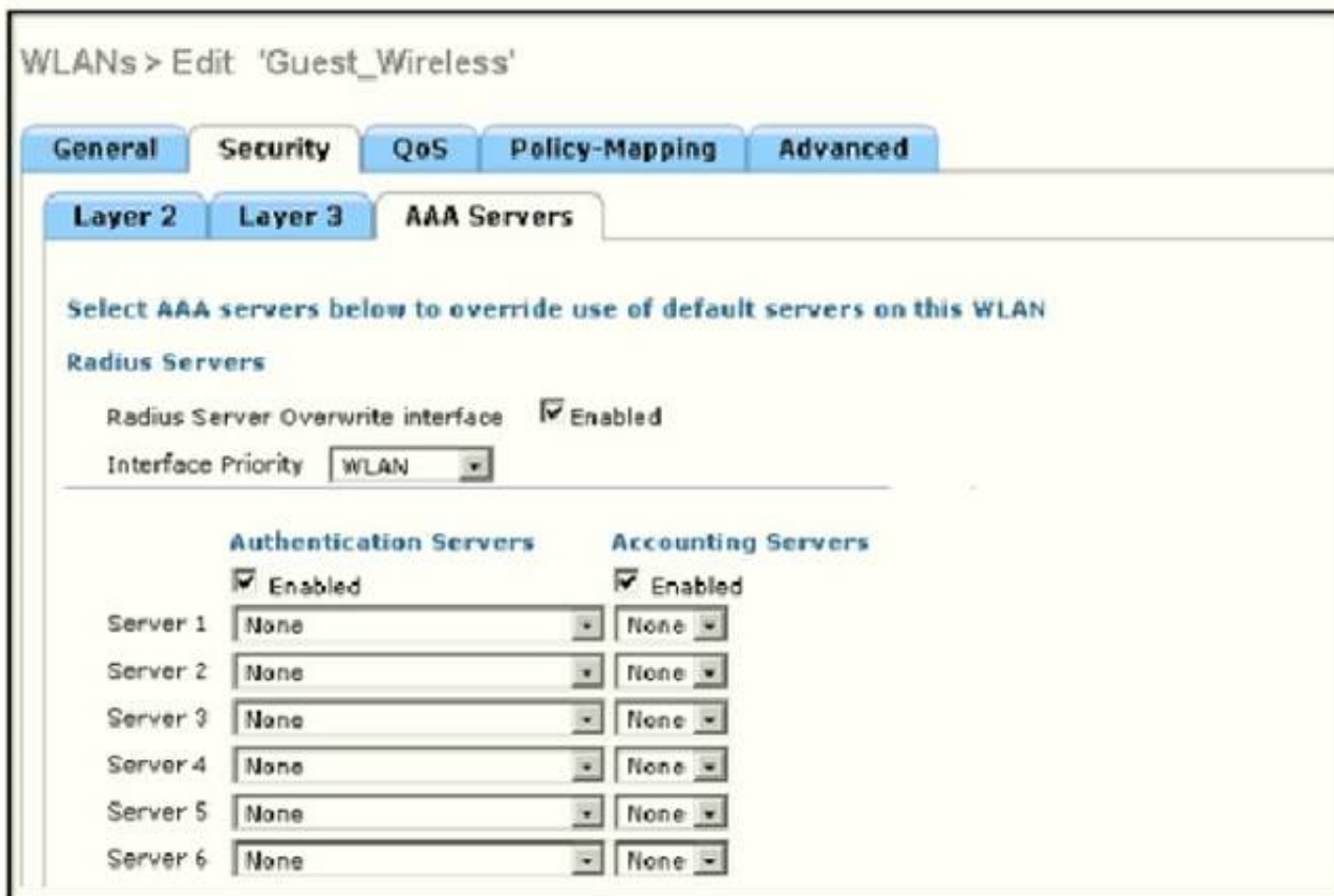
Explanation:

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

NEW QUESTION 165

- (Topic 1)

Refer to the exhibit.



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

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

Answer: A

NEW QUESTION 166

- (Topic 1)

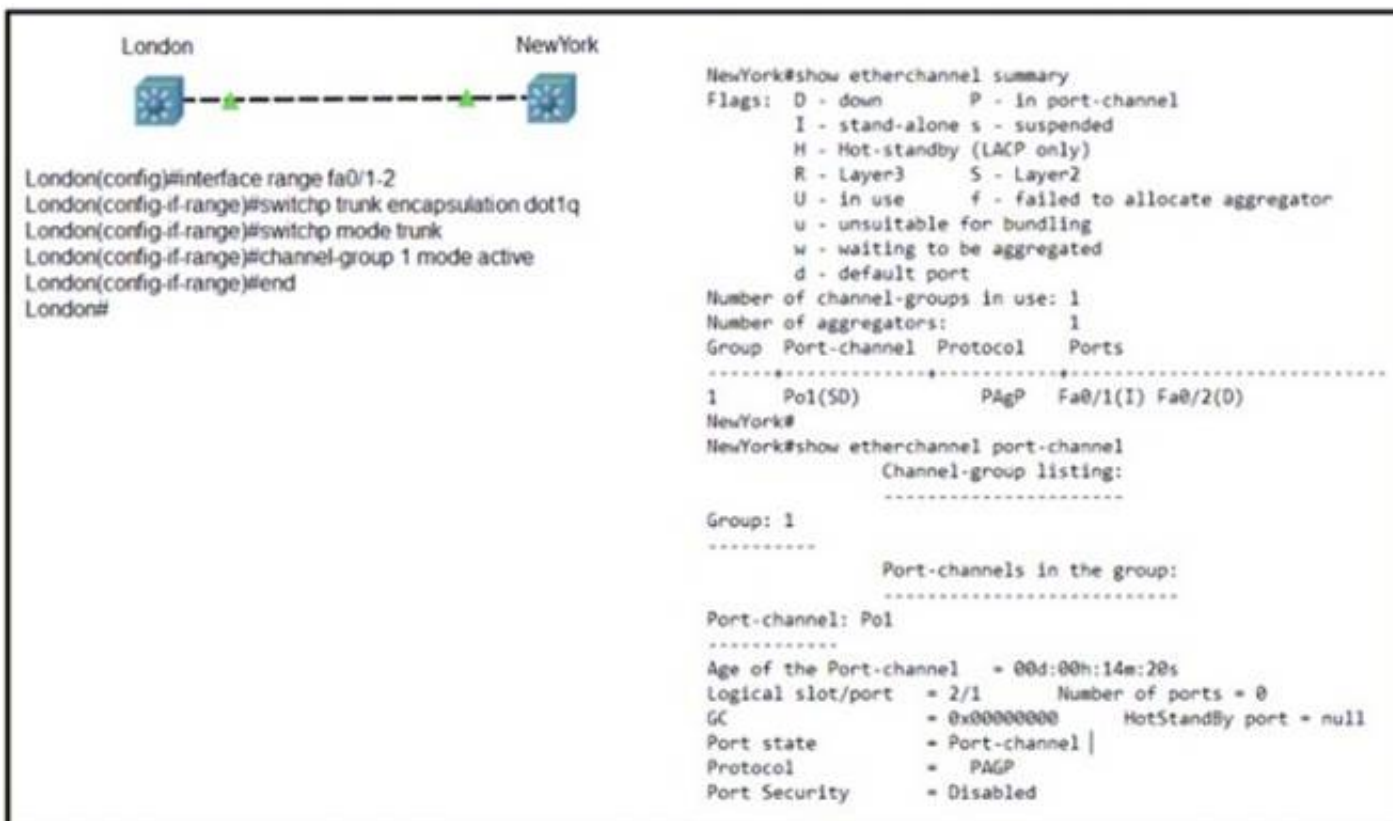
Which component of the Cisco Cyber Threat Defense solution provides user and flow context analysis?

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

Answer: B

NEW QUESTION 170

- (Topic 1)



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 175

- (Topic 1)

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

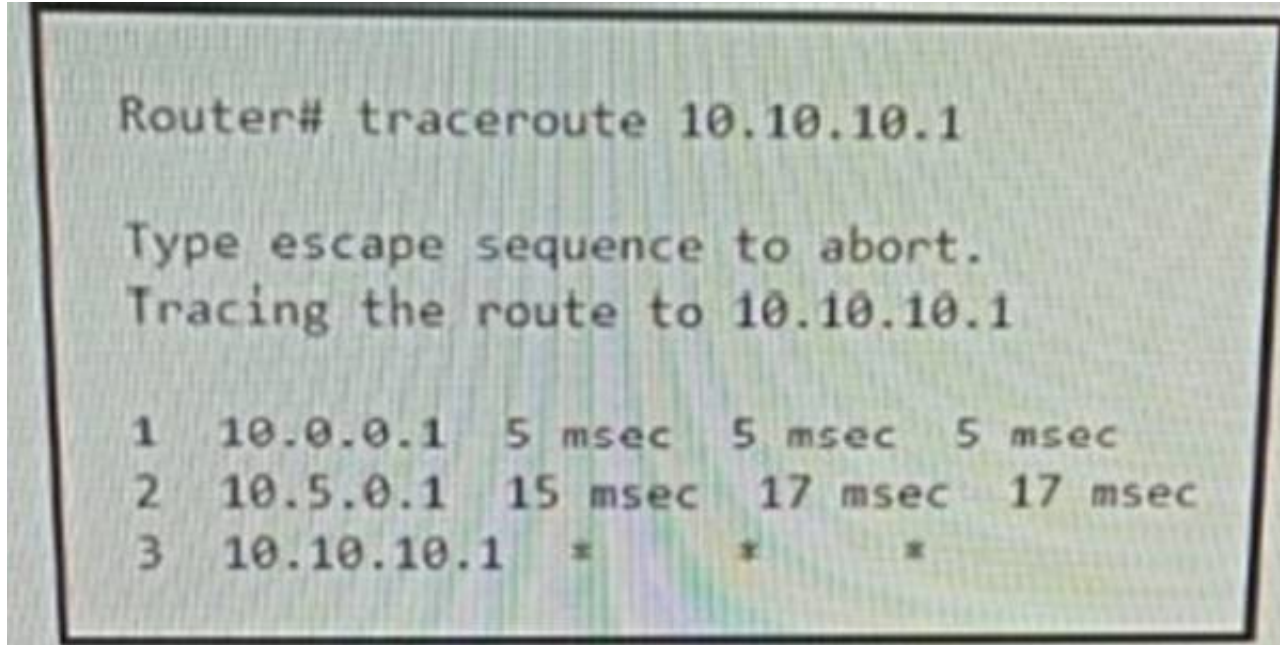
- A. MSDP depends on BGP or multiprotocol BGP for mterdomam operation
- B. MSDP SA request messages are used to request a list of active sources for a specific group
- C. SDP allows a rendezvous point to dynamically discover active sources outside of its domain
- D. MSDP messages are used to advertise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

Answer: A

NEW QUESTION 177

- (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 179

- (Topic 1)

What is a consideration when designing a Cisco SD-Access underlay network?

- A. End user subnets and endpoints are part of the underlay network.
- B. The underlay switches provide endpoint physical connectivity for users.
- C. Static routing is a requirement,
- D. It must support IPv4 and IPv6 underlay networks

Answer: B

Explanation:

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

NEW QUESTION 183

- (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 184

- (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

NEW QUESTION 185

- (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

NEW QUESTION 190

- (Topic 1)

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

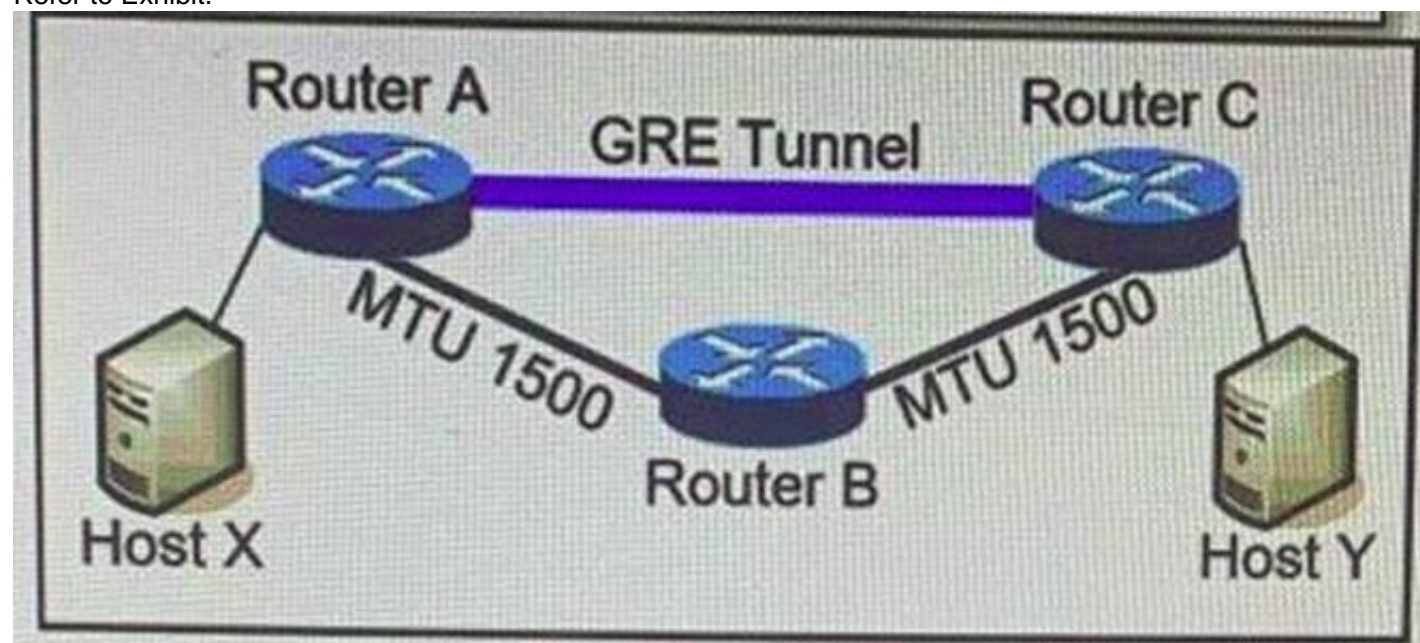
- A. list of ordered statements that define user access policies
- B. set of statements that defines how routing is performed
- C. set of rules that governs nodes authentication within the cloud
- D. list of enabled services for all nodes within the cloud

Answer: B

NEW QUESTION 191

- (Topic 1)

Refer to Exhibit.



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

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

Answer: D

Explanation:

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

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

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

NEW QUESTION 192

- (Topic 1)

Refer to the exhibit.

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

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

- A. ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 globalip route vrf Customer 192.168.1.200 255.255.255.255 192.168.1.1 globalip route 192.168.1.0 255.255.255.0 Vlan1Oip route 172.16.1.0 255.255.255.0 Vlan20
- B. ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customer2ip route vrf Customer 192.168.1.200 255.255.255.255 192.168.1.1 Customer1
- C. ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customerlip route vrf Customer 192.168.1.200 255.255.255.255 192.168.1.1 Customer2
- D. ip route vrf Customer1 172.16.1.1 255.255.255.255 172.16.1.1 globalip route vrf Customer 192.168.1.200 255.255.255.0 192.168.1.1 globalip route 192.168.1.0 255.255.255.0 Vlan1Oip route 172.16.1.0 255.255.255.0 Vlan20

Answer: A

NEW QUESTION 195

- (Topic 1)

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

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

Answer: D

NEW QUESTION 200

- (Topic 1)

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

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

Answer: B

NEW QUESTION 203

- (Topic 1)

Which data is properly formatted with JSON?

A)

```
{
    "name": "Peter",
    "age": "25",
    "likesJson": true,
    "characteristics": ["small", "strong", 18]
}
```

B)

```
{
    "name": "Peter",
    "age": "25",
    "likesJson": true,
    "characteristics": ["small", "strong", "18"],
}
```

C)

```
{
    "name":"Peter"
    "age":"25"
    "likesJson":true
    "characteristics":["small","strong",18]
}
```

