Cisco.350-401.vJul-204.by.Lounoyamo.435q

Number: 350-401
Passing Score: 800
Time Limit: 120
File Version: 42.0

Exam Code: 350-401
Exam Name: Implementing Cisco Enterprise Network Core Technologies (ENCOR)

Exam A

QUESTION 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

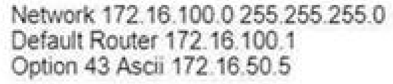
C. C0:39:83:25:258:5

D. 00:00:0c:07:ac:25

Correct Answer: D
Section:

QUESTION 2

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



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

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

A. configure option 43 Hex F104.AC10.3205

B. configure option 43 Hex F104.CA10.3205

C. configure dns-server 172.16.50.5

D. configure dns-server 172.16.100.1

Correct Answer: A
Section:
Explanation:

The Option 43 hexadecimal string is assembled as a sequence of the TLV values for the Option 43 suboption: Type + Length + Value. Type is always the suboption code 0xf1. Length is the number of controller management IP addresses times 4 in hex. Value is the IP address of the controller listed sequentially in hex.
On this question, there is 1 controller with management interface IP addresses 172.16.50.5/24. The type is 0xf1. The length is 1 * 4 = 8 = 0x04. The mgmt IP addresses 172.16.50.5 translate to ac.10.32.05 (0xac103205). When the string is assembled, it yields f108c0a80a05c0a80a14. The Cisco IOS command that is added to the DHCP scope is: option 43 hex f104ac103205

QUESTION 3

If a client's radio device receives a signal strength of -67 dBm and the noise floor is -85 dBm, what is the SNR value?

A. 15 dB

B. 16 dB

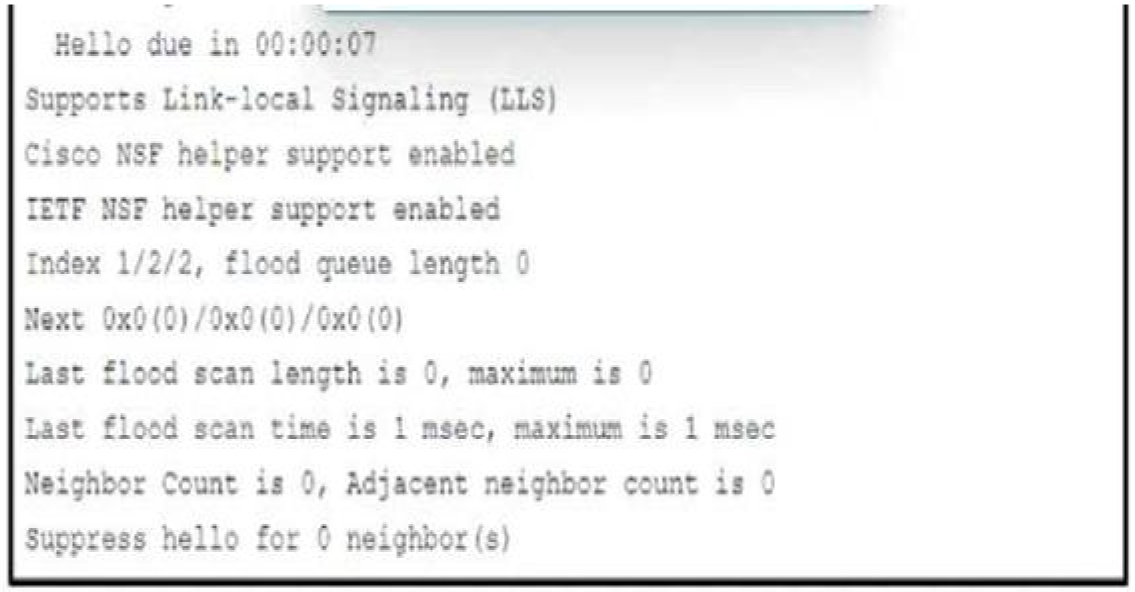
C. 18 dB

D. 20 dB

Correct Answer: C
Section:

QUESTION 4

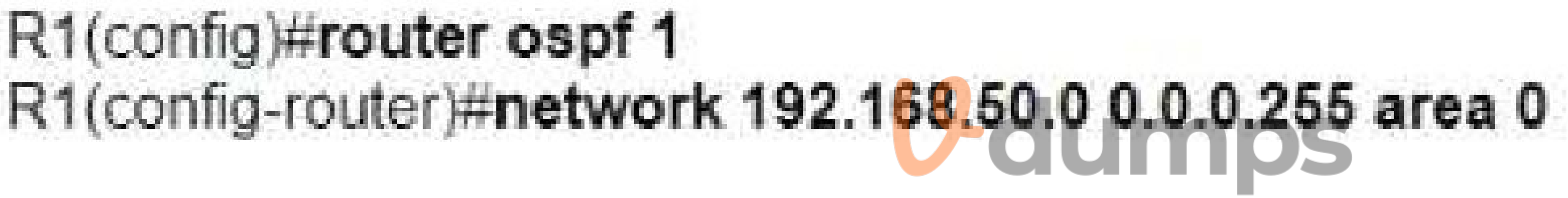
Refer to the exhibit.



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

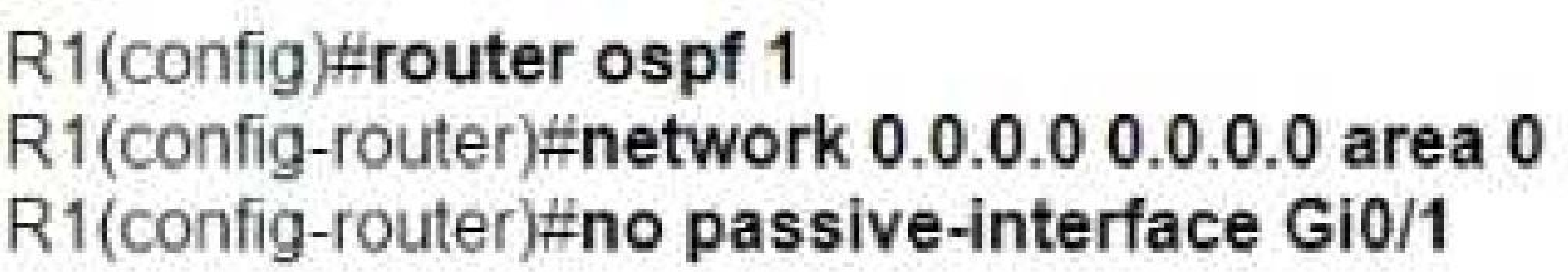
An engineer configures OSPF and wants to verify the configuration Which configuration is applied to this device?

A.