D)

```
{
    "name": Peter,
    "age": 25,
    "likesJson": true,
    "characteristics": ["small", "strong", "18"],
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

NEW QUESTION 206

- (Topic 1)

What are two characteristics of VXLAN? (Choose two)

A. It uses VTEPs to encapsulate and decapsulate frames.

B. It has a 12-bit network identifier

C. It allows for up to 16 million VXLAN segments

D. It lacks support for host mobility

E. It extends Layer 2 and Layer 3 overlay networks over a Layer 2 underlay.

Answer: AC

NEW QUESTION 210

- (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 ) FAqP 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 213

- (Topic 1)

An engineer must provide wireless converge in a square office. The engineer has only one AP and believes that it should be placed it in the middle of the room. Which antenna type should the engineer use?

- A. directional
- B. polarized
- C. Yagi
- D. omnidirectional

Answer: D

NEW QUESTION 215

- (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 216

- (Topic 1)

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

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

Answer: B

NEW QUESTION 221

- (Topic 1)

Which characteristic distinguishes Ansible from Chef?

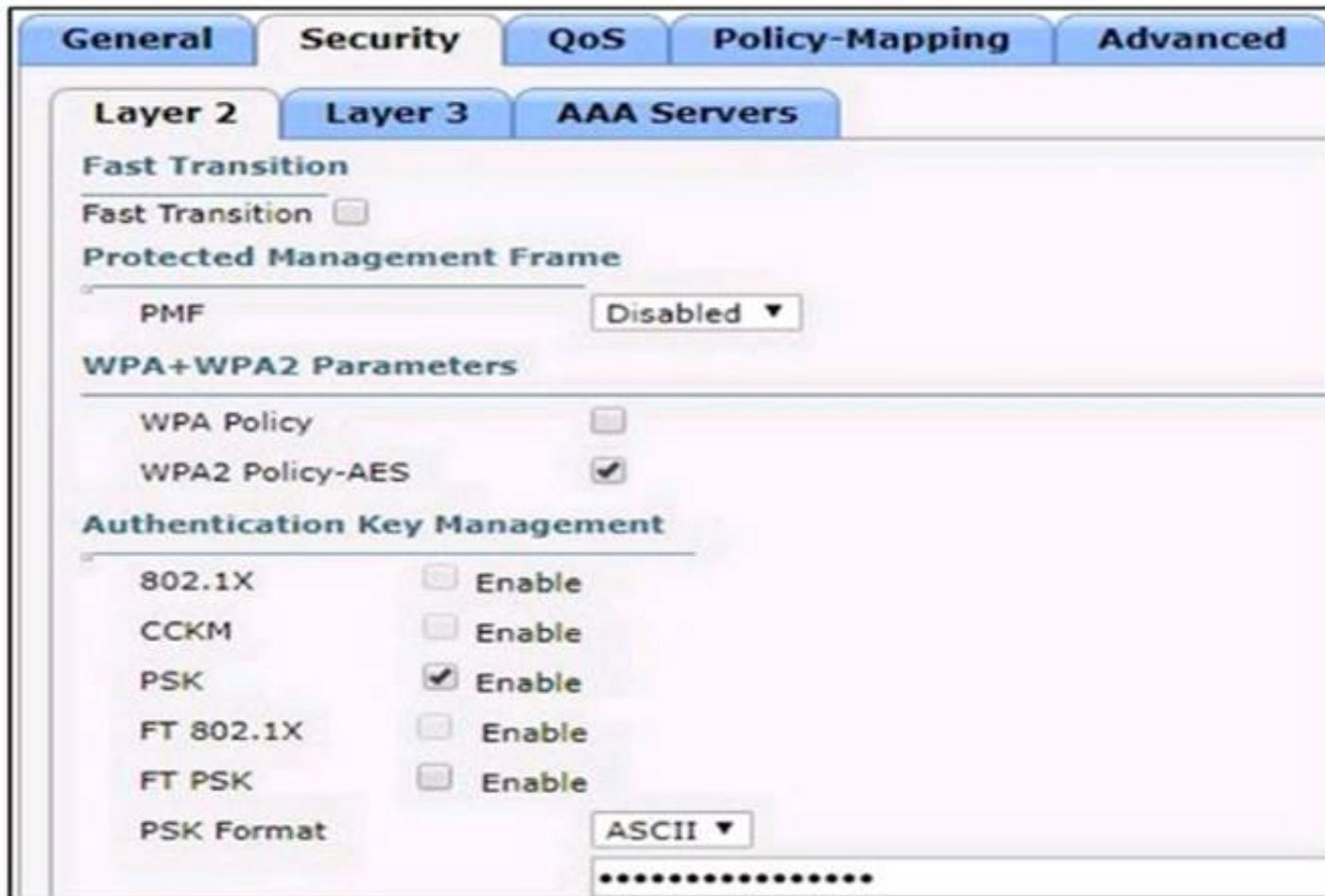
- A. Ansible lacks redundancy support for the master serve
- B. Chef runs two masters in an active/active mode.
- C. Ansible uses Ruby to manage configuration
- D. Chef uses YAML to manage configurations.
- E. Ansible pushes the configuration to the clien
- F. Chef client pulls the configuration from the server.
- G. The Ansible server can run on Linux, Unix or Window
- H. The Chef server must run on Linux or Unix.

Answer: C

NEW QUESTION 223

- (Topic 1)

Refer to the exhibit.



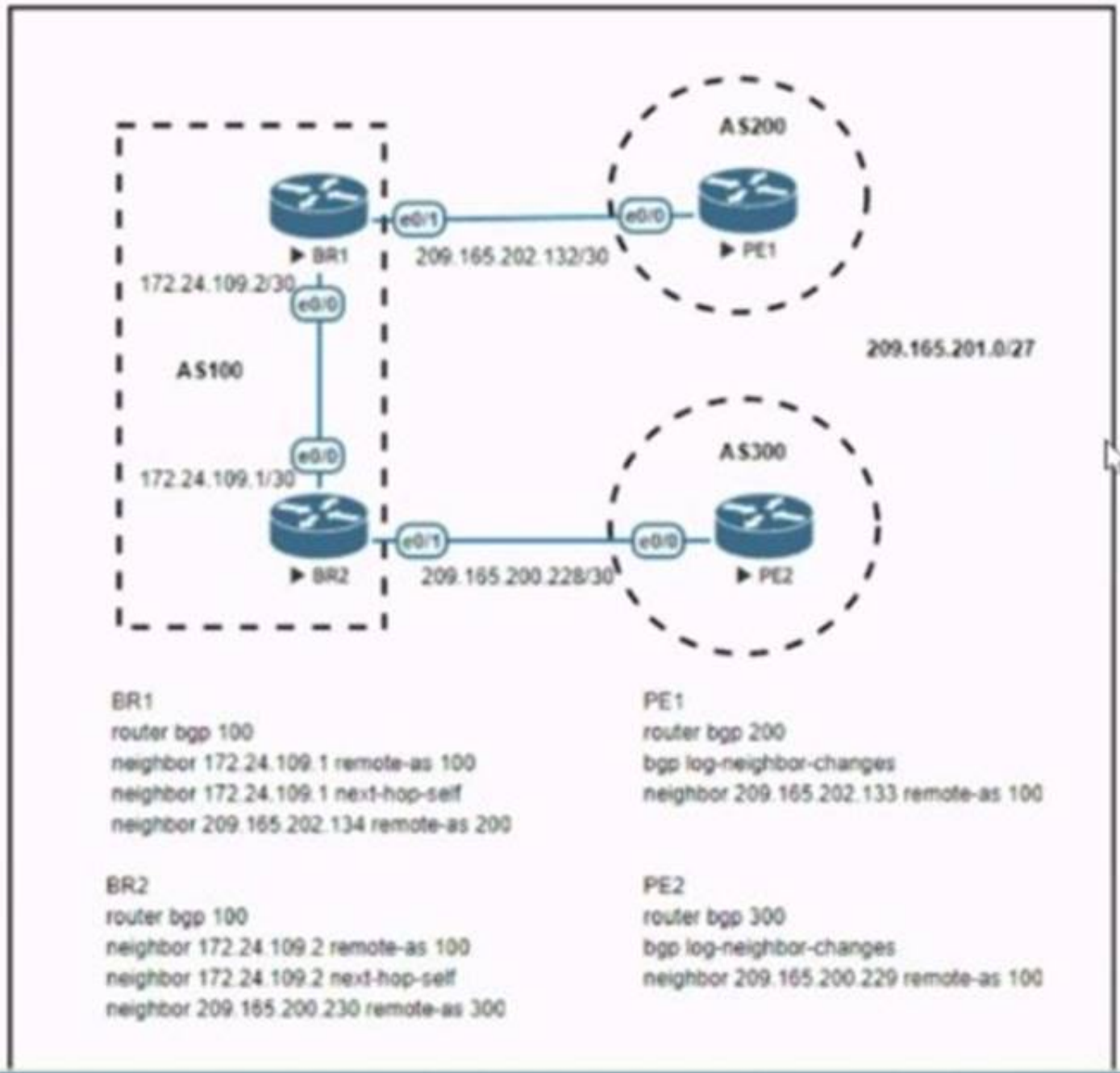
Based on the configuration in this WLAN security setting, Which method can a client use to authenticate to the network?

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

Answer: A

NEW QUESTION 225

- (Topic 1)



```
BR2#sh ip route | i 209.165.201.0
209.165.201.0/27 is subnetted, 1 subnets
B 209.165.201.0 [20/0] via 209.165.200.230, 00:00:17
```

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:

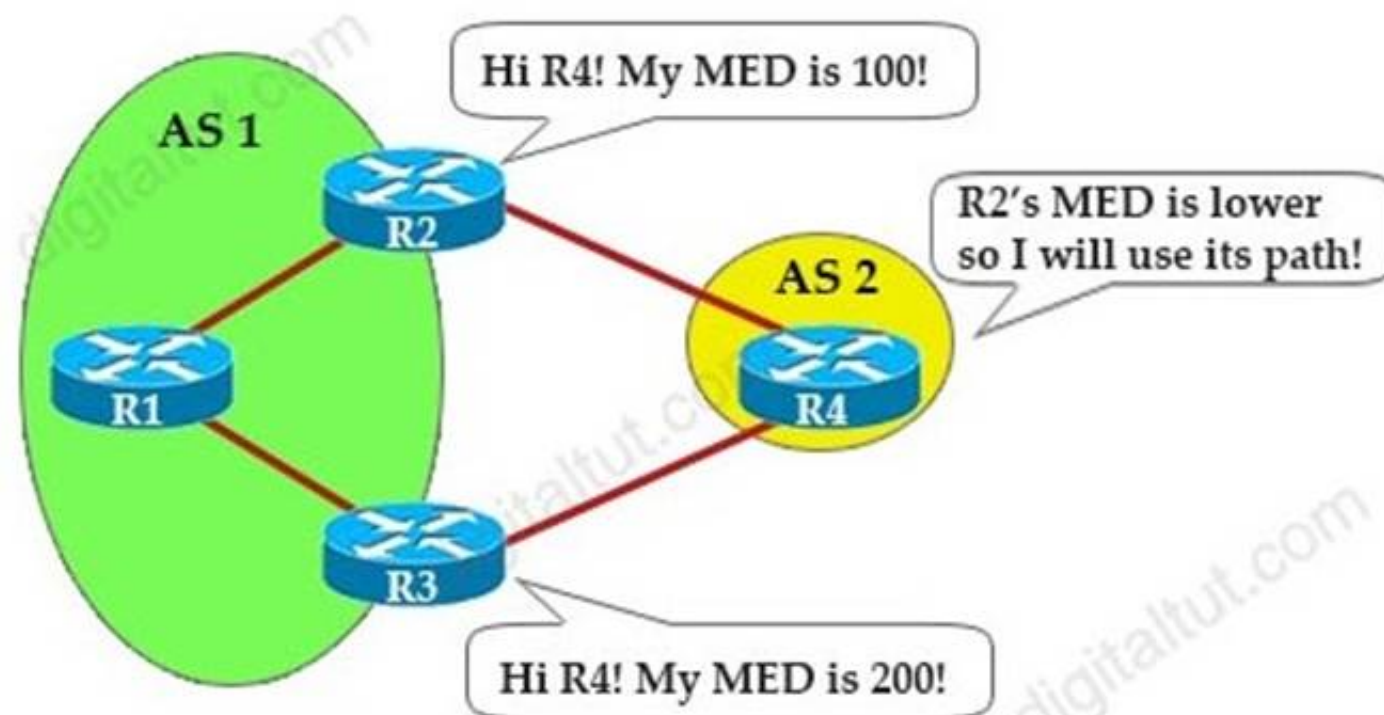


Diagrama Descripción generada automáticamenteMED Attribute:+ Optional nontransitive attribute (nontransitive means that we can only advertise MED to routers that are one AS away)+ Sent through ASes to external BGP neighbors+ Lower value is preferred (it can be considered the external metric of a route)+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

NEW QUESTION 228

- (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 autocmd keyword to the username command
- D. Add the autocmd keyword to the aaa authentication command

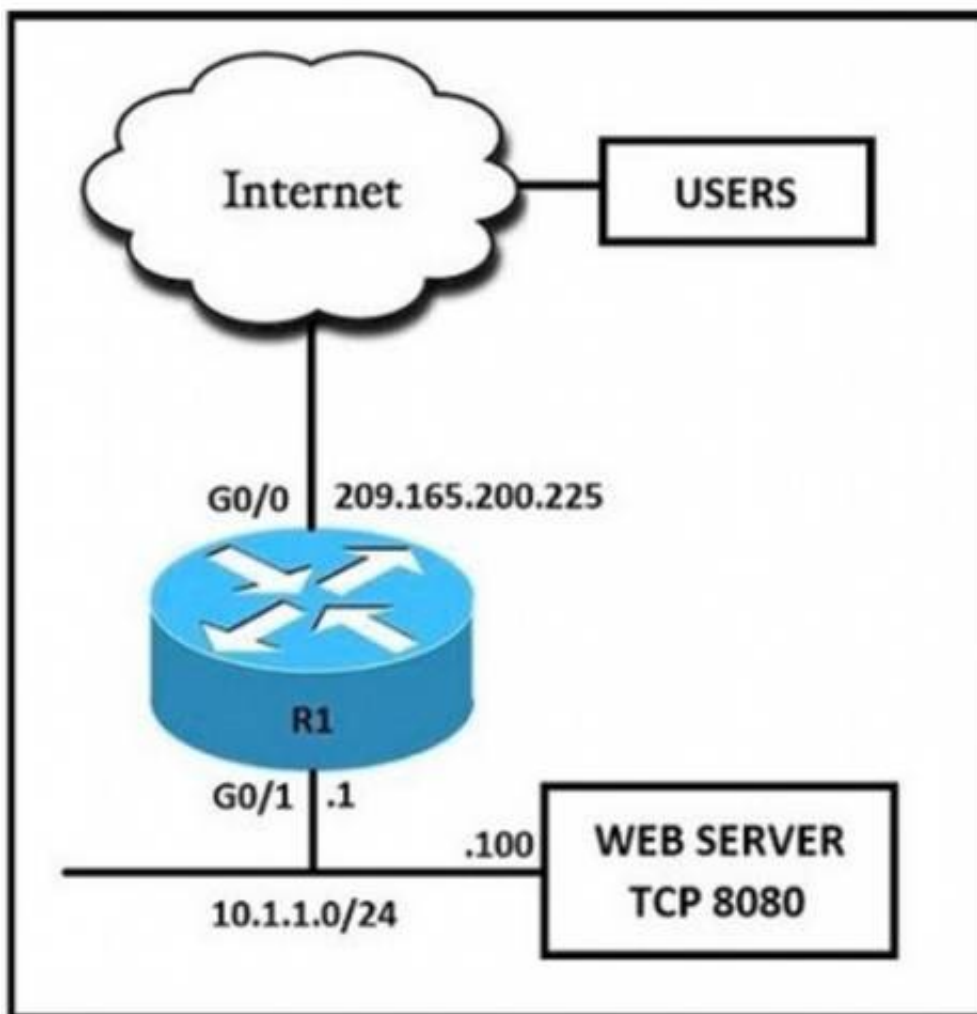
Answer: C

Explanation:

The autocmd 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 autocmd keyword must be the last option on the line. In this specific question, we have to enter this line username CCNP autocmd show running-config.

NEW QUESTION 229

- (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
```

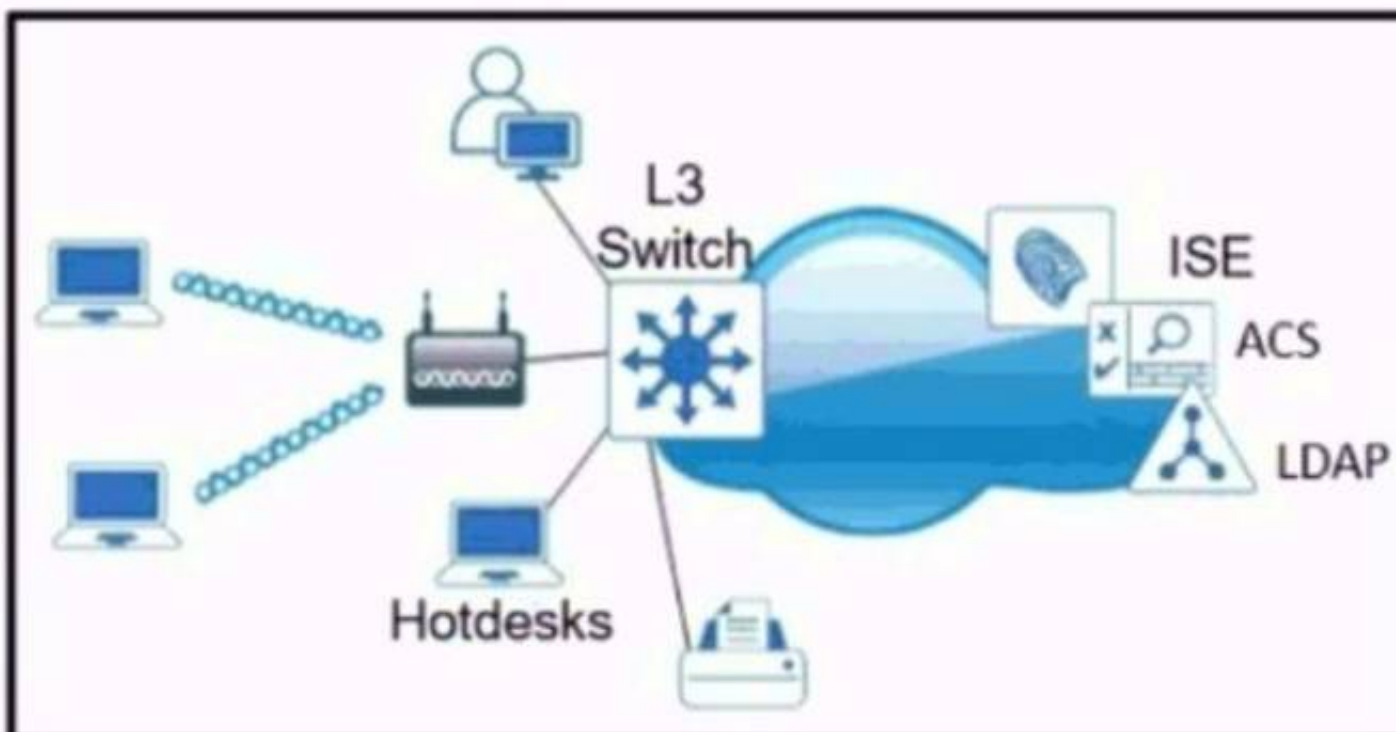
```
interface G0/1
ip address 10.1.1.1 255.255.255.0
ip nat outside
```

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

Answer: B

NEW QUESTION 233

- (Topic 1)



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

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

Answer: B

NEW QUESTION 237

- (Topic 1)

```
Switch2#
01:25:08: %PM-4-ERR_DISABLE: channel-misconfig error detected on
Fa0/23, putting Fa0/23 in err-disable
state
01:25:08: %PM-4-ERR_DISABLE: channel-misconfig error detected on
Fa0/24, putting Fa0/24 in err-disable
state
Switch2#

Switch1#show etherchannel summary

!output omitted

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
1      Po2(SD)          LACP      Fa1/0/23 (D)

Switch2#show etherchannel summary

!output omitted

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
1      Po1(SD)          -         Fa0/23 (D)  Fa0/24 (D)
```

Refer to the exhibit. An engineer is configuring an EtherChannel between Switch1 and Switch2 and notices the console message on switch2. Based on the output, which action resolves this issue?

- A. Configure less member ports on Switch2.
- B. Configure the same port channel interface number on both switches
- C. Configure the same EtherChannel protocol on both switches
- D. Configure more member ports on Switch1.

Answer: C

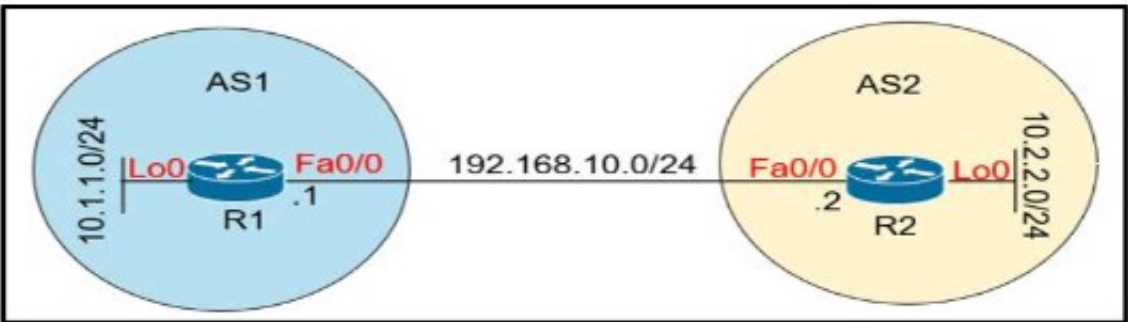
Explanation:

In this case, we are using your EtherChannel without a negotiation protocol on Switch2. 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 240

- (Topic 1)

Refer to the exhibit.



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

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

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

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

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

C)

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

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

D)

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

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

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

**Answer:** A

**Explanation:**

With BGP, we must advertise the correct network and subnet mask in the “network” command (in this case network 10.1.1.0/24 on R1 and network 10.2.2.0/24 on R2). BGP is very strict in the routing advertisements. In other words, BGP only advertises the network which exists exactly in the routing table. In this case, if you put the command “network x.x.0.0 mask 255.255.0.0” or “network x.0.0.0 mask 255.0.0.0” or “network x.x.x.x mask 255.255.255.255” then BGP will not advertise anything.

It is easy to establish eBGP neighborship via the direct link. But let's see what are required when we want to establish eBGP neighborship via their loopback interfaces. We will need two commands:  
+ the command “neighbor 10.1.1.1 ebgp-multihop 2” on R1 and “neighbor 10.2.2.2 ebgpmultihop 2” on R1. This command increases the TTL value to 2 so that BGP updates can reach the BGP neighbor which is two hops away.

```
+ Answer 'R1 (config) #router bgp 1
R1 (config-router) #neighbor 192.168.10.2 remote-as 2
R1 (config-router) #network 10.1.1.0 mask 255.255.255.0
R2 (config) #router bgp 2
R2 (config-router) #neighbor 192.168.10.1 remote-as 1
R2 (config-router) #network 10.2.2.0 mask 255.255.255.0
```

Quick Wireless Summary  
Cisco Access Points (APs) can operate in one of two modes: autonomous or lightweight

+ Autonomous: self-sufficient and standalone. Used for small wireless networks.

+ Lightweight: A Cisco lightweight AP (LAP) has to join a Wireless LAN Controller (WLC) to function. LAP and WLC communicate with each other via a logical pair of CAPWAP tunnels.

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

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

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

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

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

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

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

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

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



troubleshooting purposes.

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

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

#### NEW QUESTION 242

- (Topic 4)

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

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

**Answer: B**

#### NEW QUESTION 243

- (Topic 4)

A network administrator is designing a new network for a company that has frequent power spikes. The company wants to ensure that employees can the best solution for the administrator to recommend?

- A. Generator
- B. Cold site
- C. Redundant power supplies
- D. Uninterruptible power supply

**Answer: D**

#### Explanation:

This is because an uninterruptible power supply (UPS) is a device that provides backup power to a network device or a computer in case of a power outage or a power spike. A UPS can prevent data loss, corruption, or damage to the device by providing a smooth and continuous power supply. A UPS can also protect the device from power surges, brownouts, or voltage fluctuations. The source of this answer is the Cisco ENCOR v1.1 course, module 2, lesson 2.1: Implementing Device Hardening.

#### NEW QUESTION 247

- (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 249

- (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 252

- (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**

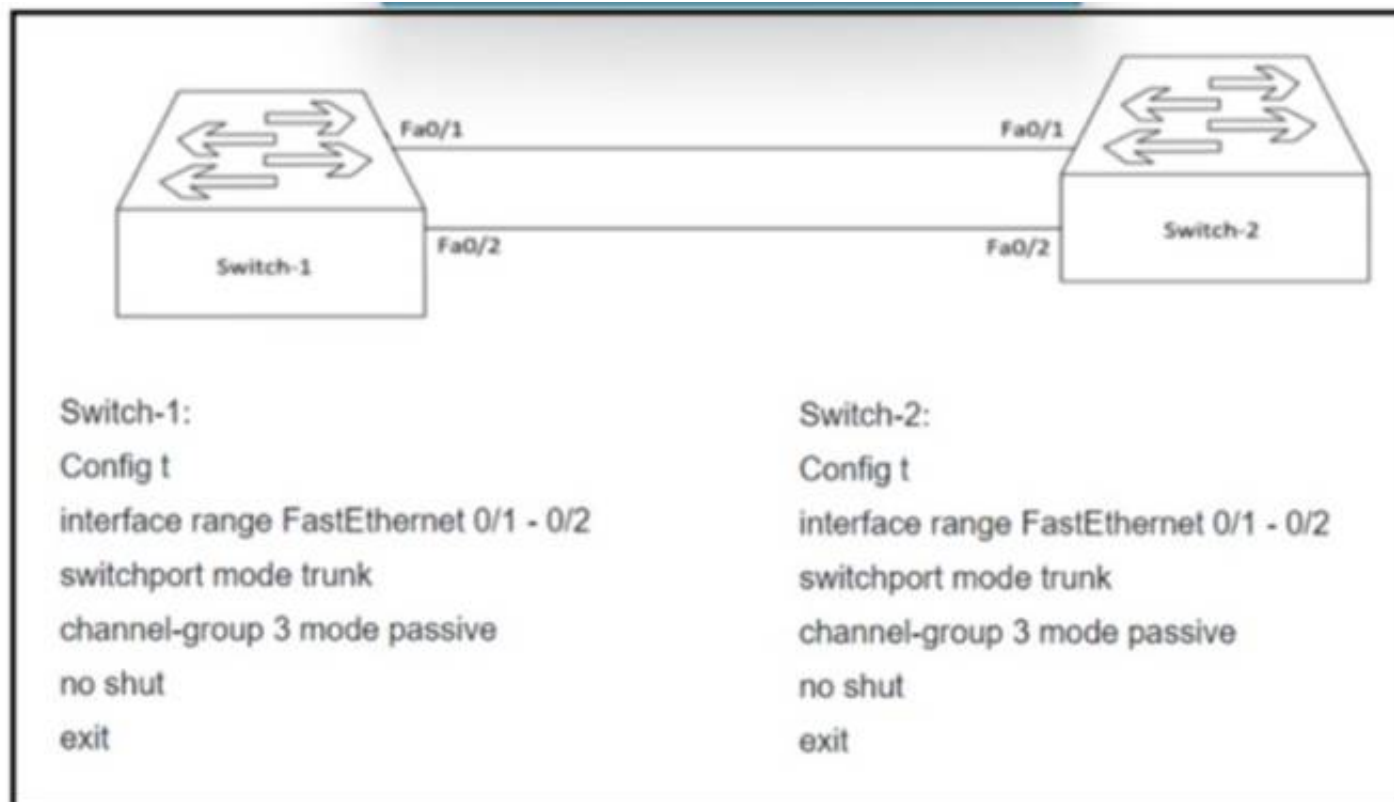
**Explanation:**

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 255**

- (Topic 4)

Refer to the exhibit.



An LACP port channel is configured between Switch-1 and Switch-2, but It falls to come up. Which action will resolve the issue?

- A. Configure Switch-1 with channel-group mode active
- B. Configure Switch-2 with channel-group mode desirable.
- C. Configure Switch-1 with channel-group mode on.
- D. Configure SwKch-2 with channel-group mode auto

**Answer: A**

**NEW QUESTION 259**

- (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 263**

- (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 266**

- (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 267

- (Topic 4)

Which of the following protocols has a default administrative distance value of 90?

- A. RIP
- B. EIGRP
- C. OSPF
- D. BGP

**Answer:** B

#### Explanation:

This is because EIGRP is an advanced distance vector routing protocol that uses a composite metric to calculate the best path to a destination. EIGRP has a default administrative distance value of 90, which means that it is more trustworthy than RIP (120) or OSPF (110), but less trustworthy than BGP (20). The source of this answer is the Cisco ENCOR v1.1 course, module 4, lesson 4.1: Implementing EIGRP.

#### NEW QUESTION 271

- (Topic 4)

What do Chef and Ansible have in common?

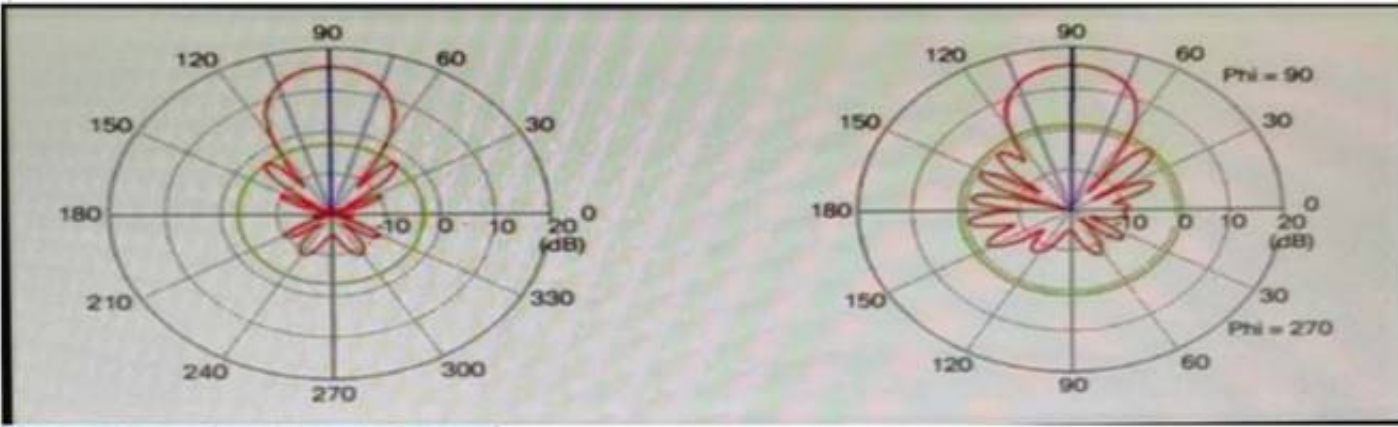
- A. They rely on a declarative approach.
- B. They rely on a procedural approach.
- C. They use YAML as their primary configuration syntax.
- D. They are clientless architectures.

**Answer:** B

#### NEW QUESTION 275

- (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 277

- (Topic 4)

```
<?xml version="1.0"?>
<nc:rpc message-id="101" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
 <nc:get>
 <nc:filter type="subtree">
 <native xmlns="http://cisco.com/ns/yang/netconf:ios">
 <interface>
 <GigabitEthernet>
 <name>1</name>
 <ip></ip>
 </GigabitEthernet>
 </interface>
 </native>
 </nc:filter>
 </nc:get>
</nc:rpc>
]]>]]>
```

Refer to me exhibit. The NETCONF object is sent to a Cisco IOS XE switch. What is me purpose of the object?

- A. view the configuration of all GigabitEthernet interfaces.
- B. Discover the IP address of interface GigabitEthernet.
- C. Set the description of interface GigabitEthernet1 to \*1\*.
- D. Remove the IP address from interface GigabitEthernet1.

**Answer:** A

#### NEW QUESTION 282

- (Topic 4)

```
monitor session 11 type erspan-source
source interface GigabitEthernet3
destination
erspan-id 12
ip address 10.10.10.10
origin ip address 10.100.10.10
```

Refer to the exhibit. Which command set completes the ERSPAN session configuration?

- ☐ monitor session 12 type erspan-destination  
destination interface GigabitEthernet4  
source  
erspan-id 12  
ip address 10.10.10.10
- ☐ monitor session 11 type erspan-destination  
destination interface GigabitEthernet4  
source  
erspan-id 12  
ip address 10.100.10.10
- ☐ monitor session 11 type erspan-destination  
destination interface GigabitEthernet4  
source  
erspan-id 11  
ip address 10.10.10.10
- ☐ monitor session 12 type erspan-destination  
destination interface GigabitEthernet4  
source  
erspan-id 11  
ip address 10.10.10.10

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

**Answer:** A

#### NEW QUESTION 285

- (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 289

- (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 291

- (Topic 4)

What is a characteristics of Cisco SD-WAN?

- A. operates over DTLS/TLS authenticated and secured tunnels
- B. requires manual secure tunnel configuration
- C. uses unique per-device feature templates
- D. uses control connections between routers

**Answer:** A



**NEW QUESTION 295**

- (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 298**

- (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 wth 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 302**

- (Topic 4)

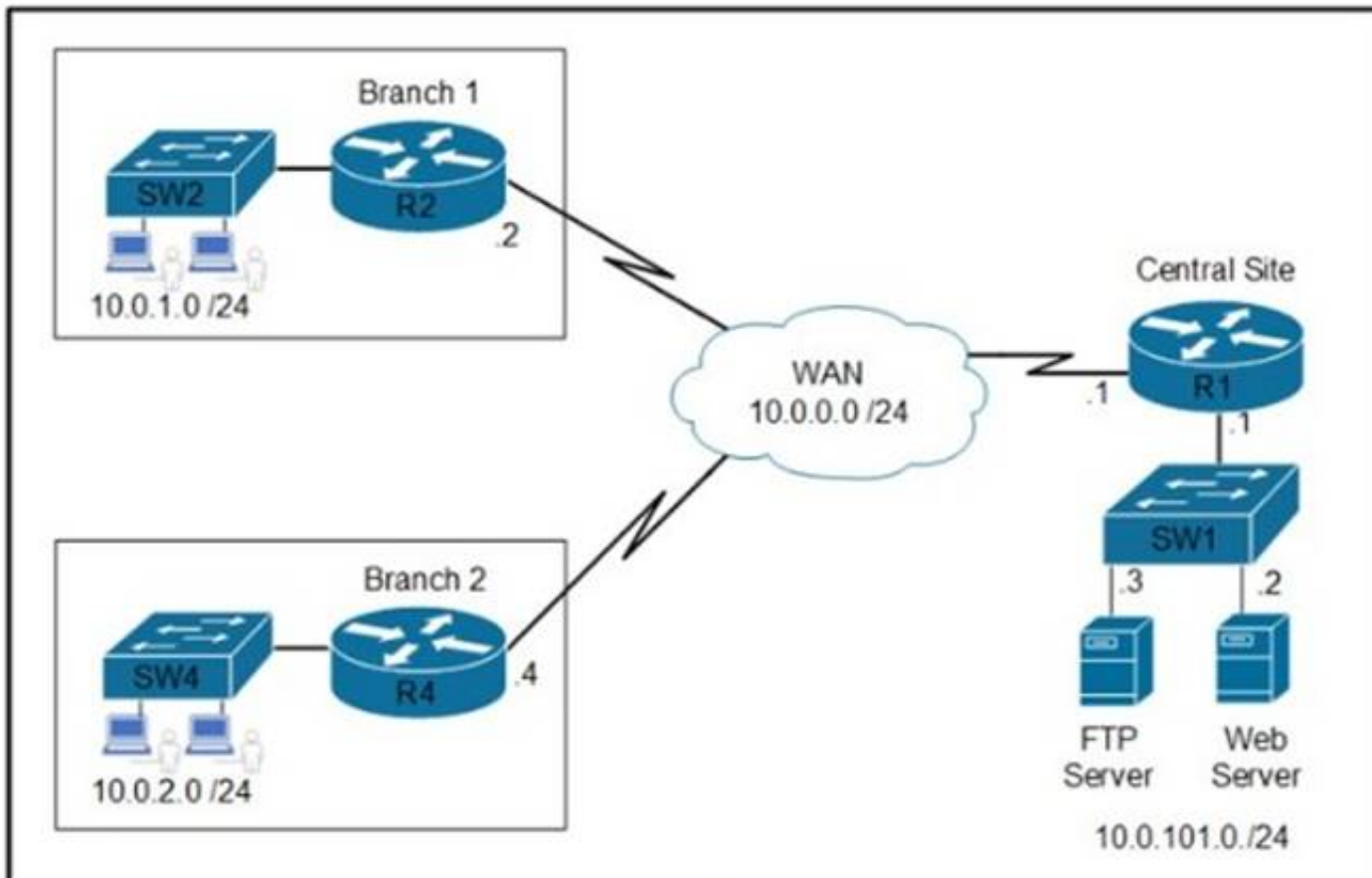
Which solution simplifies management ot secure access to network resources?