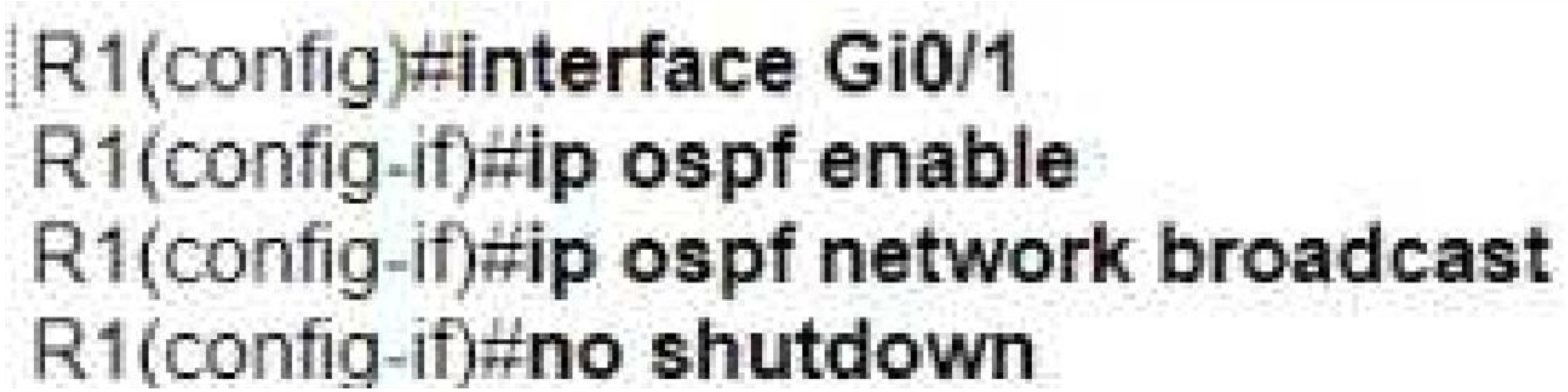
```
R1(config)#router ospf 1
R1(config-router)#network 192.168.50.0 0.0.0.255 area 0
```

B.



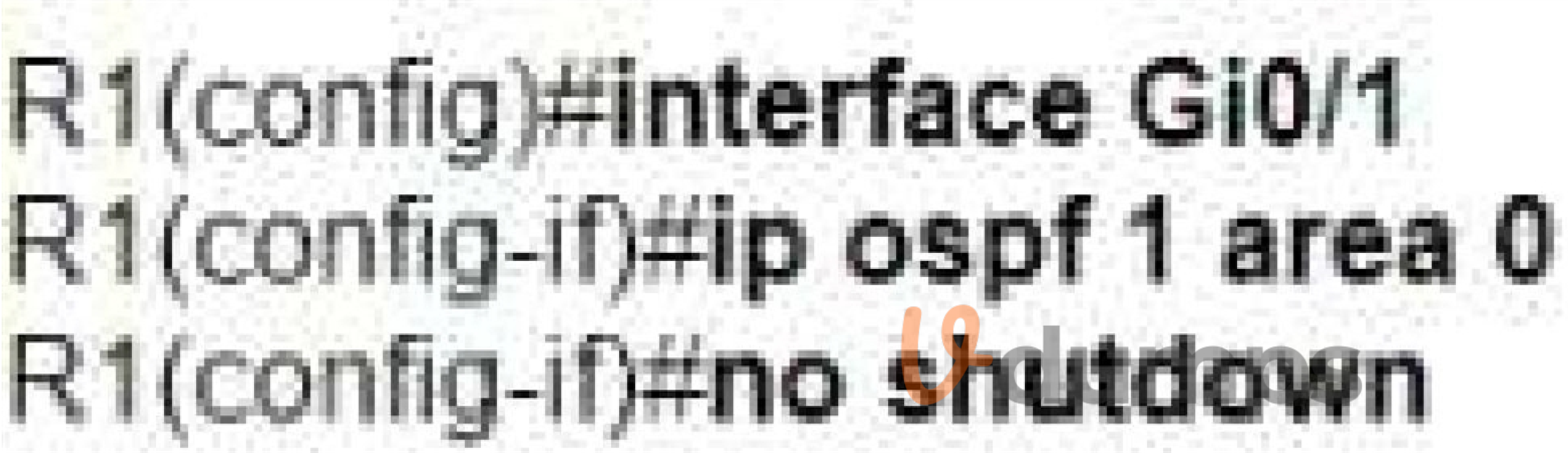
```
R1(config)#router ospf 1
R1(config-router)#network 0.0.0.0 0.0.0.0 area 0
R1(config-router)#no passive-interface Gi0/1
```

C.



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

D.



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

Correct Answer: C
Section:

QUESTION 5
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.

Correct Answer: B
Section:

QUESTION 6
In a Cisco SD-Access solution, which protocol is used by an extended node to connect to a single edge node?

A. VXLAN
B. IS-IS

C. 802 1Q

D. CTS

Correct Answer: C
Section:
Explanation:
SD-Access Extended Nodes provide the ability to extend the enterprise network by providing connectivity to non-carpeted spaces of an enterprise – commonly called the Extended Enterprise.
This allows network connectivity and management of IoT devices and the deployment of traditional enterprise end devices in outdoor and non-carpeted environments such as distribution centers, warehouses, or Campus parking lots.
This feature extends consistent, policy-based automation to Cisco Industrial Ethernet, Catalyst 3560- CX Compact, and Digital Building Series switches and enables segmentation for user endpoints and IoT devices connected to these nodes. Using Cisco DNA Center automation, switches in the extended node role are onboarded to their connected edge node using an 802.1Q trunk over an EtherChannel with one or multiple physical link members.
Extended nodes are discovered using zero-touch Plugand- Play.
Reference: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-designguide.html#Network_Components

QUESTION 7
An engineer must enable a login authentication method that allows a user to log in by using local authentication if all other defined authentication methods fail Which configuration should be applied?