- 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 305**

- (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 310

- (Topic 4)

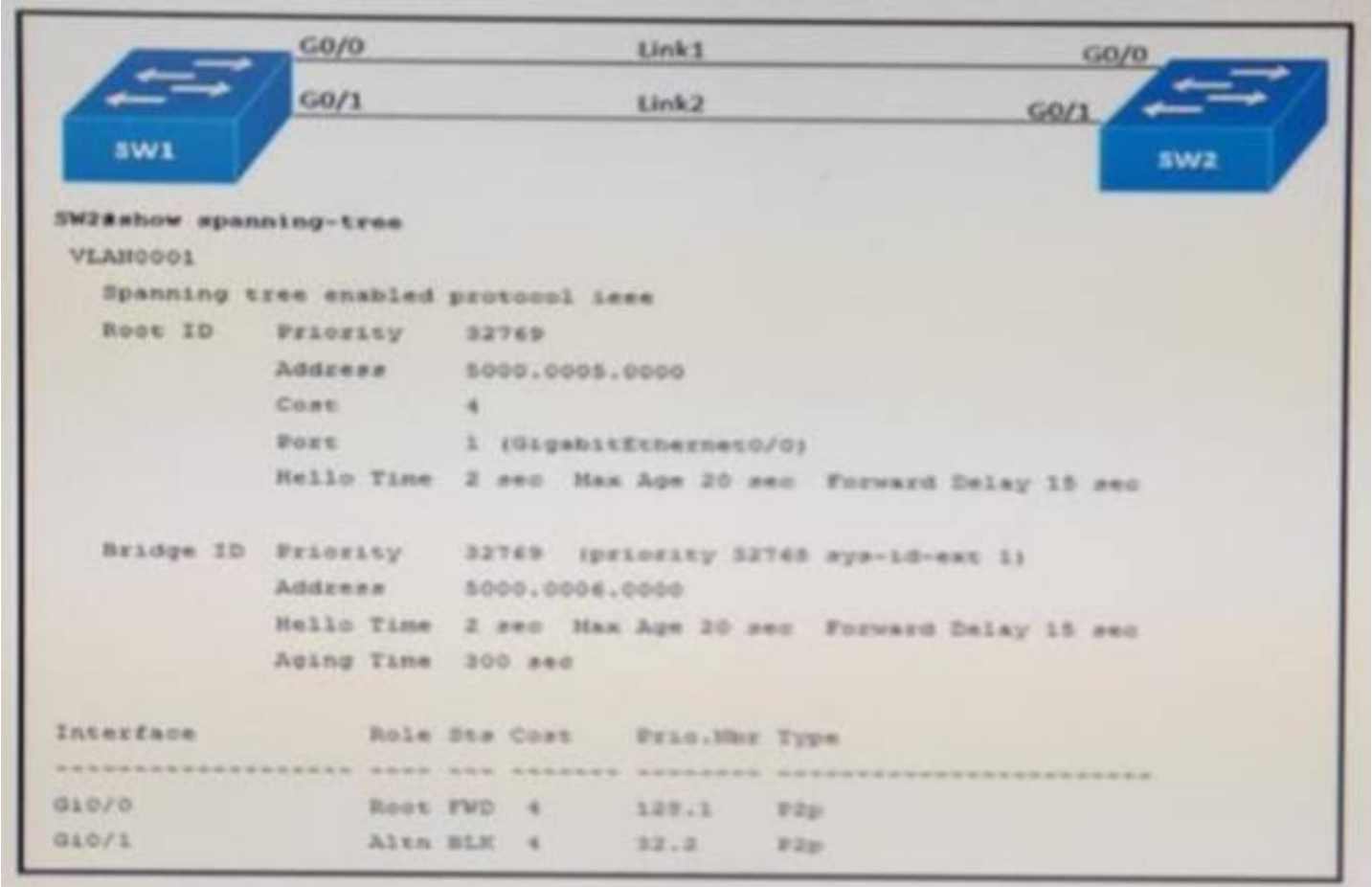
A network engineer wants to configure console access to a router without using AAA so that the privileged exec mode is entered directly after a user provides the correct login credentials. Which action achieves this goal?

- A. Configure login authentication privileged on line con 0.
- B. Configure a local username with privilege level 15.
- C. Configure privilege level 15 on line con 0.
- D. Configure a RADIUS or TACACS+ server and use it to send the privilege level.

**Answer: C**

#### NEW QUESTION 312

- (Topic 4)



Refer to the exhibit. Link 1 uses a copper connection and link 2 uses a fiber connection. The fiber port must be the primary port for all forwarding. The output of the show spanning- tree command on SW2 shows that the fiber port is blocked by Spanning Tree. After entering the spanning-tree port-priority 32 command on G0/1 on SW2, the port remains blocked. Which command should be entered on the ports connected to Link 2 is resolve the issue?

- A. Enter spanning-tree port-priority 64 on SW2
- B. Enter spanning-tree port-priority 224 on SW1.
- C. Enter spanning-tree port-priority 4 on SW2.
- D. Enter spanning-tree port-priority 32 on SW1.

Answer: D

NEW QUESTION 313

- (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 315

- (Topic 4)  
Which JSON script is properly formatted?  
A)

```
[
 "Session":{
 "title":"Writing 201",
 "grade":"11",
 "location":"Maine",
 }
]
```

B)



```
{
 "river": [
 {
 "name": "Mississippi",
 "state": "Louisiana",
 "ranking": "13"
 }
]
}
```

C)

```
"paint":[
 {
 "type": "indoor",
 "color": "white",
 "sheen": "satin"
 }
]
```

D)

```
{
 "file":
 [
 "name": "File_4616",
 "location": "User_files",
 "bytes": "13070",
]
}
```

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

**Answer:** A

**Explanation:**

Option A is the properly formatted JSON script. JSON (JavaScript Object Notation) is a standard text-based format for representing structured data based on JavaScript object syntax. It is commonly used for transmitting data in web applications (e.g., sending some data from the server to the client, so it can be displayed on a web page, or vice versa). The JSON syntax rules are as follows<sup>12</sup>:

? Data is in name/value pairs, separated by commas. A name/value pair consists of a field name (in double quotes), followed by a colon, followed by a value: "name": "value".

? Curly braces hold objects. An object can contain multiple name/value pairs: {"name": "value", "name": "value", ...}.

? Square brackets hold arrays. An array can contain multiple values, separated by commas: ["value", "value", ...].

? Values can be strings (in double quotes), numbers, booleans (true or false), null, objects, or arrays.

Option A follows these rules and is a valid JSON script. It defines an object with four name/value pairs: "name", "age", "hobbies", and "address". The value of "name" is a string, the value of "age" is a number, the value of "hobbies" is an array of strings, and the value of "address" is another object with two name/value pairs: "city" and "country". The object is enclosed in curly braces and the name/value pairs are separated by commas.

Option B is not a valid JSON script because it uses single quotes instead of double quotes for the field names and string values. JSON requires double quotes for strings<sup>12</sup>.

Option C is not a valid JSON script because it does not use commas to separate the name/value pairs. JSON requires commas to separate the data elements within an object or an array<sup>12</sup>.

Option D is not a valid JSON script because it uses a semicolon instead of a colon to separate the field name and the value. JSON requires a colon to separate the name and the value in a name/value pair<sup>12</sup>. References: 1: JSON Introduction, 2: JSON Syntax

**NEW QUESTION 320**

- (Topic 4)

A customer has a wireless network deployed within a multi-tenant building. The network provides client access, location-based services, and is monitored using Cisco DNA Center. The security department wants to locate and track malicious devices based on threat signatures. Which feature is required for this solution?

- A. Cisco aWIPS policies on the WLC
- B. Cisco aWIPS policies on Cisco DNA Center
- C. malicious rogue rules on the WLC
- D. malicious rogue rules on Cisco DNA Center

**Answer:** B

**NEW QUESTION 321**

- (Topic 4)

Refer to the exhibit.

```
R2(config)#event manager applet script_1
R2(config-applet)#action 1 cli command "enable"
R2(config-applet)#action 2 cli command "config t"
R2(config-applet)#action 3 cli command "interface ge0/0"
R2(config-applet)#action 4 cli command "ip add 172.16.1.1 255.255.255.0"
R2(config-applet)#action 5 cli command "no sh"
R2(config-applet)#action 6 cli command "end"
R2(config-applet)#exit
```

An engineer must create a manually triggered EEM applet to enable the R2 router interface and assign an IP address to it. What is required to complete this configuration?

- A. R2(config-applet)# event oir
- B. R2(config-applet)#action 4 cli command "ip add 172.16.1.1 0.0.0.255"
- C. R2(config)# event manager session cli username
- D. R2(config-applet)# event none sync yes

**Answer:** D

#### NEW QUESTION 322

- (Topic 4)

A firewall address of 192.168.1.101 can be pinged from a router but, when running a traceroute to it, this output is received

```
1 * * *
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
```

What is the cause of this issue?

- A. The firewall blocks ICMP traceroute traffic.
- B. The firewall rule that allows ICMP traffic does not function correctly
- C. The firewall blocks ICMP traffic.
- D. The firewall blocks UDP traffic

**Answer:** D

#### NEW QUESTION 323

- (Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 328

- (Topic 4)

```
*Apr 6 13:35:07.826: AAA/BIND(00000055): Bind if
*Apr 6 13:35:07.826: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*Apr 6 13:35:07.826: TPLUS: Queuing AAA Authentication request 85 for processing
*Apr 6 13:35:07.826: TPLUS(00000055) login timer started 1020 sec timeout
*Apr 6 13:35:07.826: TPLUS: processing authentication start request id 85
*Apr 6 13:35:07.826: TPLUS: Authentication start packet created for 85()
*Apr 6 13:35:07.826: TPLUS: Using server 10.106.60.182
*Apr 6 13:35:07.826: TPLUS(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*Apr 6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: socket event 2
*Apr 6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*Apr 6 13:35:07.830: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.830: TPLUS(00000055)/0/READ: Would block while reading
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 18 bytes response
*Apr 6 13:35:07.886: TPLUS(00000055)/0/225FE2DC: Processing the reply packet
*Apr 6 13:35:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*Apr 6 13:35:07.886: TPLUS: Invalid AUTHEN packet (check keys).
```

Refer to the exhibit. An engines configured TACACS^ to authenticate remote users but the configuration is not working as expected Which configuration must be applied to enable access?

A)

```
R1(config)# ip tacacs source-interface Gig 0/0
```

B)

```
R1(config)# tacacs server prod
R1(config-server-tacacs)# key cisco123
```

C)

```
R1(config)# aaa authorization exec default group tacacs+ local
```

D)

```
R1(config)# tacacs server prod
R1(config-server-tacacs)# port 1020
```

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

Answer: C

#### NEW QUESTION 330

- (Topic 4)

Which JSON script is properly formatted?

A)

```
["Lodging":
 {
 "type":B&B,
 "location":Oceanfront,
 "contact":946-230-7462
 }
]
```

B)



```
{
 "frames": [
 {
 "type": "premium",
 "material": "wood",
 "shape": "square"
 }
]
}
```

C)

```
[
 {
 "subject": {
 [
 "title": "Sewing"
 "listing": "elective"
 "session": "Summer"
]
 }
]
}
```

D)

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

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

**Answer: A****Explanation:**

Option A is the properly formatted JSON script. JSON (JavaScript Object Notation) is a standard text-based format for representing structured data based on JavaScript object syntax. It is commonly used for transmitting data in web applications (e.g., sending some data from the server to the client, so it can be displayed on a web page, or vice versa). The JSON syntax rules are as follows<sup>12</sup>:

? Data is in name/value pairs, separated by commas. A name/value pair consists of a field name (in double quotes), followed by a colon, followed by a value: "name": "value".

? Curly braces hold objects. An object can contain multiple name/value pairs: {"name": "value", "name": "value", ...}.

? Square brackets hold arrays. An array can contain multiple values, separated by commas: ["value", "value", ...].

? Values can be strings (in double quotes), numbers, booleans (true or false), null, objects, or arrays.

Option A follows these rules and is a valid JSON script. It defines an object with four name/value pairs: "name", "age", "hobbies", and "address". The value of "name" is a string, the value of "age" is a number, the value of "hobbies" is an array of strings, and the value of "address" is another object with two name/value pairs: "city" and "country". The object is enclosed in curly braces and the name/value pairs are separated by commas.

Option B is not a valid JSON script because it uses single quotes instead of double quotes for the field names and string values. JSON requires double quotes for strings<sup>12</sup>.

Option C is not a valid JSON script because it does not use commas to separate the name/value pairs. JSON requires commas to separate the data elements within an object or an array<sup>12</sup>.

Option D is not a valid JSON script because it uses a semicolon instead of a colon to separate the field name and the value. JSON requires a colon to separate the name and the value in a name/value pair<sup>12</sup>. References: 1: JSON Introduction, 2: JSON Syntax

**NEW QUESTION 332**

- (Topic 4)

What is a characteristic of the Cisco DNA Center Template Editor feature?

- A. It facilitates software upgrades to network devices from a central point.  
B. It facilitates a vulnerability assessment of the network devices.  
C. It provides a high-level overview of the health of every network device.  
D. It uses a predefined configuration through parameterized elements or variables.

**Answer: D****Explanation:**

This is because the Cisco DNA Center Template Editor feature is a tool that allows the network administrator to create and deploy configuration templates to multiple network devices. The configuration templates use parameterized elements or variables, which are placeholders for values that can be customized for each device. For example, a variable can represent the hostname, IP address, or interface number of a device. The parameterized elements or variables can be defined manually or automatically using the Cisco DNA Center inventory. The source of this answer is the Cisco ENCOR v1.1 course, module 8, lesson 8.5: Implementing

Network Configuration Management.

NEW QUESTION 335

- (Topic 4)

What is the result when an active route processor fails that combines NSF with SSO?

- A. An NSF-capable device immediately updates the standby route processor RIB without churning the network.
- B. The standby route processor immediately takes control and forwards packets along known routes.
- C. An NSF-aware device immediately updates the standby route processor RIB without churning the network.
- D. The standby route processor temporarily forwards packets until route convergence is complete.

Answer: B

NEW QUESTION 338

DRAG DROP - (Topic 4)

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

The forwarding table is created in advance.

The router processor is involved with every forwarding decision.

All forwarding decisions are made in software.

All packets are switched using hardware.

Cisco Express Forwarding

Process Switching

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The forwarding table is created in advance.

The router processor is involved with every forwarding decision.

All forwarding decisions are made in software.

All packets are switched using hardware.

Cisco Express Forwarding

The forwarding table is created in advance.

All forwarding decisions are made in software.

Process Switching

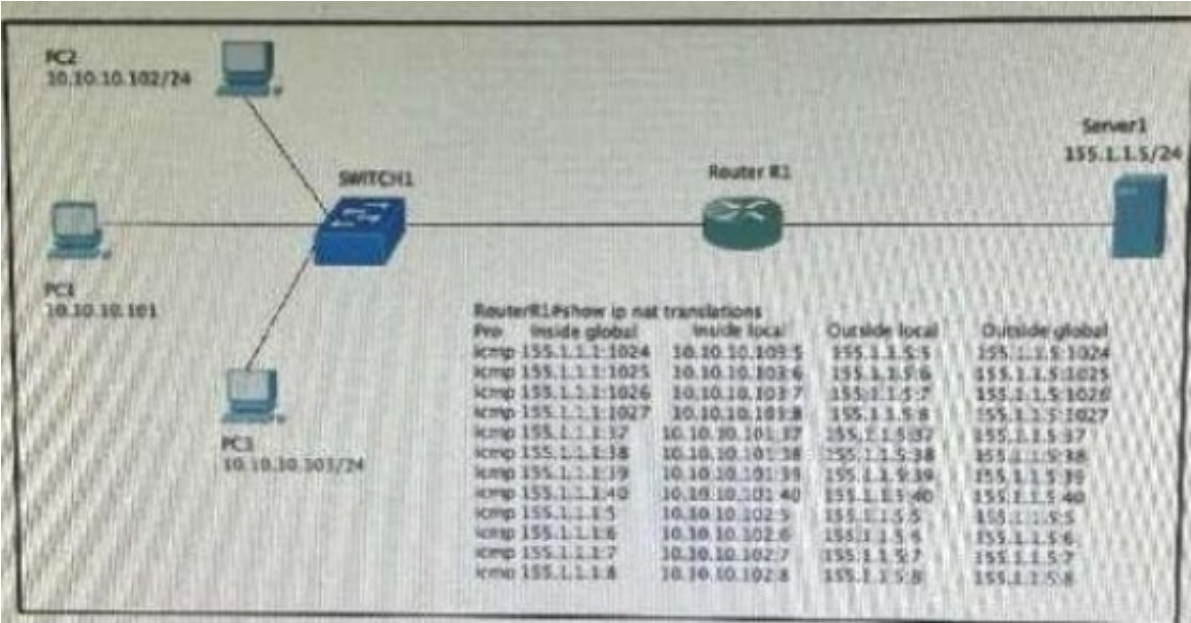
The router processor is involved with every forwarding decision.

All packets are switched using hardware.

NEW QUESTION 341

- (Topic 4)

Refer to the exhibit.



Hosts PC1 PC2 and PC3 must access resources on Serve 1. An engineer configures NAT on Router R1 1e enable the communication and enters the show

command to verify operation Which IP address is used by the hosts when they communicate globally to Server1?

- A. 155.1.1.1
- B. random addresses in the 155.1.1.0/24 range
- C. their own address in the 10.10.10.0/24 range
- D. 155.1.1.5

**Answer:** A

#### NEW QUESTION 343

- (Topic 4)

Which technology reduces the implementation of STP and leverages both unicast and multicast?

- A. VSS
- B. VXLAN
- C. VPC
- D. VLAN

**Answer:** B

#### NEW QUESTION 346

- (Topic 4)

Which function is performed by vSmart in the Cisco SD-WAN architecture?

- A. distribution of IPsec keys
- B. Redistribution between OMP and other routing protocols
- C. facilitation of NAT detection and traversal
- D. execution of localized policies

**Answer:** B

#### NEW QUESTION 350

- (Topic 4)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 355

SIMULATION - (Topic 4)

Simulation 02

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

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



Comment

Guidelines Topology Tasks

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

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

DISTRO-SW1 DISTRO-SW2

DISTRO-SW1>

Guidelines Topology Tasks

DISTRO-SW1 DISTRO-SW2

DISTRO-SW1>

```

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

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

```

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

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

```
!
interface Vlan100
 ip address 192.168.1.2 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
!
!
!
!
control-plane
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
```

DISTRO-SW2

```
no ipv6 cef
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
!
interface Ethernet0/0
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
!
```

```

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

```

- A. Mastered  
B. Not Mastered

**Answer: A**

**Explanation:**

DISTRO-SW1

Sw1



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

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

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

Description automatically generated

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

DISTRO-SW1

Sw1

```
int vlan 100
glbp 1 ip 192.168.1.254
glbp 1 priority 110
glbp 1 timers 5 15
glbp 1 preempt
copy run start
DISTRO-SW2 SW2
int vlan 100
glbp 1 ip 192.168.1.254
glbp 1 timers 5 15
glbp 1 preempt copy run start
```

#### NEW QUESTION 357

- (Topic 4)



Refer to the exhibit. Which two configurations enable R1 and R2 to advertise routes into OSPF? (Choose two)

A)

```
R2
router ospf 0
network 172.16.1.0 255.255.255.0 area 0
network 172.16.2.0 255.255.255.0 area 0
```

B)

```
R2
router ospf 0
network 172.16.1.0 0.0.0.255 area 0
network 172.16.2.0 255.255.255.0 area 0
```

C)

```
R1
router ospf 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
```

D)

```
R2
router ospf 0
network 172.16.1.0 0.0.0.255 area 0
network 172.16.2.0 0.0.0.255 area 0
```

E)

```
R1
router ospf 0
network 192.168.1.0 255.255.255.0 area 0
network 192.168.2.0 255.255.255.0 area 0
```

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

Answer: CD

NEW QUESTION 361

DRAG DROP - (Topic 4)

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

works at the control plane

works at the data plane

derived from routing protocols

installed on line cards

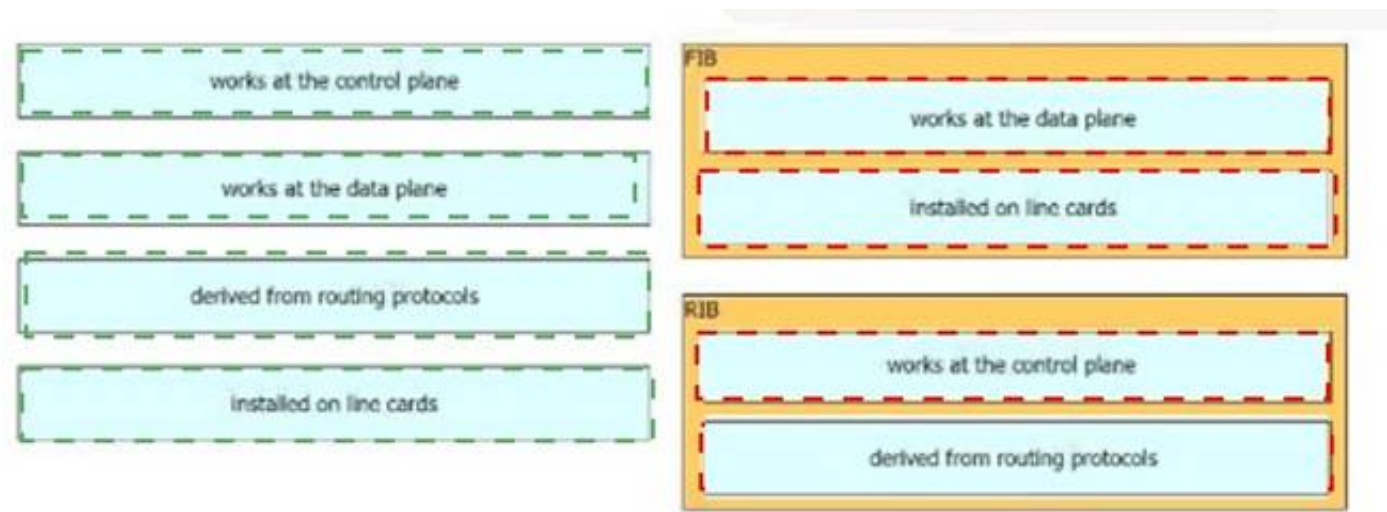
FIB

RIB

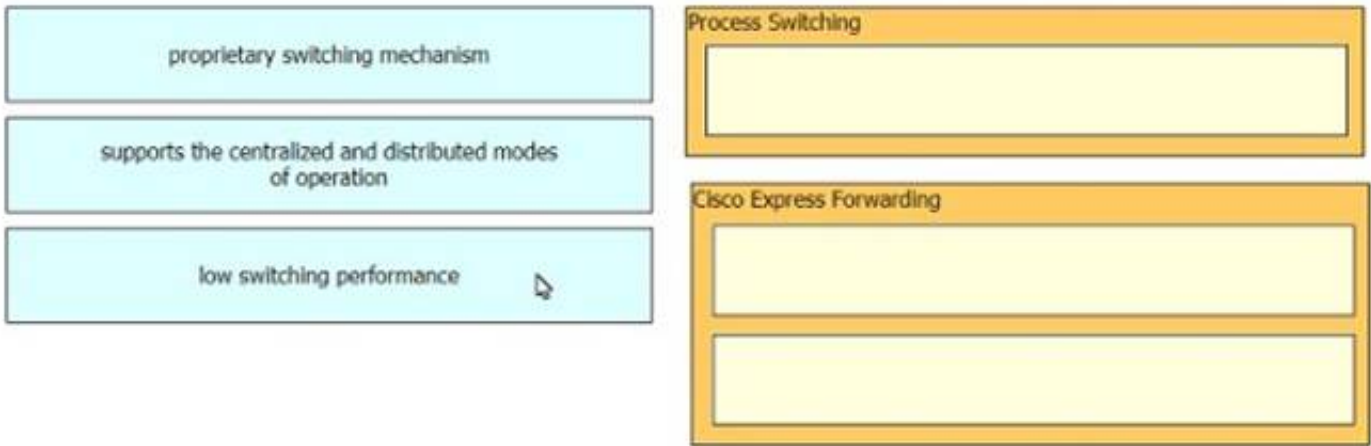
- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



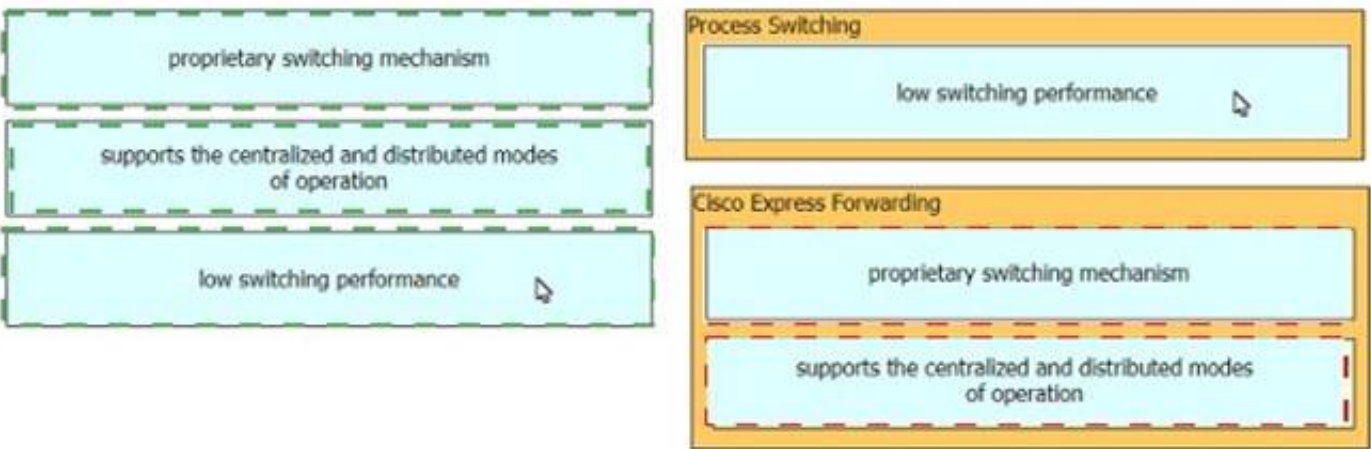
**NEW QUESTION 363**  
DRAG DROP - (Topic 4)  
Drag and drop the characteristics from the left onto the switching architectures on the right.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



**NEW QUESTION 367**  
- (Topic 2)  
What occurs when a high bandwidth multicast stream is sent over an MVPN using Cisco hardware?

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

Answer: D

**NEW QUESTION 372**  
DRAG DROP - (Topic 2)  
An engineer is working with the Cisco DNA Center API Drag and drop the methods from the left onto the actions that they are used for on the right.



|        |                                  |
|--------|----------------------------------|
| GET    | remove an element using the API  |
| POST   | update an element                |
| DELETE | extract information from the API |
| PUT    | create an element                |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

|        |        |
|--------|--------|
| GET    | DELETE |
| POST   | PUT    |
| DELETE | GET    |
| PUT    | POST   |

NEW QUESTION 375

- (Topic 2)

```
RP/0/0/CPU0:R2#debug isis adjacencies
RP/0/0/CPU0:Apr 2 20:57:00.421 : isis[1010]: RECV P2P IIH (L2)
from GigabitEthernet0/0/0/0 SNPA fa16.3ebe.a7bc: System ID R2,
Holdtime 30, length 1429
RP/0/0/CPU0:Apr 2 20:57:01.761 : isis[1010]: SEND P2P IIH (L1)
on GigabitEthernet0/0/0/0: Holdtime 30s, Length 41
```

Refer to the exhibit. A network operator is attempting to configure an IS-IS adjacency between two routers, but the adjacency cannot be established. To troubleshoot the problem, the operator collects this debugging output. Which interfaces are misconfigured on these routers?

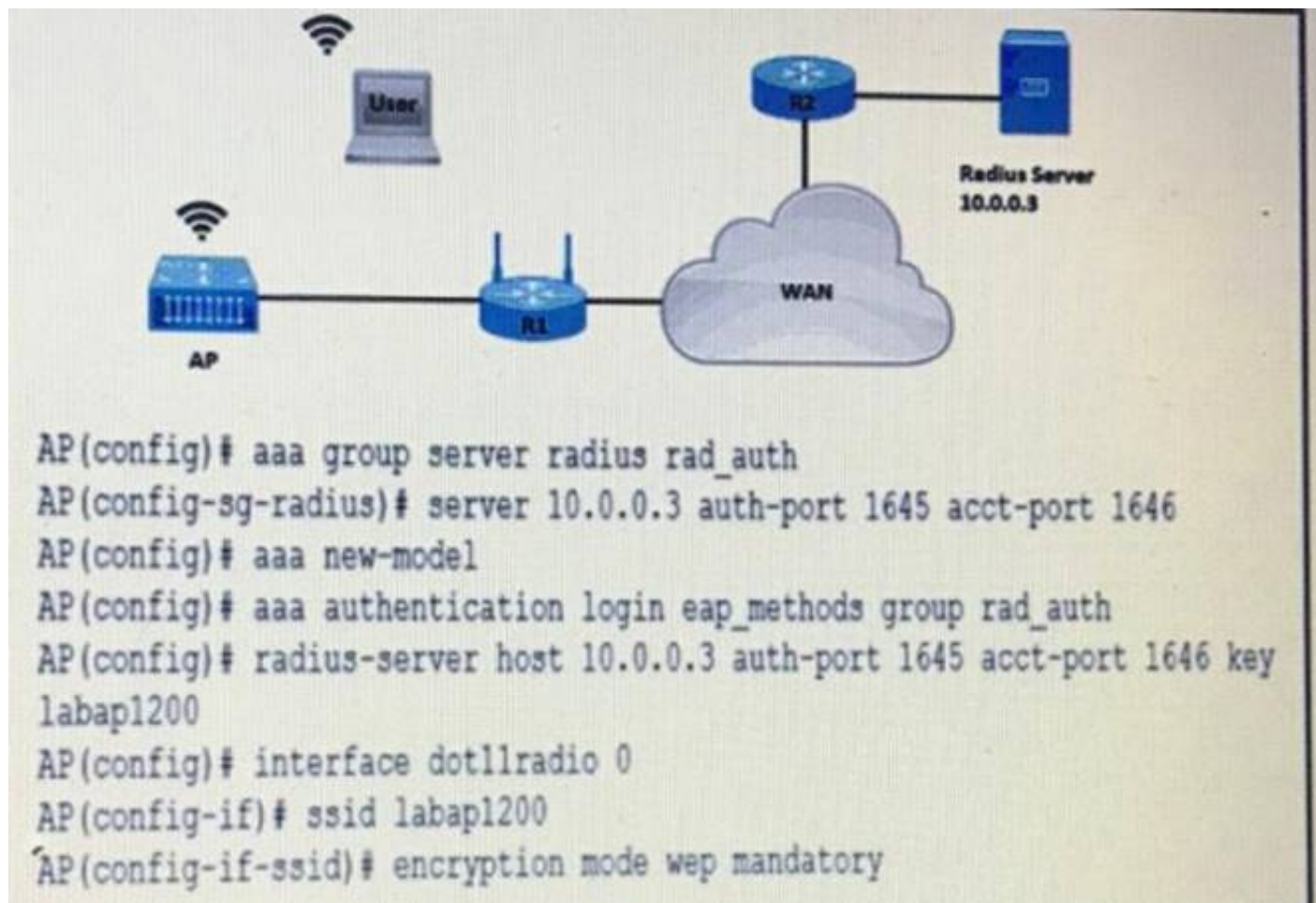
- A. The peer router interface is configured as Level 1 only, and the R2 interface is configured as Level 2 only
- B. The R2 interface is configured as Level 1 only, and the Peer router interface is configured as Level 2 only
- C. The R2 interface is configured as point-to-point, and the peer router interface is configured as multipoint.
- D. The peer router interface is configured as point-as-point, and the R2 interface is configured as multipoint.

Answer: C

NEW QUESTION 379

- (Topic 2)

Refer to the exhibit.



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

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

**Answer: D**

#### NEW QUESTION 382

- (Topic 2)

A client device roams between access points located on different floors in an atrium. The access points are Joined to the same controller and configured in local mode. The access points are in different AP groups and have different IP addresses, but the client VLAN in the groups is the same. Which type of roam occurs?

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

**Answer: D**

#### Explanation:

Mobility, or roaming, is a wireless LAN client's ability to maintain its association seamlessly from one access point to another securely and with as little latency as possible. Three popular types of client roaming are:

Intra-Controller Roaming: Each controller supports same-controller client roaming across access points managed by the same controller. This roaming is transparent to the client as the session is sustained, and the client continues using the same DHCP-assigned or client-assigned IP address.

Inter-Controller Roaming: Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group and on the same subnet. This roaming is also transparent to the client because the session is sustained and a tunnel between controllers allows the client to continue using the same DHCP- or client-assigned IP address as long as the session remains active.

Inter-Subnet Roaming: Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group on different subnets. This roaming is transparent to the client because the session is sustained and a tunnel between the controllers allows the client to continue using the same DHCP-assigned or client-assigned IP address as long as the session remains active. Reference:

[https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b\\_cg74\\_CONSOLIDATED/b\\_cg74\\_CONSOLIDATED\\_chapter\\_01100.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01100.html)

In three types of client roaming above, only with Inter-Subnet Roaming the controllers are in different subnets.

#### NEW QUESTION 387

- (Topic 2)

What are two benefits of implementing a Cisco SD-WAN architecture? (Choose two)

- A. It provides resilient and effective traffic flow using MPLS.
- B. It improves endpoint protection by integrating embedded and cloud security features.
- C. It allows configuration of application-aware policies with real time enforcement.
- D. It simplifies endpoint provisioning through standalone router management
- E. It enforces a single
- F. scalability
- G. hub-and-spoke topology.

**Answer: CD**

#### Explanation:

The top SD-WAN benefits are:

- + Increased bandwidth at a lower cost
- + Centralized management across branch networks
- + Full visibility into the network
- + Providing organizations with more connection type options and vendor selection when building a network.

Reference: <https://www.sdxcentral.com/networking/sd-wan/definitions/sd-wan-technology/>

-> We can provision endpoints (vEdges) through a centralized router vManage -> Answer D is correct.

Answer A is not correct as we can use different kind of connections on SD-WAN: MPLS, LTE, 4G, xDSL, Internet connections...

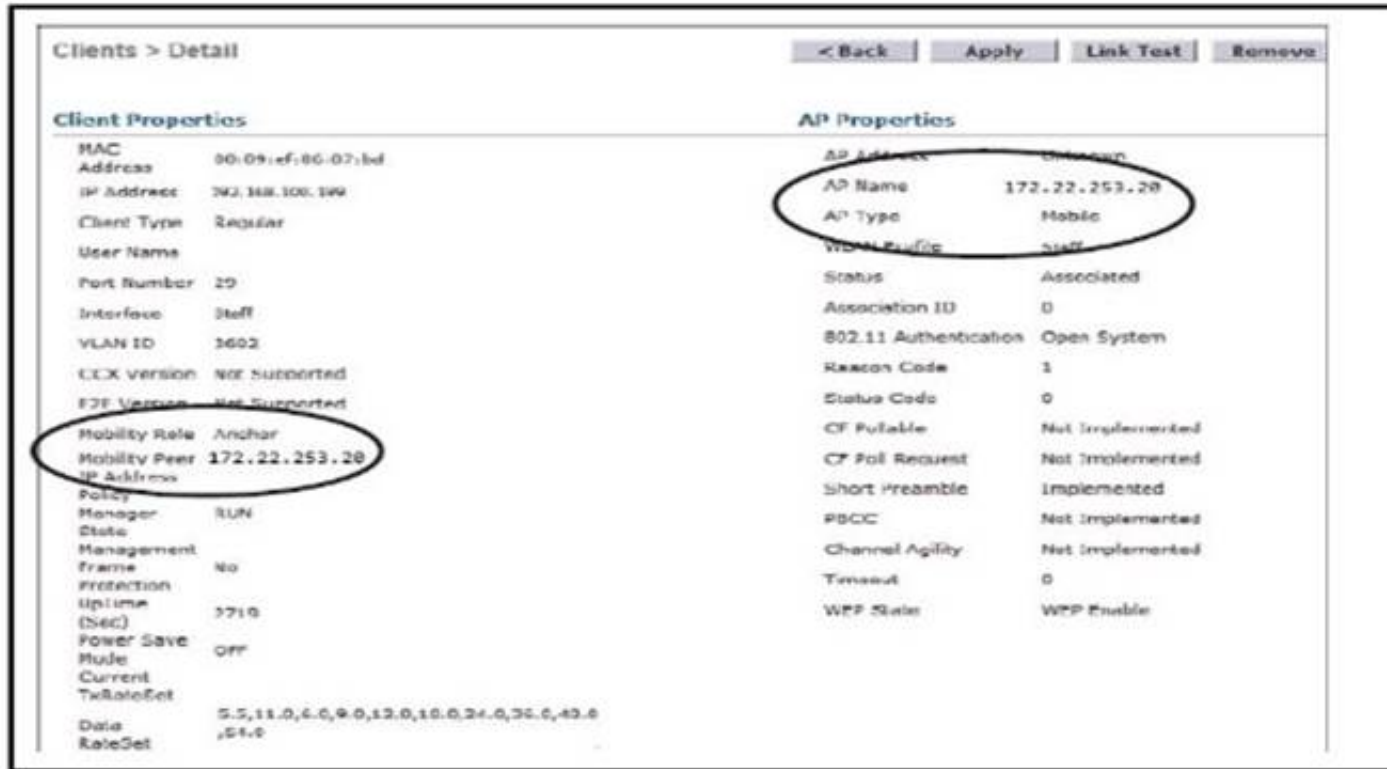
Application-Aware Routing policy is configured in vManage as a centralized data policy that maps the service- side application(s) to specific SLA requirements. The centralized policies provisioned in vSmart controller is pushed to relevant WAN Edge devices for enforcement. The defined policy consists of match- action pairs, where the match statement defines the application-list or the type of traffic to match, and the action statement defines the SLA action the WAN Edge devices must enforce for the specified traffic.