A. aaa authentication login CONSOLE group radius local-case enable aaa

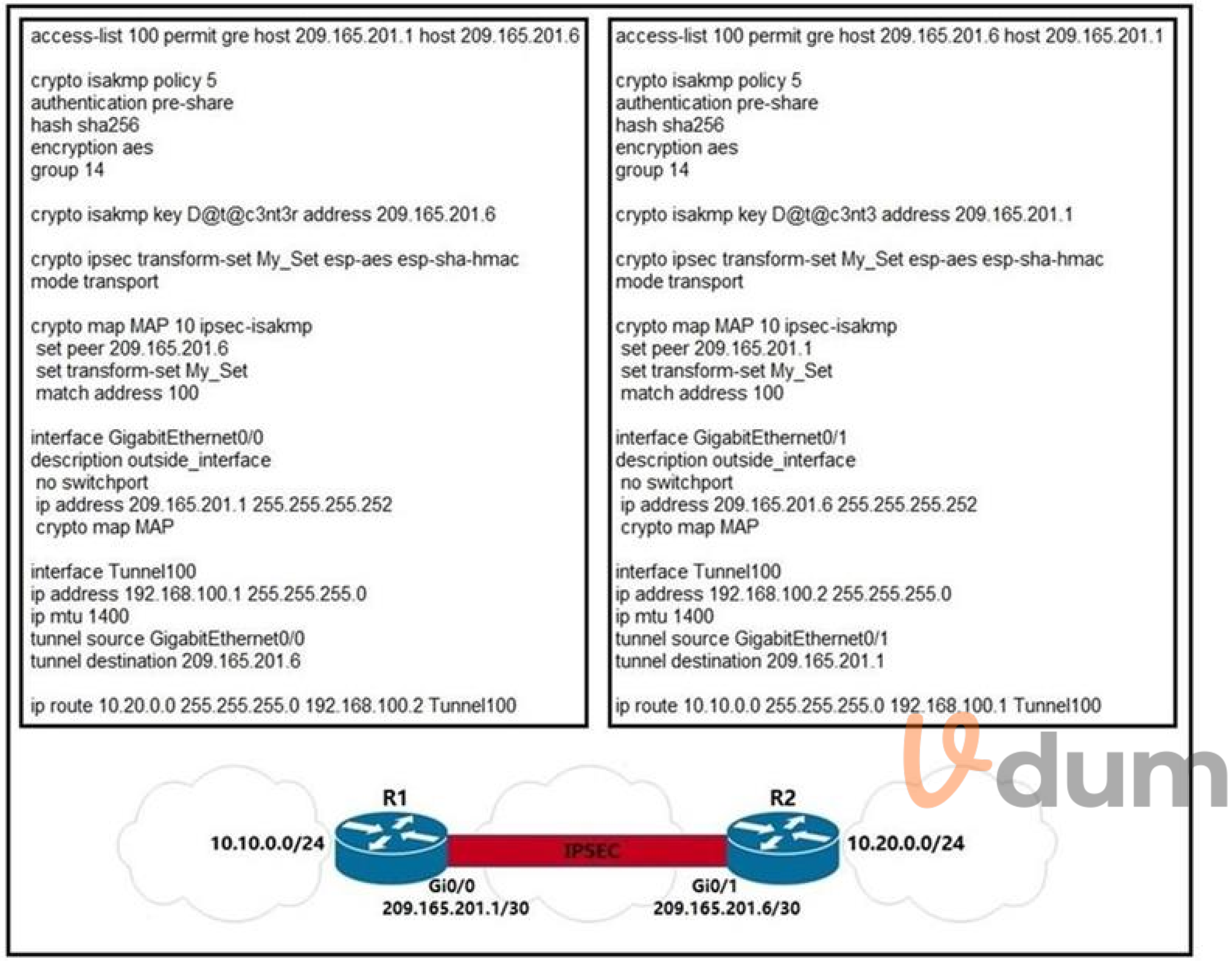
B. authentication login CONSOLE group radius local enable none

C. aaa authentication login CONSOLE group radius local enable

D. aaa authentication login CONSOLE group tacacs+ local enable

Correct Answer: D
Section:

QUESTION 8
Refer to the exhibit.



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

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

crypto isakmp key D@t@c3nt3r address 209.165.201.6

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

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

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

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

ip route 10.20.0.0 255.255.255.0 192.168.100.2 Tunnel100
```

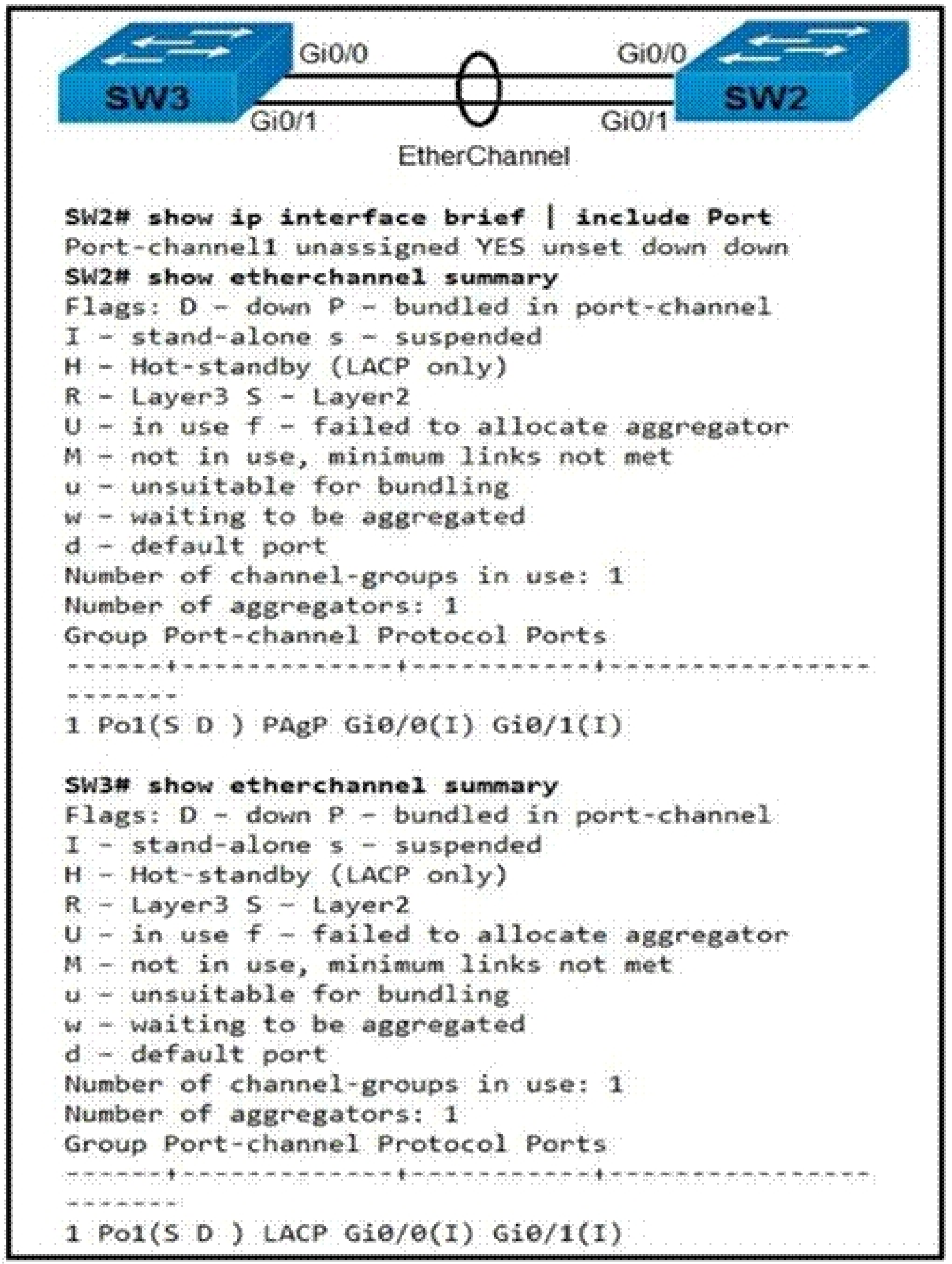
```
access-list 100 permit gre host 209.165.201.6 host 209.165.201.1

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

crypto isakmp key D@t@c3nt3 address 209.165.201.1

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

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

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

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

ip route 10.10.0.0 255.255.255.0 192.168.100.1 Tunnel100
```

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

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

Correct Answer: C, D
Section:

QUESTION 9
Refer to the exhibit.



```
SW2# show ip interface brief | include Port
Port-channel1 unassigned YES unset down down
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 ) PAgP Gi0/0(I) Gi0/1(I)

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

Which action resolves the EtherChannel issue between SW2 and SW3?

A. Configure switchport mode trunk on SW2.

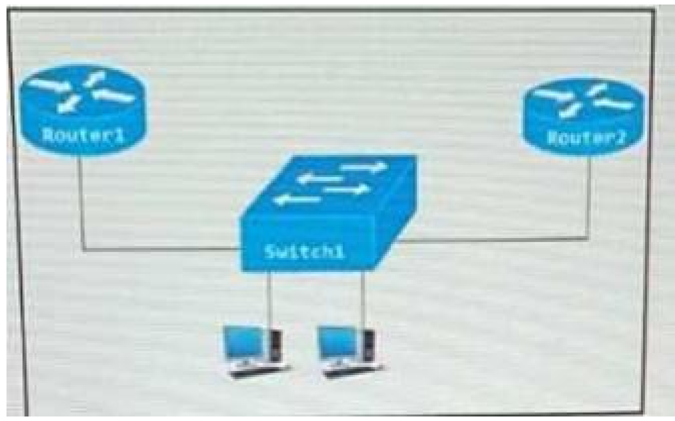
B. Configure switchport nonegotiate on SW3

C. Configure channel-group 1 mode desirable on both interfaces.

D. Configure channel-group 1 mode active on both interfaces.

Correct Answer: D
Section:

QUESTION 10
Refer to the exhibit.

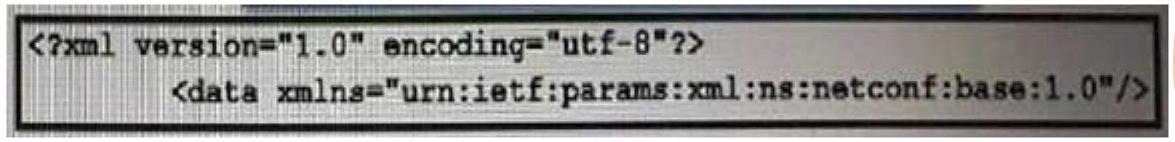


Router 1 is currently operating as the HSRP primary with a priority of 110 router1 fails and router2 take over the forwarding role. Which command on router1 causes it to take over the forwarding role when it return to service?

A. standby 2 priority
B. standby 2 preempt
C. standby 2 track
D. standby 2 timers

Correct Answer: B
Section:

QUESTION 11

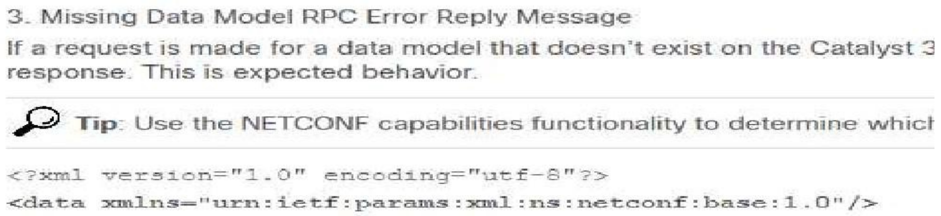


```
<?xml version="1.0" encoding="utf-8"?>
        <data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"/>
```

Refer to the exhibit. What does the error message relay to the administrator who is trying to configure a Cisco IOS device?

A. A NETCONF request was made for a data model that does not exist.
B. The device received a valid NETCONF request and serviced it without error.
C. A NETCONF message with valid content based on the YANG data models was made, but the request failed.
D. The NETCONF running datastore is currently locked.

Correct Answer: A
Section:
Explanation:



3. Missing Data Model RPC Error Reply Message

If a request is made for a data model that doesn't exist on the Catalyst 3
response. This is expected behavior.

Tip: Use the NETCONF capabilities functionality to determine whicl

```
<?xml version="1.0" encoding="utf-8"?>
<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"/>
```

Reference: https://www.cisco.com/c/en/us/support/docs/storagenetworking/management/200933-YANG-NETCONF-Configuration-Validation.html

QUESTION 12

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

A. ETR
B. ITR

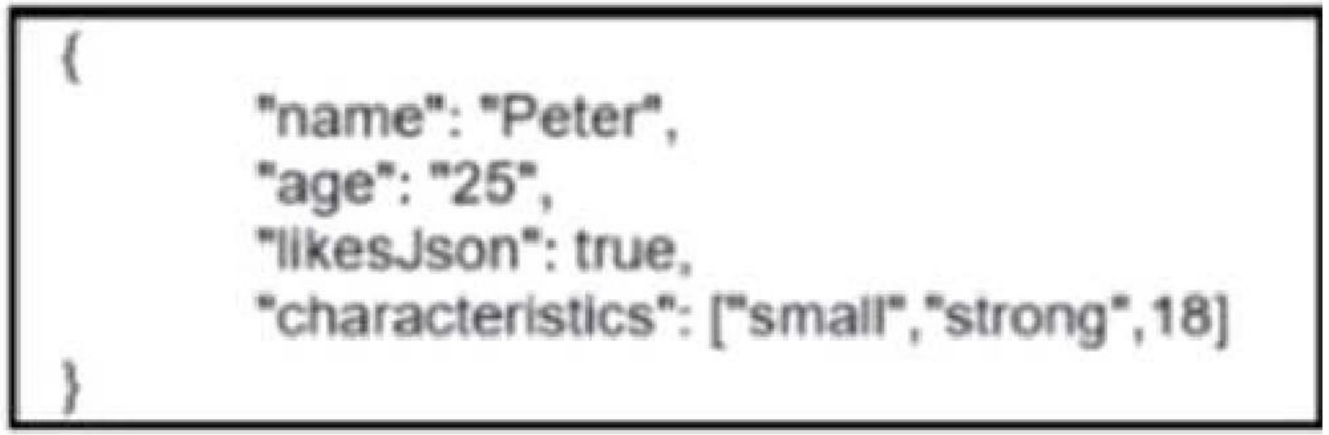
C. Proxy ETR

D. Proxy ITR

Correct Answer: C
Section:

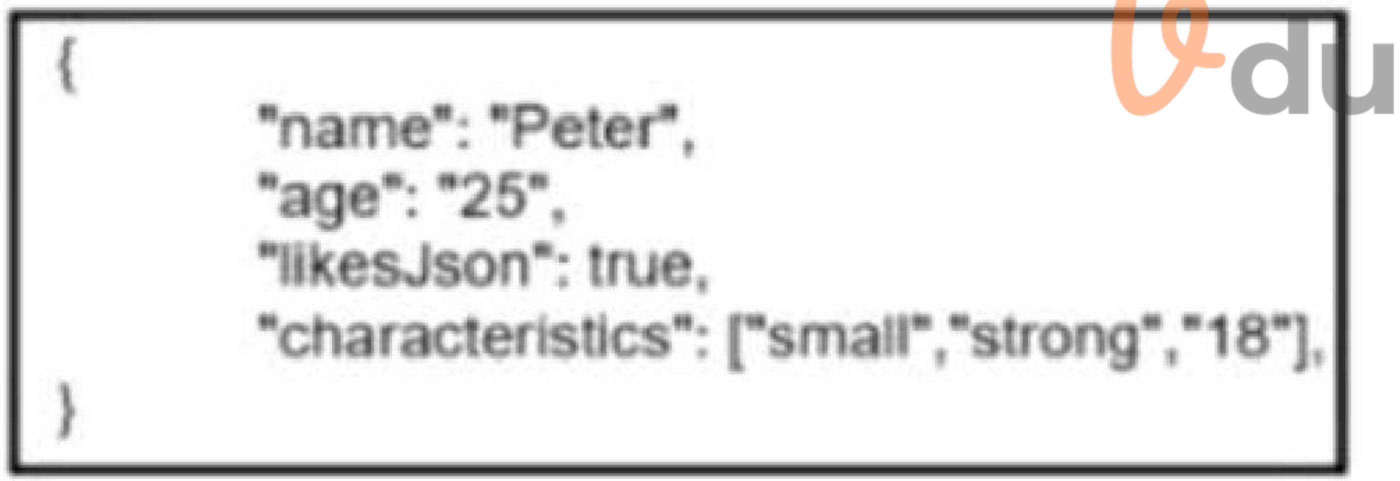
QUESTION 13
Which data is properly formatted with JSON?

A.



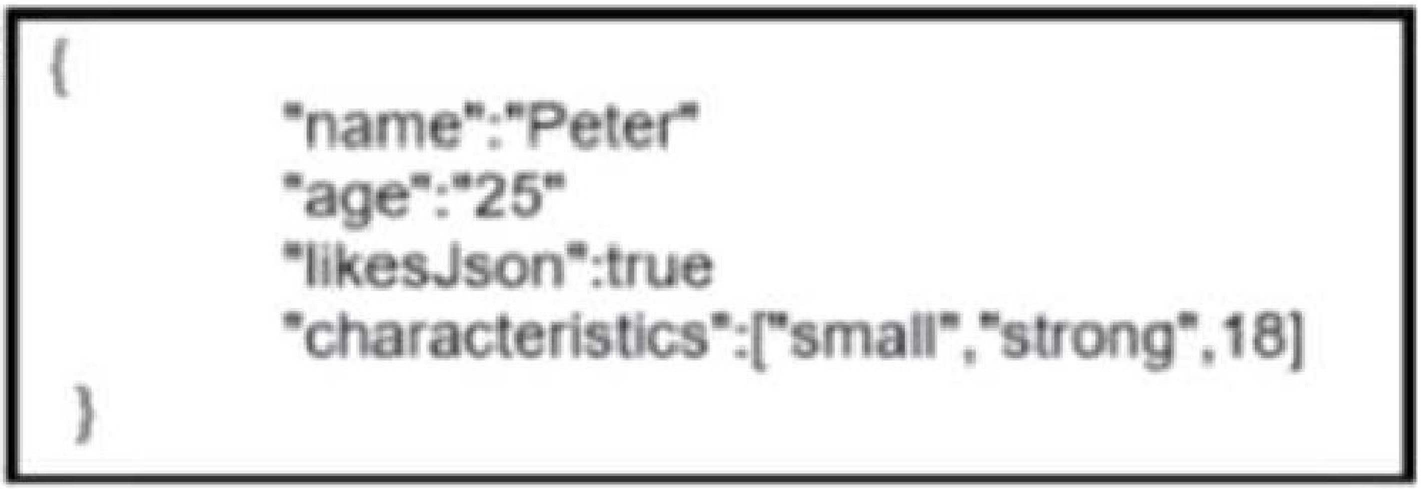
```
{
        "name": "Peter",
        "age": "25",
        "likesJson": true,
        "characteristics": ["small","strong",18]
}
```

B.



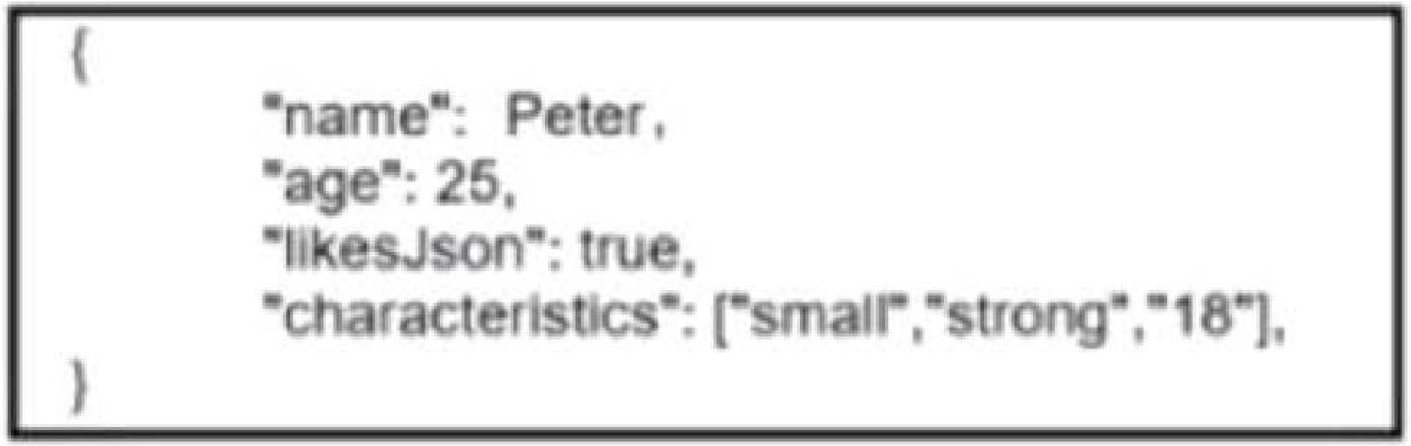
```
{
        "name": "Peter",
        "age": "25",
        "likesJson": true,
        "characteristics": ["small","strong","18"],
}
```

C.



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

D.