Reference: <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan- application-awarerouting-deploy-guide.html>

#### NEW QUESTION 391

- (Topic 4)

Refer to the exhibit.



The WLC administrator sees that the controller to which a roaming client associates has Mobility Role Anchor configured under Clients > Detail. Which type of roaming is supported?

- A. Indirect
- B. Layer 3 intercontroller
- C. Layer 2 intercontroller
- D. Intracontroller

**Answer: B**

#### NEW QUESTION 396

- (Topic 4)

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

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

**Answer: A**

#### NEW QUESTION 397

- (Topic 4)

Which free 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 402

- (Topic 4)

Refer to the exhibit.



```
DSW1#sh spanning-tree
MST1
 Spanning tree enabled protocol mstp
 Root ID Priority 32769
 Address 001b.7363.4300
 Cost 2
 Port 13 (FastEthernet1/0/11)
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

 Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
 Address 001b.0d8e.e080
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type

Fa1/0/7 Desg FWD 2 128.9 P2p Bound (PVST)
Fa1/0/10 Desg FWD 2 128.12 P2p Bound (PVST)
Fa1/0/11 Root FWD 2 128.13 P2p
Fa1/0/12 Altn BLK 2 128.14 P2p

DSW1#sh spanning-tree mst

MST1 vlans mapped: 10,20
Bridge address 001b.0d8e.e080 priority 32769 (32768 sysid 1)
Root address 001b.7363.4300 priority 32769 (32768 sysid 1)
 port Fa1/0/11 cost 2 rem hops 19

!
... output omitted
!
```

Which two commands ensure that DSW1 becomes root bridge for VLAN 10 and 20?

- A. spanning-tree mst 1 priority 1
- B. spanning-tree mst 1 root primary
- C. spanning-tree mstp vlan 10,20 root primary
- D. spanning-tree mst vlan 10,20 priority root
- E. spanning-tree mst 1 priority 4096

Answer: BE

NEW QUESTION 403

- (Topic 4)  
Why would an architect use an OSPF virtual link?

- A. to allow a stub area to transit another stub area
- B. to connect two networks that have overlapping private IP address space
- C. to merge two existing Area 0s through a nonbackbone
- D. to connect a nonbackbone area to Area 0 through another nonbackbone area

Answer: D

Explanation:

A virtual link is a logical connection between two OSPF routers that belong to different areas but share a common border with a transit area. A virtual link allows an OSPF router to participate in the backbone area (Area 0) even if it is not physically connected to it. This way, the OSPF network can maintain connectivity and routing consistency across all areas. A virtual link is configured between the OSPF router IDs of the two routers that need to be connected to the backbone area123.

Option A is incorrect because a stub area is an area that does not receive external routes from other autonomous systems or other OSPF areas. A stub area can only transit traffic to and from the backbone area, and it cannot be used as a transit area for a virtual link12. Option B is incorrect because a virtual link does not change the IP address space of the networks that it connects. A virtual link is transparent to the IP layer and only affects the OSPF routing protocol. To connect two networks that have overlapping private IP address space, other solutions such as NAT or VPN are required12.

Option C is incorrect because a virtual link cannot merge two existing Area 0s through a nonbackbone area. A virtual link can only extend an existing Area 0 through a nonbackbone area. If there are two separate Area 0s in an OSPF network, they cannot be merged by a virtual link, and the network is considered to be partitioned. A partitioned network can cause routing loops and inconsistencies, and it should be avoided12. References: 1: Configure OSPF Connection in a Virtual Link Environment, 2: How to configure OSPF Virtual Link, 3: Understand OSPF Areas and Virtual Links

NEW QUESTION 407

- (Topic 4)  
Refer to the exhibit.

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

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

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

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

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

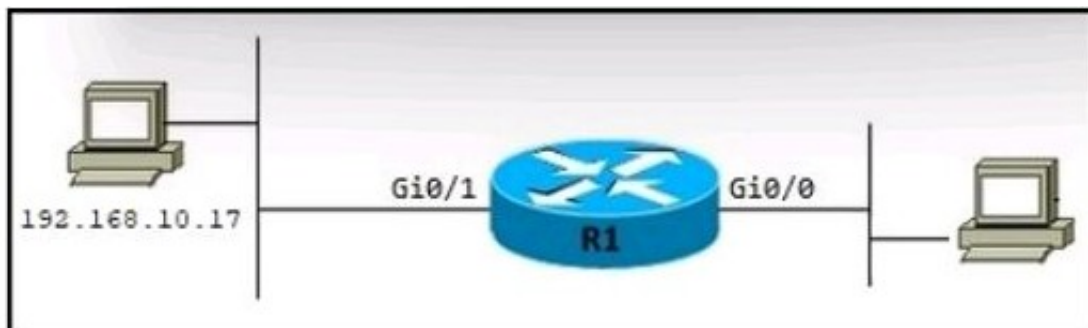
- A. Configure SW1 with dynamic auto mode on interface FastEthernet0/1.
- B. Configure the native VLAN to be the same VLAN on both switches on interface FastEthernet0/1.
- C. Configure SW2 with encapsulation dot1q on interface FastEthernet0/1.
- D. Configure FastEthernet0/1 on both switches for static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

**Answer: C**

#### NEW QUESTION 409

- (Topic 4)

Refer to the exhibit.



An engineer applies this configuration to R1:

```
ip nat inside source static 192.168.10.17 192.168.27.42
```

Which command set should be added to complete the configuration?

A)

```
R1(config)# interface GigabitEthernet 0/0
R1(config)# ip nat inside
```

```
R1(config)# interface GigabitEthernet 0/1
R1(config)# ip nat outside
```

B)

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip nat outside
```

```
R1(config)# interface GigabitEthernet 0/1
R1(config-if)# ip nat inside
```

C)

```
R1(config)# interface GigabitEthernet 0/0
R1(config)# ip pat outside
```

```
R1(config)# interface GigabitEthernet 0/1
R1(config)# ip pat inside
```

D)

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip nat inside
```

```
R1(config)# interface GigabitEthernet 0/1
R1(config-if)# ip nat outside
```

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

**Answer:** C

**Explanation:**

Option C is the correct set of commands to complete the configuration of NAT on R1. The configuration steps are as follows<sup>12</sup>:

? Define the inside and outside interfaces for NAT using the ip nat inside and ip nat

outside commands. In this case, the inside interface is GigabitEthernet0/0 and the outside interface is GigabitEthernet0/1: interface GigabitEthernet0/0 and ip nat inside, interface GigabitEthernet0/1 and ip nat outside.

? Configure a static NAT entry that maps the inside local address 192.168.10.17 to

the inside global address 192.168.27.42 using the ip nat inside source static command: ip nat inside source static 192.168.10.17 192.168.27.42.

? Verify the NAT configuration using the show ip nat translations and show ip nat

statistics commands: show ip nat translations and show ip nat statistics. Option A is incorrect because it does not define the inside and outside interfaces for NAT, which is required for NAT to function properly<sup>1</sup>.

Option B is incorrect because it uses the ip nat outside source static command, which is used to translate the source address of packets that travel from outside to inside, and the destination address of packets that travel from inside to outside. This is not the desired behavior for this scenario, where the inside local address 192.168.10.17 should be translated to the inside global address 192.168.27.42 in both directions<sup>1</sup>.

Option D is incorrect because it uses the ip nat pool and ip nat inside source

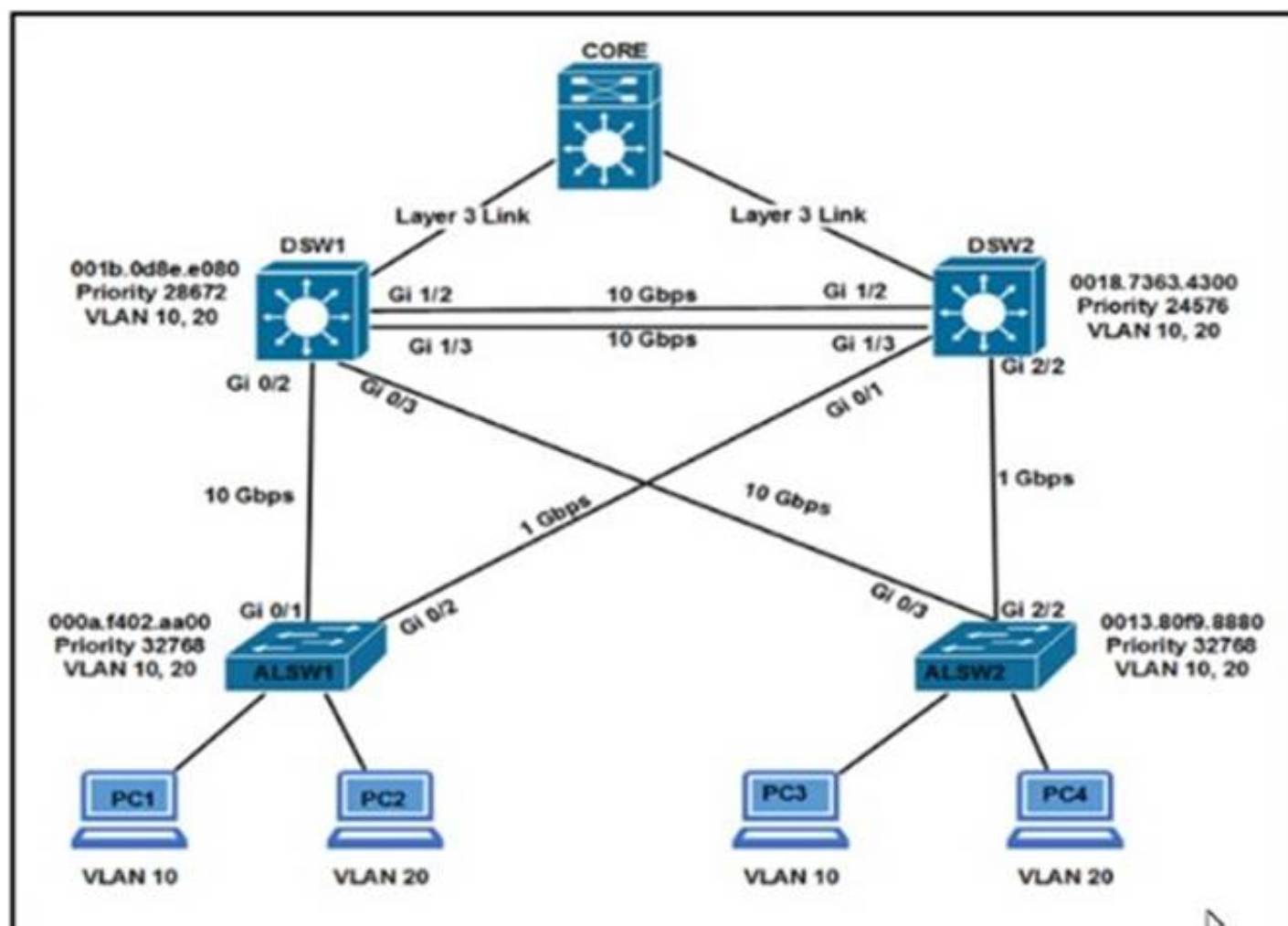
list commands, which are used to configure dynamic NAT or PAT, not static NAT. These commands create a pool of inside global addresses and an access list to define which inside local addresses are eligible for translation. However, in this scenario, there is only one inside local address and one inside global address, so a static NAT entry is sufficient<sup>1</sup>. References: 1: Configure Network Address Translation, 2: Static NAT

**NEW QUESTION 411**

- (Topic 4)

Refer to the exhibit.





Assuming all links are functional, which path does PC1 take to reach DSW1?

- A. PC1 goes from ALSW1 to DSW2 to CORE to DSW1.
- B. PC1 goes from ALSW1 to DSW2 to DSW1.
- C. PC1 goes from ALSW1 to DSW1.
- D. PC1 goes from ALSW1 to DSW2 to ALSW2 to DSW1.

**Answer: B**

#### NEW QUESTION 413

- (Topic 4)

What is the purpose of the weight attribute in an EID-Io-RLOC mapping?

- A. it indicates the preference for using LISP over native IP connectivity.
- B. it determines the administrative distance of LISP generated routes in the RIB
- C. It identifies the preferred RLOC address family.
- D. it indicates the load-balancing ratio between CTRs of 9m earns priority.

**Answer: D**

#### NEW QUESTION 418

DRAG DROP - (Topic 4)

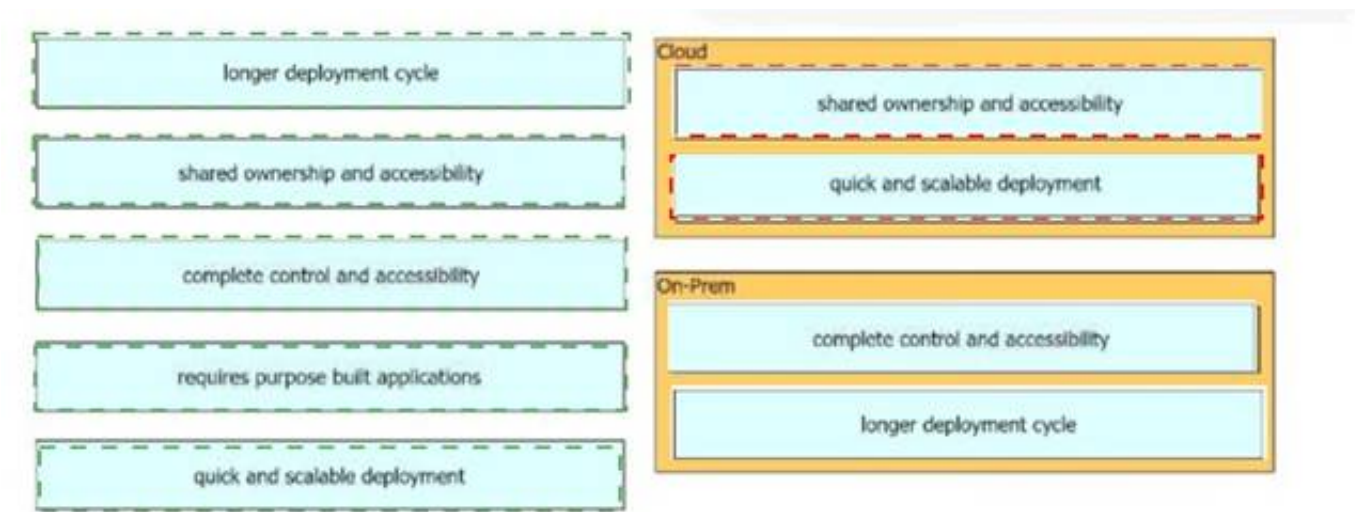
Drag and drop the characteristics from the left onto the deployment models on the right Not all options are used.

|                                     |         |
|-------------------------------------|---------|
| longer deployment cycle             | Cloud   |
| shared ownership and accessibility  |         |
| complete control and accessibility  |         |
| requires purpose built applications | On-Prem |
| quick and scalable deployment       |         |

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**



NEW QUESTION 422

- (Topic 4)  
When a wired client connects to an edge switch in a Cisco SD-Access fabric, which component decides whether the client has access to the network?

- A. control-plane node
- B. edge node
- C. Identity services Engine
- D. RADIUS server

Answer: C

NEW QUESTION 423

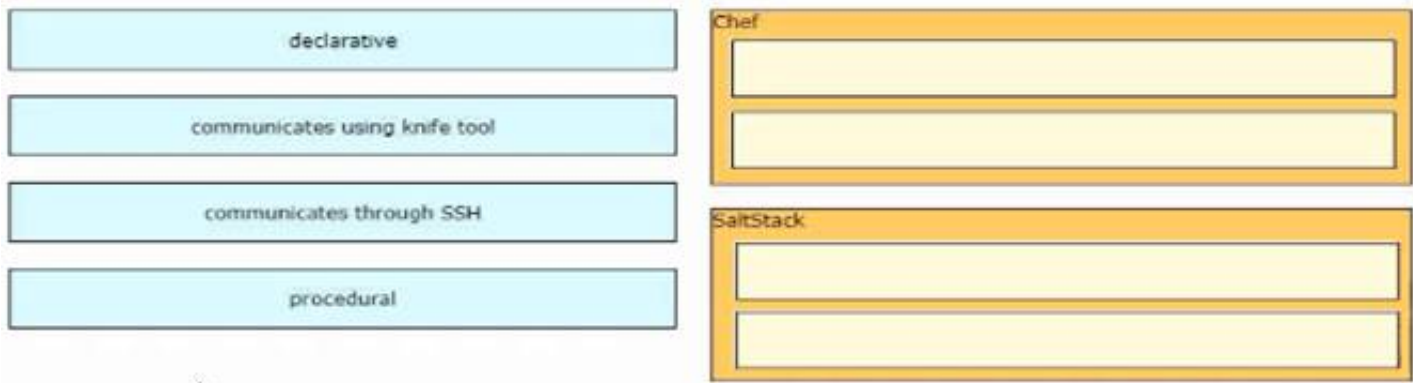
- (Topic 4)  
An engineer is configuring RADIUS-Based Authentication with EAP. MS-CHAPv2 is configured on a client device. Which outer method protocol must be configured on the ISE to support this authentication type?

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

Answer: D

NEW QUESTION 427

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Chef  
Communicates using knife tool Procedural  
SaltStack  
Communicates through SSH Declarative

NEW QUESTION 431

- (Topic 3)  
What Is a characteristic of a WLC that is in master controller mode?