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

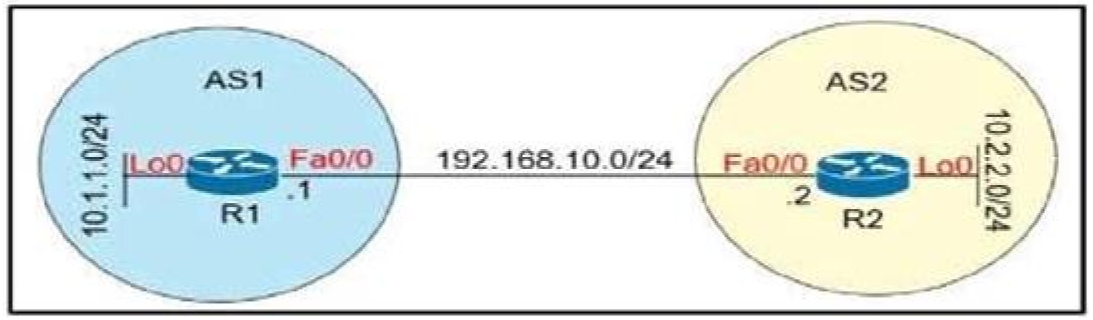
Correct Answer: A
Section:

QUESTION 14
How are the different versions of IGMP compatible?

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

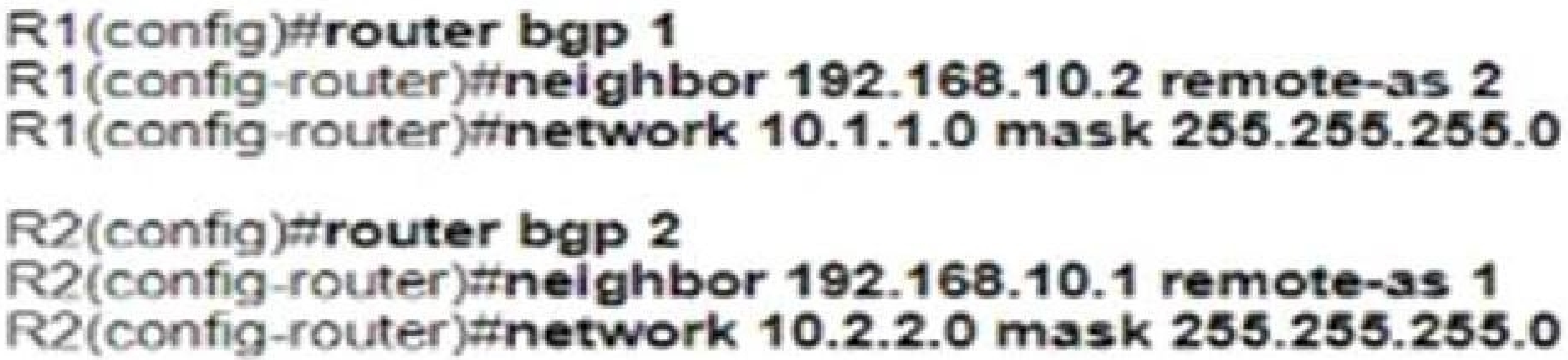
Correct Answer: A
Section:

QUESTION 15
Refer to the exhibit.



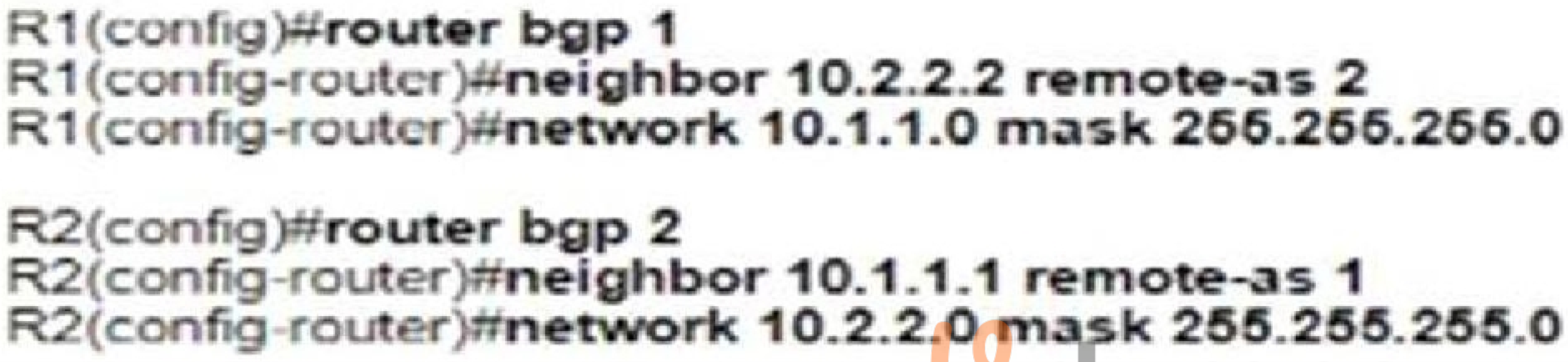
Which configuration establishes EBGP neighborship between these two directly connected neighbors and exchanges the loopback network of the two routers through BGP?

A.



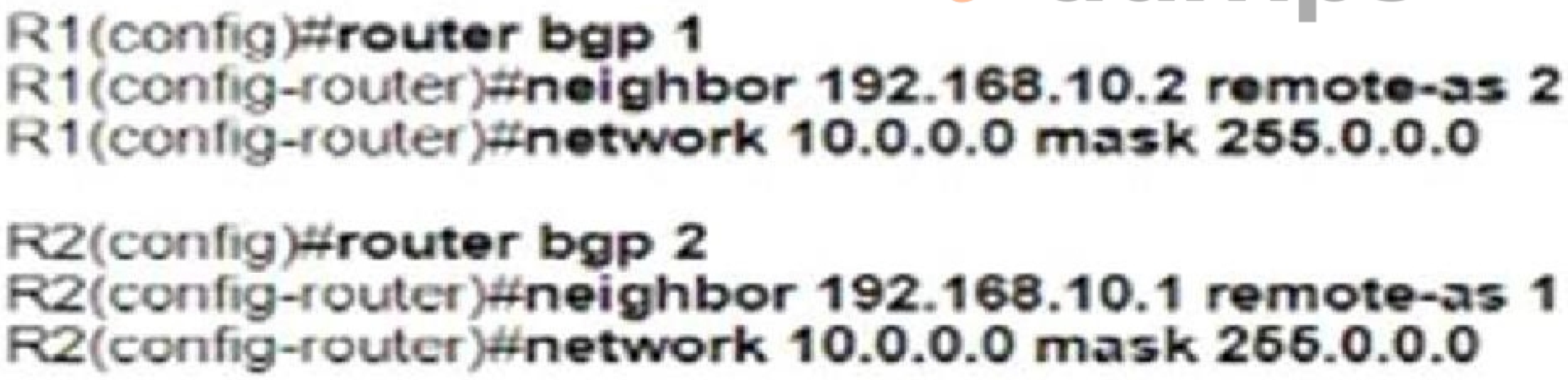
```
R1(config)#router bgp 1
R1(config-router)#neighbor 192.168.10.2 remote-as 2
R1(config-router)#network 10.1.1.0 mask 255.255.255.0

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

B.



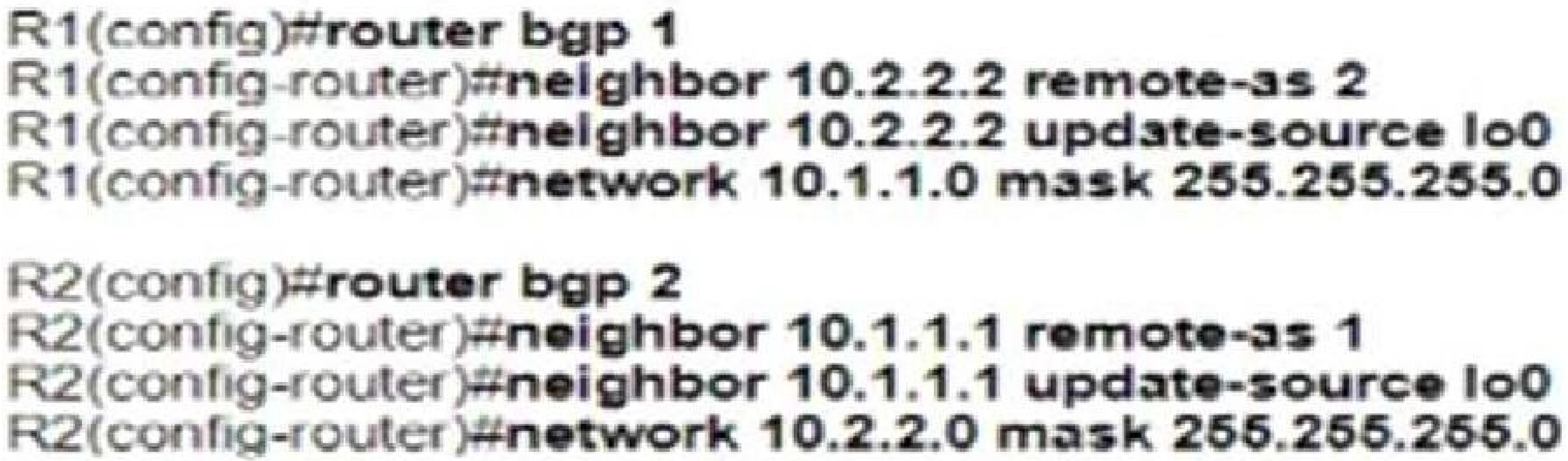
```
R1(config)#router bgp 1
R1(config-router)#neighbor 10.2.2.2 remote-as 2
R1(config-router)#network 10.1.1.0 mask 255.255.255.0

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

C.



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

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

D.



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

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

Correct Answer: A
Section:
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

QUESTION 16
In a Cisco SD-Access solution, what is the role of the Identity Services Engine?

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

Correct Answer: A
Section:

QUESTION 17
Which encryption hashing algorithm does NTP use for authentication?

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

Correct Answer: B
Section:
Explanation:
An example of configuring NTP authentication is shown below:

```
Router1(config)#ntp authentication-key 2 md5 itexamanswers
Router1(config)#ntp authenticate
Router1(config)#ntp trusted-key 2
```

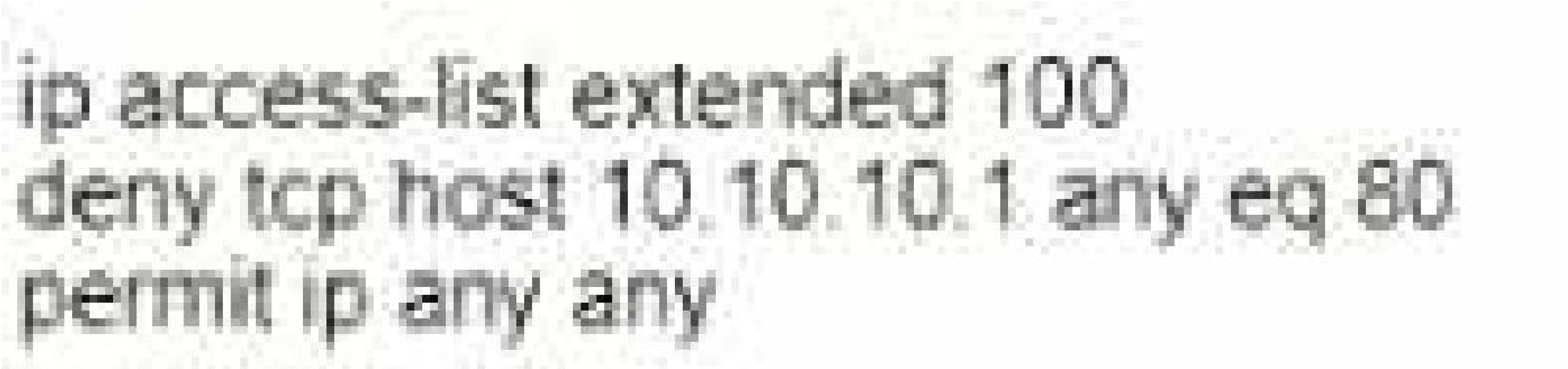
QUESTION 18
Which controller is capable of acting as a STUN server during the onboarding process of Edge devices?

A. vBond
B. vSmart
C. vManage
D. PNP server

Correct Answer: A
Section:

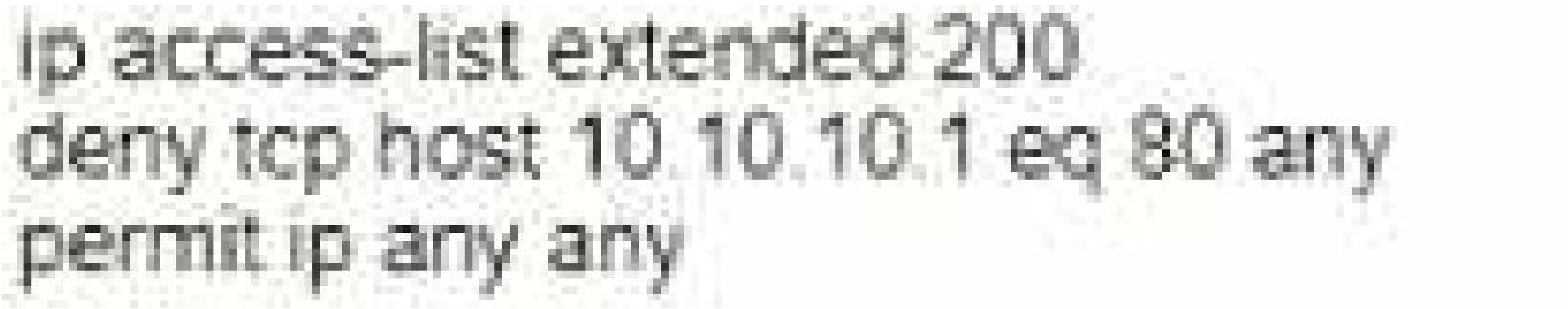
QUESTION 19
Which outbound access list, applied to the WAN interface of a router, permits all traffic except for http traffic sourced from the workstation with IP address 10.10.10.1?