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



Answer: B

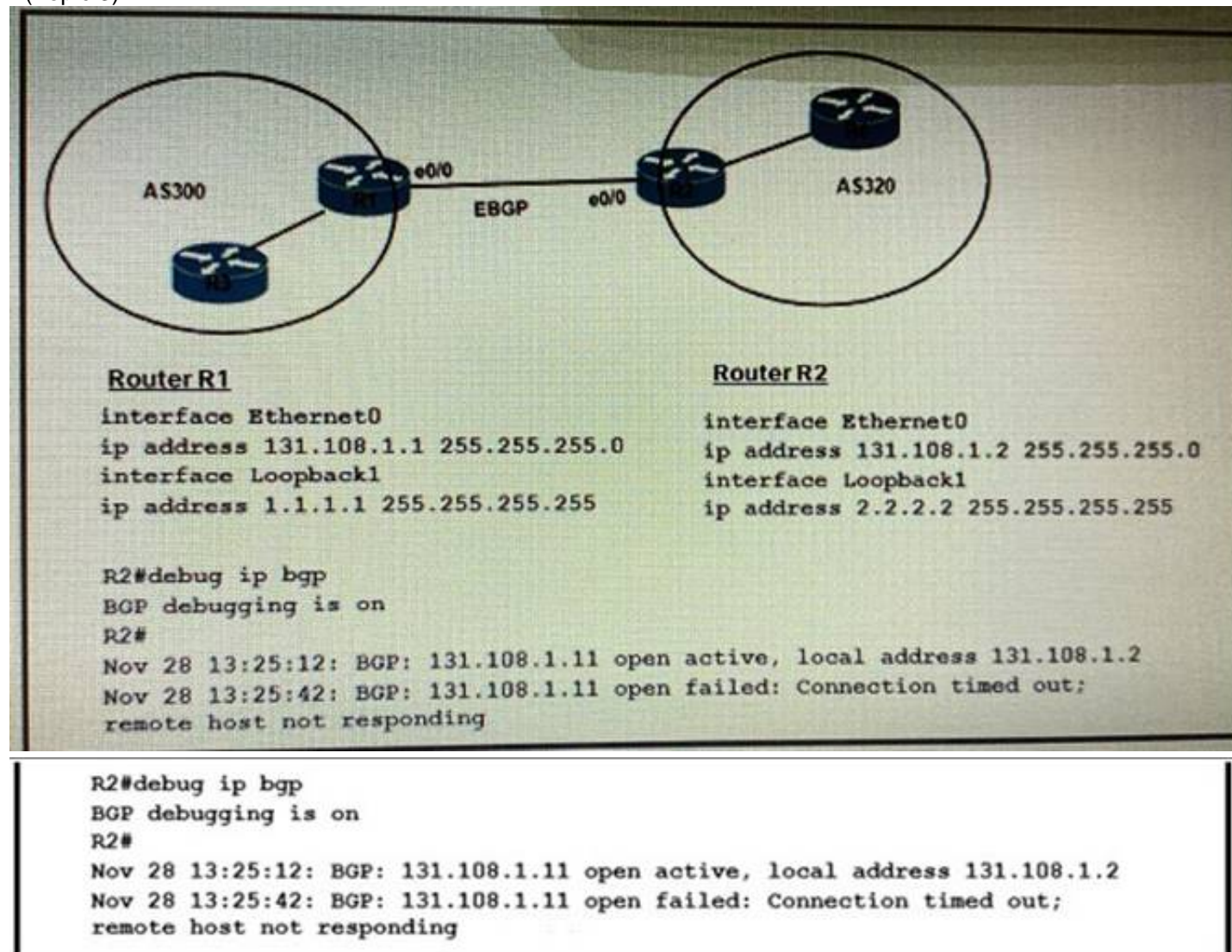
**Explanation:**

When should I use the master controller mode on a WLC? – When there is a master controller enabled, all newly added access points with no primary, secondary, or tertiary controllers assigned associate with the master controller on the same subnet. Reference:

<https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/69561-wlc-faq.html>

**NEW QUESTION 434**

- (Topic 3)



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

- ☒ R2  
**router bgp 320**  
**neighbor 131.108.1.1 remote-as 300**  
R1  
**router bgp 300**  
**neighbor 131.108.1.2 remote-as 320**
- ☐ R2  
**router bgp 320**  
**neighbor 131.108.1.11 remote-as 300**  
R1  
**router bgp 300**  
**neighbor 131.108.1.2 remote-as 320**
- ☐ R2  
**router bgp 300**  
**neighbor 131.108.1.1 remote-as 320**  
R1  
**router bgp 320**  
**neighbor 131.108.1.2 remote-as 300**
- ☐ R2  
**router bgp 320**  
**neighbor 1.1.1.1 remote-as 300**  
R1  
**router bgp 300**  
**neighbor 2.2.2.2 remote-as 320**

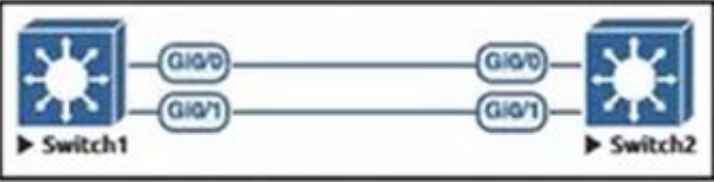


- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

NEW QUESTION 439

- (Topic 3)  
Refer to the exhibit.



Switch1#show run interface Gi0/0

!

interface GigabitEthernet0/0

switchport trunk encapsulation dot1q

switchport mode trunk

negotiation auto

channel-group 1 mode active

end

Switch1#show run interface Gi0/1

!

interface GigabitEthernet0/1

switchport trunk encapsulation dot1q

switchport mode trunk

negotiation auto

channel-group 1 mode passive

end

Switch2#show run interface Gi0/0

!

interface GigabitEthernet0/0

negotiation auto

channel-group 1 mode active

end

Switch2#show run interface Gi0/1

!

interface GigabitEthernet0/1

negotiation auto

channel-group 1 mode passive

end

The port channel between the switches does not work as expected. Which action resolves the issue?

- A. Interface Gi0/0 on Switch2 must be configured as passive.
- B. Interface Gi0/1 on Switch1 must be configured as desirable.
- C. interface Gi0/1 on Switch2 must be configured as active.
- D. Trucking must be enabled on both Interfaces on Switch2.

Answer: C

NEW QUESTION 441

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

sends hello packets every 5 seconds on high-bandwidth links

uses virtual links to link an area that does not have a connection to the backbone

cost is based on interface bandwidth

EIGRP

OSPF

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

sends hello packets every 5 seconds on high-bandwidth links

uses virtual links to link an area that does not have a connection to the backbone

cost is based on interface bandwidth

EIGRP

sends hello packets every 5 seconds on high-bandwidth links

OSPF

cost is based on interface bandwidth

uses virtual links to link an area that does not have a connection to the backbone

#### NEW QUESTION 446

- (Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 448

- (Topic 3)

Which resource is able to be shared among virtual machines deployed on the same physical server?

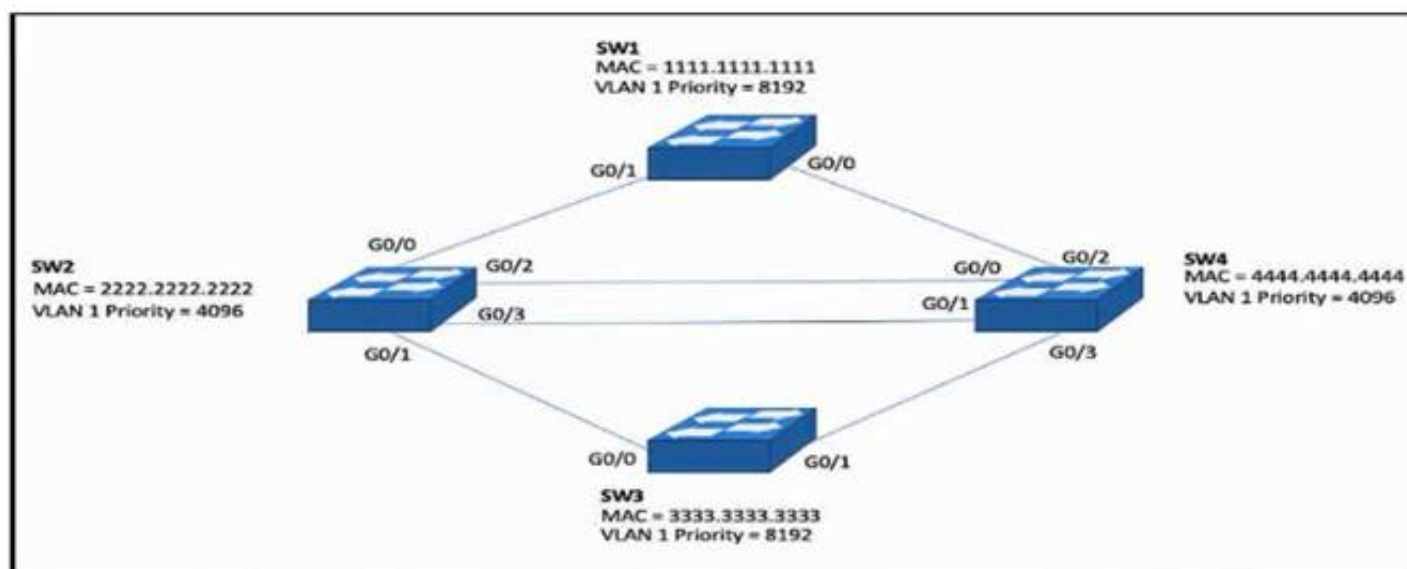
- A. applications
- B. disk
- C. VM configuration file
- D. operating system

**Answer: B**

#### NEW QUESTION 452

- (Topic 3)

Refer the exhibit.



Which configuration elects SW4 as the root bridge for VLAN 1 and puts G0/2 on SW2 into a blocking state?

A)

```
SW4(config)#spanning-tree vlan 1 priority 0
!
SW2(config)#interface G0/2
SW2(config-if)#spanning-tree vlan 1 port-priority 64
```

B)

```
SW4(config)#spanning-tree vlan 1 priority 0
!
SW2(config)#int G0/2
SW2(config-if)#spanning-tree cost 128
```

C)

```
SW4(config)#spanning-tree vlan 1 priority 32768
!
SW2(config)#interface G0/2
SW2(config-if)#spanning-tree vlan 1 port-priority 0
```

D)

```
SW4(config)#spanning-tree vlan 1 priority 32768
!
SW2(config)#int G0/2
SW2(config-if)#spanning-tree cost 128
```

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

**Answer: B**

#### NEW QUESTION 455

- (Topic 3)

```
switch1(config)# interface GigabitEthernet 1/1
switch1(config-if)# switchport mode trunk
switch1(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70-90
switch1(config)# exit
switch1(config)# monitor session 1 source vlan 10
switch1(config)# monitor session 1 destination remote vlan 70

switch2(config)# interface GigabitEthernet 1/1
switch2(config-if)# switchport mode trunk
switch2(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,80-90
switch2(config)# exit
switch2(config)# monitor session 2 source remote vlan 70
switch2(config)# monitor session 2 destination interface GigabitEthernet1/1
```

Refer to the exhibit. A network administrator configured RSPAN to troubleshoot an issue between switch1 and switch2. The switches are connected using interface GigabitEthernet 1/1. An external packet capture device is connected to switch2 interface GigabitEthernet 1/2. Which two commands must be added to complete this configuration? (Choose two)

- ☐ switch2(config)# monitor session 1 source remote vlan 70  
switch2(config)# monitor session 1 destination interface GigabitEthernet1/2
- ☐ switch2(config)# monitor session 1 source remote vlan 70  
switch2(config)# monitor session 1 destination interface GigabitEthernet1/1
- ☐ switch1(config)# interface GigabitEthernet 1/1  
switch1(config-if)# switchport mode access  
switch1(config-if)# switchport access vlan 10  
  
switch2(config)# interface GigabitEthernet 1/1  
switch2(config-if)# switchport mode access  
switch2(config-if)# switchport access vlan 10
- ☐ switch2(config)# monitor session 2 destination vlan 10
- ☐ switch2(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70-80

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

**Answer:** AE

#### NEW QUESTION 458

- (Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 462

- (Topic 3)

Refer to the exhibit.



```
import json
from requests import get

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

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

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

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

Insert after the for loop:

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

B)

Insert after the for loop:

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

C)

Append to the body of the for loop:

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

D)

Insert immediately before the for loop:

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

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

**Answer:** A

#### NEW QUESTION 464

- (Topic 3)

What is one main REST security design principle?

- A. separation of privilege
- B. password hashing
- C. confidential algorithms
- D. OAuth

**Answer:** A

#### Explanation:

Separation of Privilege: Granting permissions to an entity should not be purely based on a single condition, a combination of conditions based on the type of resource is a better idea.

<https://restfulapi.net/security-essentials/#:~:text=REST%20Security%20Design%20Principles&text=Least%20Privilege%3A%20An%20entity%20should,when%20no%20longer%20in%20use.>

#### NEW QUESTION 468

- (Topic 3)

Refer to the exhibit.

```
DSW2#sh spanning-tree vlan 10
VLAN0010
Spanning tree enabled protocol ieee
Root ID Priority 10
Address 0013.80f9.8880
Cost 2
Port 9 (FastEthernet1/0/7)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 4106 (priority 4096 sys-id-ext 10)
Address 0019.7363.4300
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type

Fa1/0/7 Root FWD 2 128.9 P2p
Fa1/0/10 Desg FWD 4 128.12 P2p
Fa1/0/11 Desg FWD 2 128.13 P2p
Fa1/0/12 Desg FWD 2 128.14 P2p

DSW2#
*Mar 3 07:29:24.854: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa1/0/7
with BPDU Guard enabled. Disabling port.
*Mar 3 07:29:24.854: %PM-4-ERR_DISABLE: bpduguard error detected on Fa1/0/7, put
ting Fa1/0/7 in err-disable state
*Mar 3 07:29:24.879: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa1/0/7
with BPDU Guard enabled. Disabling port.
*Mar 3 07:29:25.869: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtherne
t1/0/7, changed state to down
*Mar 3 07:29:26.884: %LINK-3-UPDOWN: Interface FastEthernet1/0/7, changed state
to down
```

An engineer entered the command no spanning-tree bpduguard enable on interface Fa 1/0/7. What is the effect of this command on Fa 1/0/7?

- A. It remains in err-disabled state until the shutdown/no shutdown command is entered in the interface configuration mode.
- B. It remains in err-disabled state until the errdisable recovery cause failed-port-state command is entered in the global configuration mode.
- C. It remains in err-disabled state until the no shutdown command is entered in the interface configuration mode.
- D. It remains in err-disabled state until the spanning-tree portfast bpduguard disable command is entered in the interface configuration mode.

**Answer:** A

**Explanation:**

sw2#show errdisable recovery ErrDisable Reason Timer Status

```

arp-inspection Disabled bpduguard Disabled
channel-misconfig (STP) Disabled dhcp-rate-limit Disabled
dtp-flap Disabled gbic-invalid Disabled inline-power Disabled l2ptguard Disabled link-flap Disabled mac-limit Disabled
link-monitor-failure Disabled loopback Disabled
oam-remote-failure Disabled pagp-flap Disabled
port-mode-failure Disabled pppoe-ia-rate-limit Disabled psecure-violation Disabled security-violation Disabled sfp-config-mismatch Disabled storm-control Disabled
udld Disabled
unicast-flood Disabled sw2#
```

**NEW QUESTION 471**

- (Topic 3)

```
Router#show access-lists
Extended IP access list 100
 10 permit ip 192.168.0.0 0.0.255.255 any
 20 permit ip 172.16.0.0 0.0.15.255 any
```

Refer to the exhibit. Which command set must be added to permit and log all traffic that comes from 172.20.10.1 in interface GigabitEthernet0/1 without impacting the functionality of the access list?

- ☐ Router(config)#no access-list 100 permit ip 172.16.0.0 0.0.15.255 any  
Router(config)#access-list 100 permit ip 172.16.0.0 0.0.15.255 any log  
Router(config)#interface GigabitEthernet0/1  
Router(config-if)#access-group 100 in
- ☐ Router(config)#access-list 100 seq 5 permit ip host 172.20.10.1 any log  
Router(config)#Interface GigabitEthernet0/1  
Router(config-if)#access-group 100 in
- ☐ Router(config)#ip access-list extended 100  
Router(config-ext-nacl)#5 permit ip 172.20.10.0 0.0.0.255 any log  
Router(config)#interface GigabitEthernet0/1  
Router(config-if)#access-group 100 in
- ☐ Router(config)#access-list 100 permit ip host 172.20.10.1 any log  
Router(config)#Interface GigabitEthernet0/1  
Router(config-if)#access-group 100 in



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

**Answer: B**

**NEW QUESTION 475**

DRAG DROP - (Topic 3)

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

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

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

**NEW QUESTION 477**

- (Topic 3)

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

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

**Answer: A**

**Explanation:**

Fabric Enabled WLC:

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

For WLC Fabric Integration:

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

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

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

**NEW QUESTION 481**

- (Topic 3)

Which two characteristics apply to the endpoint security aspect of the Cisco Threat Defense architecture? (Choose two.)

- A. detect and black ransomware in email attachments
- B. outbound URL analysis and data transfer controls
- C. user context analysis
- D. blocking of fileless malware in real time
- E. cloud-based analysis of threats



**Answer:** BD

**NEW QUESTION 483**

- (Topic 3)

What is a TLOC in a Cisco SD-WAN deployment?

- A. value that identifies a specific tunnel within the Cisco SD-WAN overlay
- B. identifier that represents a specific service offered by nodes within the Cisco SD-WAN overlay
- C. attribute that acts as a next hop for network prefixes
- D. component set by the administrator to differentiate similar nodes that offer a common service

**Answer:** D

**Explanation:**

A TLOC is a Transport Locator that represents an attachment point where a Cisco WAN Edge device connects to a WAN transport. A TLOC is uniquely identified by a tuple of three values - (System-IP address, Color, Encapsulation).

A TLOC route consists of all required information needed by a remote peer in order to establish an overlay tunnel with that TLOC. This includes private and public IP addresses and ports, site-id, preference, weight, status, encapsulation info such as encryption and authentication parameters, and much more.

**NEW QUESTION 487**

- (Topic 3)

Refer to the exhibit .

```
restconf
|
ip http server
ip http authentication local
ip http secure-server
|
```

Which command must be configured for RESTCONF to operate on port 8888?

- A. ip http port 8888
- B. restconf port 8888
- C. ip http restconf port 8888
- D. restconf http port 8888

**Answer:** A

**NEW QUESTION 489**

- (Topic 3)

How does NETCONF YANG represent data structures?

- A. as strict data structures denned by RFC 6020
- B. in an XML tree format
- C. in an HTML format
- D. as modules within a tree

**Answer:** A

**NEW QUESTION 490**

- (Topic 3)

Refer to the exhibit.

```
access-list 1 permit 10.1.1.0 0.0.0.31
ip nat pool CISCO 209.165.201.1 209.165.201.30 netmask 255.255.255.224
ip nat inside source list 1 pool CISCO
```

What are two effect of this configuration? (Choose two.)

- A. Inside source addresses are translated to the 209.165.201.0/27 subnet.
- B. It establishes a one-to-one NAT translation.
- C. The 10.1.1.0/27 subnet is assigned as the inside global address range.
- D. The 209.165.201.0/27 subnet is assigned as the outside local address range.
- E. The 10.1.1.0/27 subnet is assigned as the inside local addresses.

**Answer:** AE

**NEW QUESTION 495**

- (Topic 3)

Refer to the exhibit.

```
Router#show policy-map control-plane
Control Plane

Service-policy input: CoPP

Class-map: class-telnet (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match: access-group 100
 police:
 cir 100000 bps, bc 3125 bytes
 conformed 0 packets, 0 bytes; actions:
 transmit
 exceeded 0 packets, 0 bytes; actions:
 drop
 conformed 0 bps, exceed 0 bps

Class-map: class-default (match-any)
 56 packets, 9874 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match: any

Router#show access-list 100
Extended IP access list 100
 10 permit tcp any any eq telnet
```

Which commands are required to allow SSH connection to the router?

- A)
- ```
Router(config)#access-list 100 permit udp any any eq 22
Router(config)#access-list 101 permit tcp any any eq 22
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 101
Router(config)#policy-map CoPP
Router(config-pmap)#police 100000 conform-action transmit
```
- B)
- ```
Router(config)#access-list 100 permit tcp any eq 22 any
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 10
Router(config)#policy-map CoPP
Router(config-pmap)#class class-ssh
Router(config-pmap-c)#police 100000 conform-action transmit
```
- C)
- ```
Router(config)#access-list 10 permit tcp any eq 22 any
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 10
Router(config)#policy-map CoPP
Router(config-pmap)#class class-ssh
Router(config-pmap-c)#police 100000 conform-action transmit
```
- D)

```
Router(config)#access-list 100 permit tcp any any eq 22
Router(config)#access-list 101 permit tcp any any eq 22
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 101
Router(config)#policy-map CoPP
Router(config-pmap)#class class-ssh
Router(config-pmap-c)#police 100000 conform-action transmit
```

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

Answer: D

NEW QUESTION 498

- (Topic 3)

Which two Cisco SD-WAN components exchange OMP information?

- A. vAnaiytlcs
- B. vSmart
- C. WAN Edge
- D. vBond
- E. vManage

Answer: BC

NEW QUESTION 500

- (Topic 3)

```
ip sla 100
  udp-echo 10.10.10.15 6336
  frequency 30
```

Refer to the exhibit. An engineer has configured an IP SLA for UDP echo's. Which command is needed to start the IP SLA to test every 30 seconds and continue until stopped?

- A. ip sla schedule 100 start-time now life forever
- B. ip sla schedule 30 start-time now life forever
- C. ip sla schedule 100 start-time now life 30
- D. ip sla schedule 100 life forever

Answer: A

NEW QUESTION 501

- (Topic 3)

Refer to the exhibit.

```
flow monitor FLOW-MONITOR-1
  record netflow ipv6 original-input
  exit
!
sampler SAMPLER-1
  mode deterministic 1 out-of 2
  exit
!
ip cef
ipv6 cef
!
interface GigabitEthernet 0/0/0
  ipv6 address 2001:DB8:2:ABCD::2/48
  ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
!
```

What is the effect of introducing the sampler feature into the Flexible NetFlow configuration on the router?

- A. NetFlow updates to the collector are sent 50% less frequently.
- B. Every second IPv4 packet is forwarded to the collector for inspection.
- C. CPU and memory utilization are reduced when compared with what is required for full NetFlow.
- D. The resolution of sampling data increases, but it requires more performance from the router.

Answer: C

NEW QUESTION 502

DRAG DROP - (Topic 3)

Drag and drop the characteristics from the left to the table types on the right.

used to make Layer 2 forwarding decisions	MAC Address Table
used to build IP routing tables	
records MAC address, port of arrival, VLAN and time stamp	TCAM Table
stores ACL, QoS, and other upper-layer information	

- A. Mastered
 B. Not Mastered

Answer: A

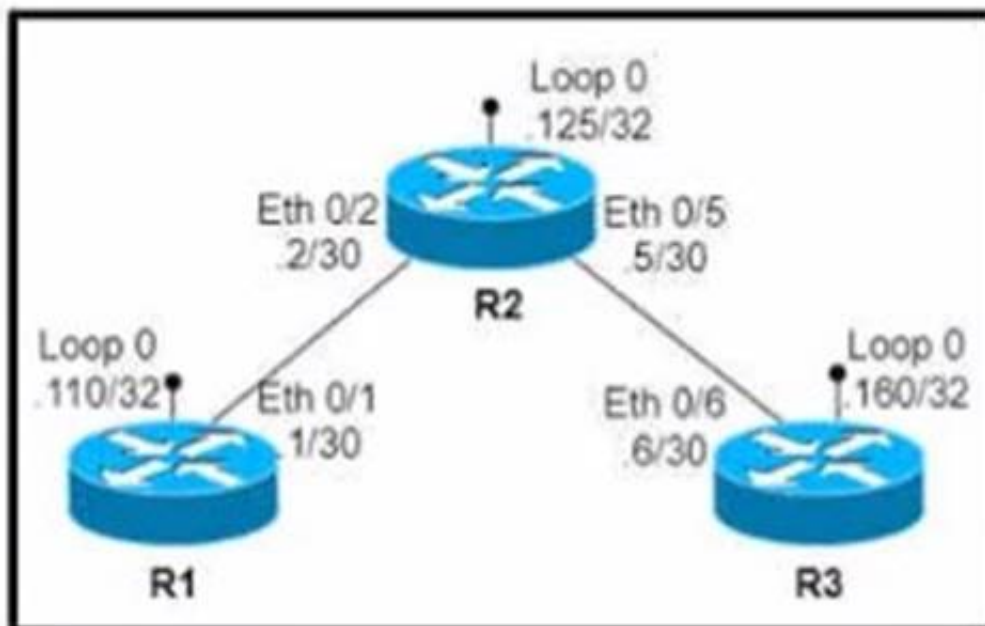
Explanation:

used to make Layer 2 forwarding decisions	MAC Address Table
used to build IP routing tables	
records MAC address, port of arrival, VLAN and time stamp	TCAM Table
stores ACL, QoS, and other upper-layer information	

NEW QUESTION 504

- (Topic 3)

Refer to the exhibit.



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

A)

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

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

B)

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

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

C)

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

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

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

D)

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

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

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

Answer: D

NEW QUESTION 507

- (Topic 3)

What is an emulated machine that has dedicated compute memory, and storage resources and a fully installed operating system?

- A. Container
- B. Mainframe
- C. Host
- D. virtual machine

Answer: B

NEW QUESTION 509

- (Topic 3)

What is one benefit of adopting a data modeling language?

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

Answer: B

NEW QUESTION 510

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 514

- (Topic 3)

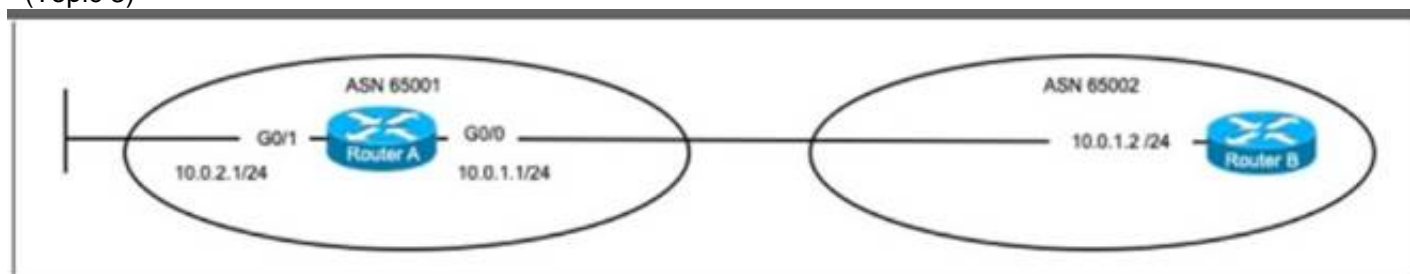
Which function does a fabric AP perform in a cisco SD-access deployment?

- A. It updates wireless clients' locations in the fabric
- B. It connects wireless clients to the fabric.
- C. It manages wireless clients' membership information in the fabric
- D. It configures security policies down to wireless clients in the fabric.

Answer: B

NEW QUESTION 519

- (Topic 3)



Refer to the exhibit. An engineer must configure an eBGP neighborship to Router B on Router A. The network that is connected to G0/1 on Router A must be advertised to Router

A. Which configuration should be applied? A)

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

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

C)

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

D)

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

B. Option A

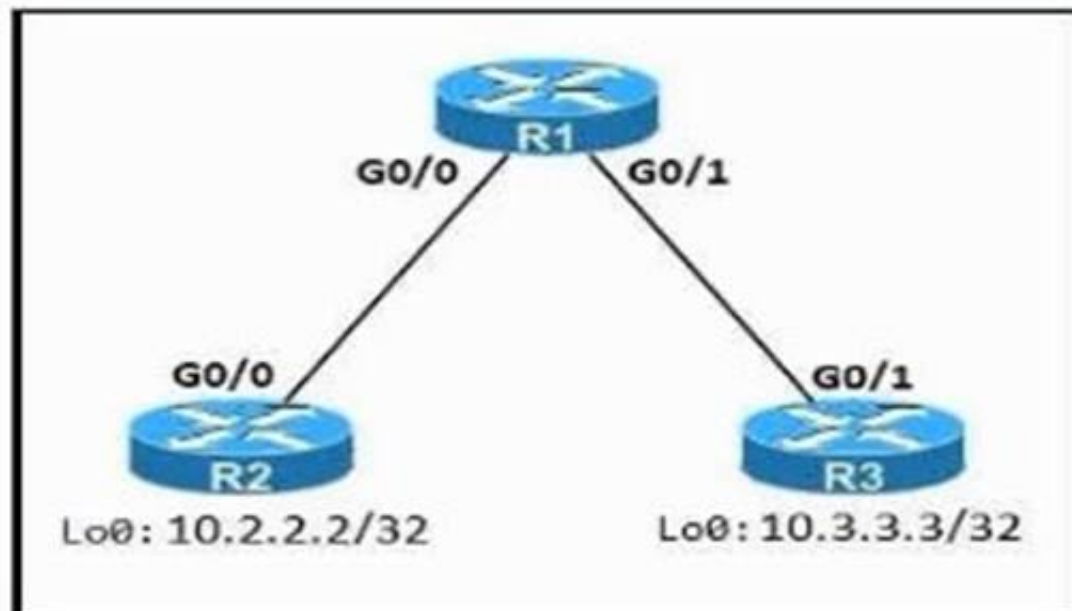
- C. Option B
- D. Option C
- E. Option D

Answer: C

NEW QUESTION 521

- (Topic 3)

Refer to the exhibit.



An engineer must deny Telnet traffic from the loopback interface of router R3 to the Loopback interface of router R2 during, the weekend hours. All other traffic between the loopback interfaces of routers R3 and R2 must be allowed at all times Which command set accomplishes this task?

A)

```

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

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

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

```

B)

```

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

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

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

```

C)

```

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

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

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

```

D)

```

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

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

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

```

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

Answer: D

Explanation:

We cannot filter traffic that is originated from the local router (R3 in this case) so we can only configure the ACL on R1 or R2. "Weekend hours" means from Saturday morning through Sunday night so we have to configure: "periodic weekend 00:00 to 23:59". Note: The time is specified in 24-hour time (hh:mm), where the hours range from 0 to 23 and the minutes range from 0 to 59.

NEW QUESTION 523

- (Topic 2)

AN engineer is implementing MPLS OAM to monitor traffic within the MPLS domain. Which action must the engineer perform to prevent from being forwarded beyond the service provider domain when the LSP is down?

- A. Disable IP redirects only on outbound interfaces
- B. Implement the destination address for the LSP echo request packet in the 127.x.y.z/8 network
- C. Disable IP redirects on all ingress interfaces
- D. Configure a private IP address as the destination address of the headend router of Cisco MPLS TE.

Answer: C

NEW QUESTION 527

- (Topic 2)

A network engineer must configure a router to send logging messages to a syslog server based on these requirements:

? uses syslog IP address: 10.10.10.1

? uses a reliable protocol

? must not use any well-known TCP/UDP ports

Which configuration must be used?

A. logging host 10.10.10.1 transport tcp port 1024

B. logging origin-id 10.10.10.1

C. logging host 10.10.10.1 transport udp port 1023

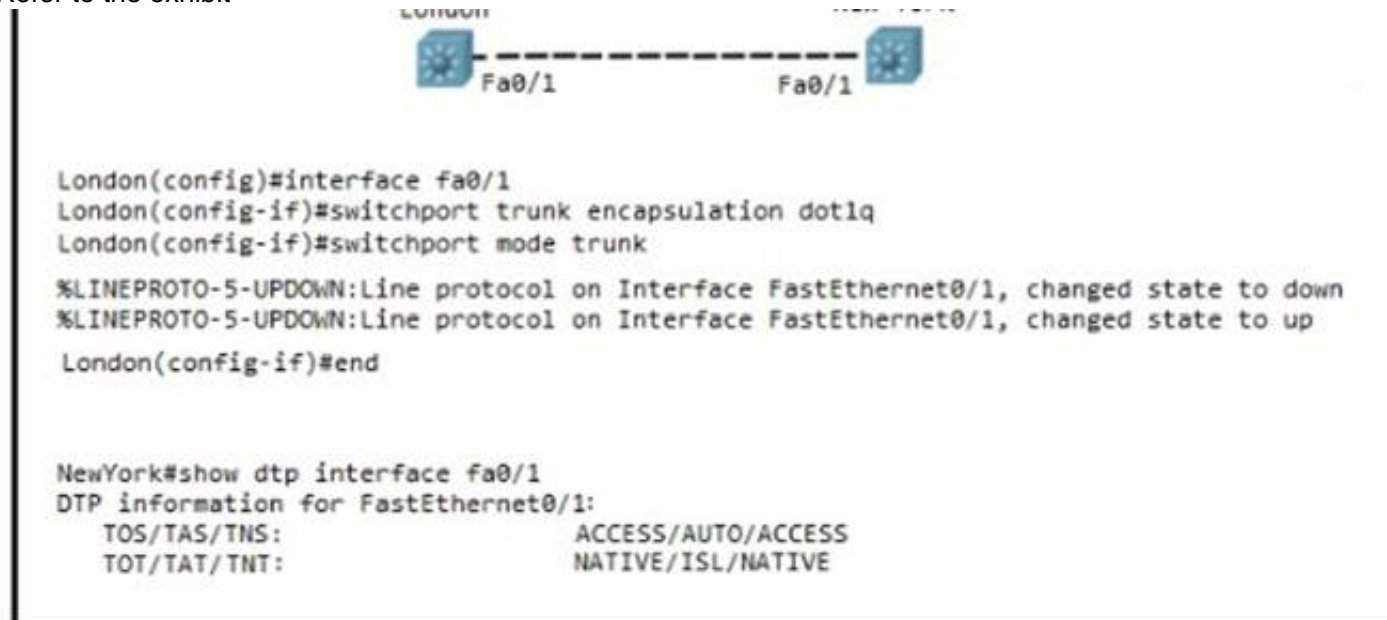
D. logging host 10.10.10.1 transport udp port 1024

Answer: A

NEW QUESTION 531

- (Topic 2)

Refer to the exhibit



```

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

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

London(config-if)#end

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

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

A)

```

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

B)

```

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

C)

```

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

D)

```

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

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

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

NEW QUESTION 536

- (Topic 2)

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

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

Answer: B

NEW QUESTION 539

- (Topic 2)

What is provided by the Stealthwatch component of the Cisco Cyber Threat Defense solution?

- A. real-time threat management to stop DDoS attacks to the core and access networks
- B. real-time awareness of users, devices and traffic on the network
- C. malware control
- D. dynamic threat control for web traffic

Answer: B

Explanation:

"Cisco Stealthwatch collects and analyzes massive amounts of data to give even the largest, most dynamic networks comprehensive internal visibility and protection. It helps security operations teams gain real-time situational awareness of all users, devices, and traffic on the extended network so they can quickly and effectively respond to threats"

Page 1

<https://media.zones.com/images/pdf/cisco-stealthwatch-solution-overview.pdf>

NEW QUESTION 541

- (Topic 2)

In which two ways does TCAM differ from CAM? (Choose two.)

- A. CAM is used to make Layer 2 forwarding decisions, and TCAM is used for Layer 3 address lookups.
- B. The MAC address table is contained in CAM, and ACL and QoS Information is stored in TCAM.
- C. CAM is used by routers for IP address lookups, and TCAM is used to make Layer 2 forwarding decisions.
- D. CAM is used for software switching mechanisms, and TCAM is used for hardware switching mechanisms.
- E. The MAC address table is contained in TCAM, and ACL and QoS information is stored in CAM.

Answer: CE

NEW QUESTION 544

- (Topic 2)

How must network management traffic be treated when defining QoS policies?

- A. as delay-sensitive traffic in a low latency queue
- B. using minimal bandwidth guarantee
- C. using the same marking as IP routing
- D. as best effort

Answer: A

Explanation:

Low latency queuing (LLQ) adds a priority queue to CBWFQ from which delay-sensitive traffic, such as voice traffic, can be transmitted ahead of packets in other queues.

By configuring the quality of service (QoS), you can provide preferential treatment to specific types of traffic at the expense of other traffic types. Without QoS, the device offers best-effort service for each packet, regardless of the packet contents or size. The device sends the packets without any assurance of reliability, delay bounds, or throughput.

The following are specific features provided by QoS:

- ? Low latency
- ? Bandwidth guarantee
- ? Buffering capabilities and dropping disciplines
- ? Traffic policing
- ? Enables the changing of the attribute of the frame or packet header
- ? Relative services
- ? Modular QoS Command-Line Interface
- ? Supported QoS Features for Wired Access
- ? Hierarchical QoS

NEW QUESTION 548

DRAG DROP - (Topic 2)

A network engineer is adding an additional 10Gbps link to an existing 2x10Gbps LACP-based LAG to augment its capacity. Network standards require a bundle interface to be taken out of service if one of its member links goes down, and the new link must be added with minimal impact to the production network. Drag and drop the tasks that the engineer must perform from the left into the sequence on the right. Not all options are used.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 550

- (Topic 2)
What are two common sources of interference for Wi-Fi networks? (Choose two.)

- A. rogue AP
- B. conventional oven
- C. fire alarm
- D. LED lights
- E. radar

Answer: AE

NEW QUESTION 554

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

350-401 Practice Exam Features:

- * 350-401 Questions and Answers Updated Frequently
- * 350-401 Practice Questions Verified by Expert Senior Certified Staff
- * 350-401 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 350-401 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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