A.



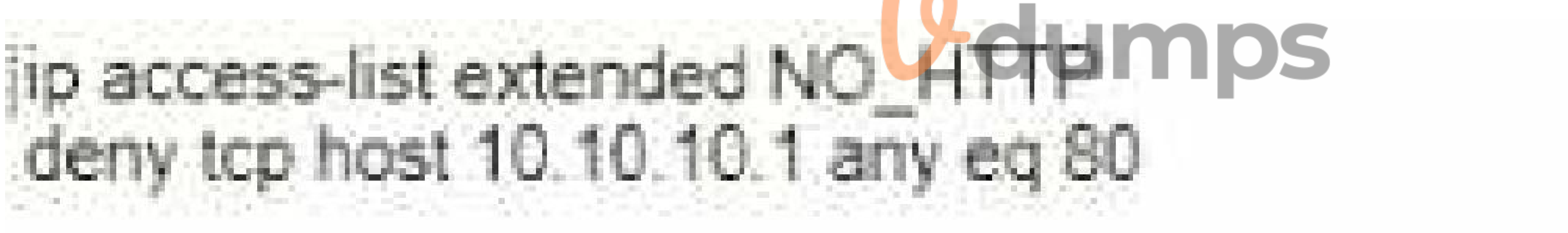
```
ip access-list extended 100
deny tcp host 10.10.10.1 any eq 80
permit ip any any
```

B.



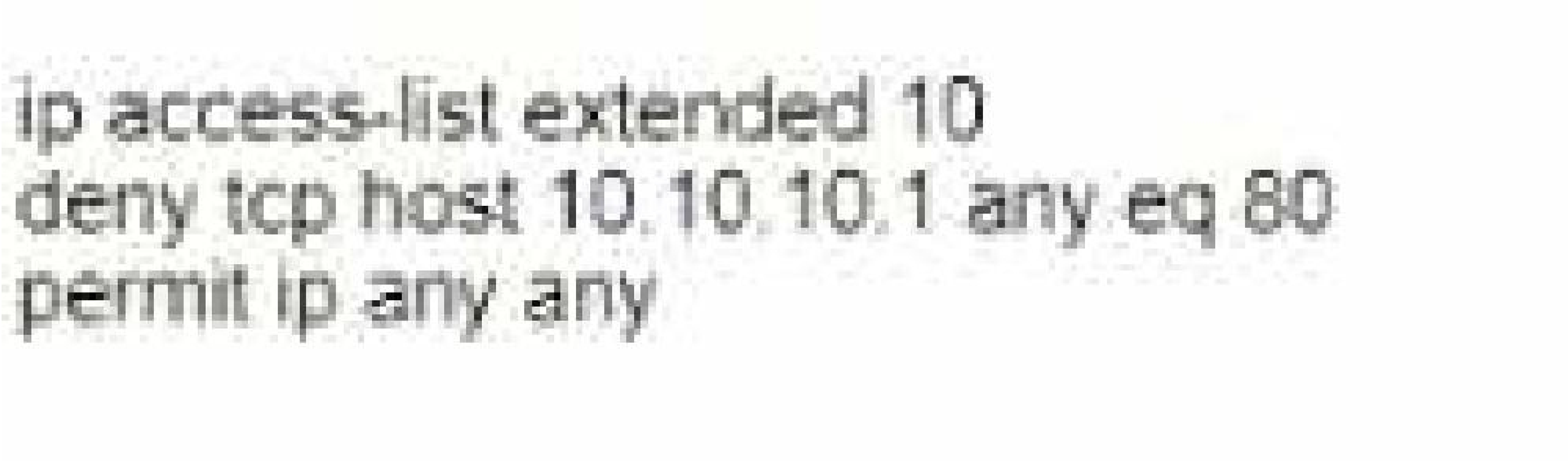
```
ip access-list extended 200
deny tcp host 10.10.10.1 eq 80 any
permit ip any any
```

C.



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

D.



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

Correct Answer: A

Section:

QUESTION 20
Which protocol does REST API rely on to secure the communication channel?

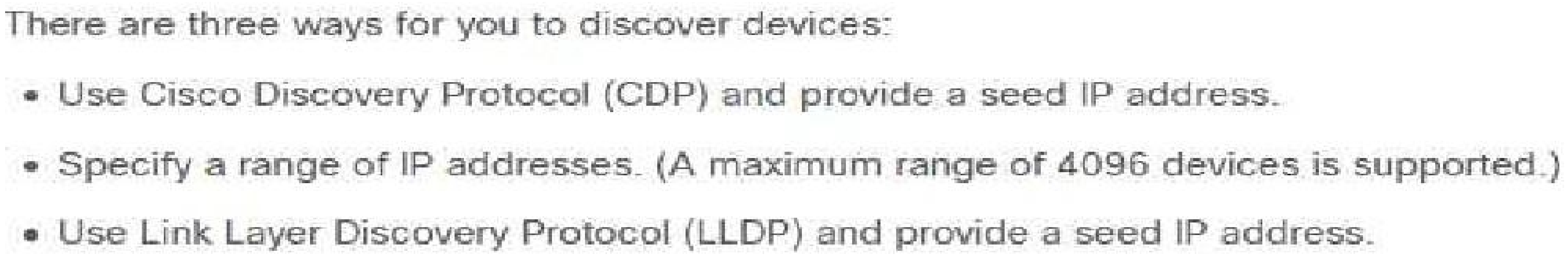
A. TCP
B. HTTPS
C. SSH
D. HTTP

Correct Answer: B
Section:
Explanation:
The REST API accepts and returns HTTP (not enabled by default) or HTTPS messages that containJavaScript Object Notation (JSON) or Extensible Markup Language (XML) documents. You can useany programming language to generate the messages and the JSON or XML documents thatcontain the API methods or Managed Object (MO) descriptions.
Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/rest_cfg/2_1_x/b_Cisco_APIC_REST_API_Configuration_Guide/b_Cisco_APIC_REST_API_Configuration_Guide_chapter_01.html

QUESTION 21
Which three methods does Cisco DNA Centre use to discover devices? (Choose three)

A. CDP
B. SNMP
C. LLDP
D. ping
E. NETCONF
F. a specified range of IP addresses

Correct Answer: A, C, F
Section:
Explanation:



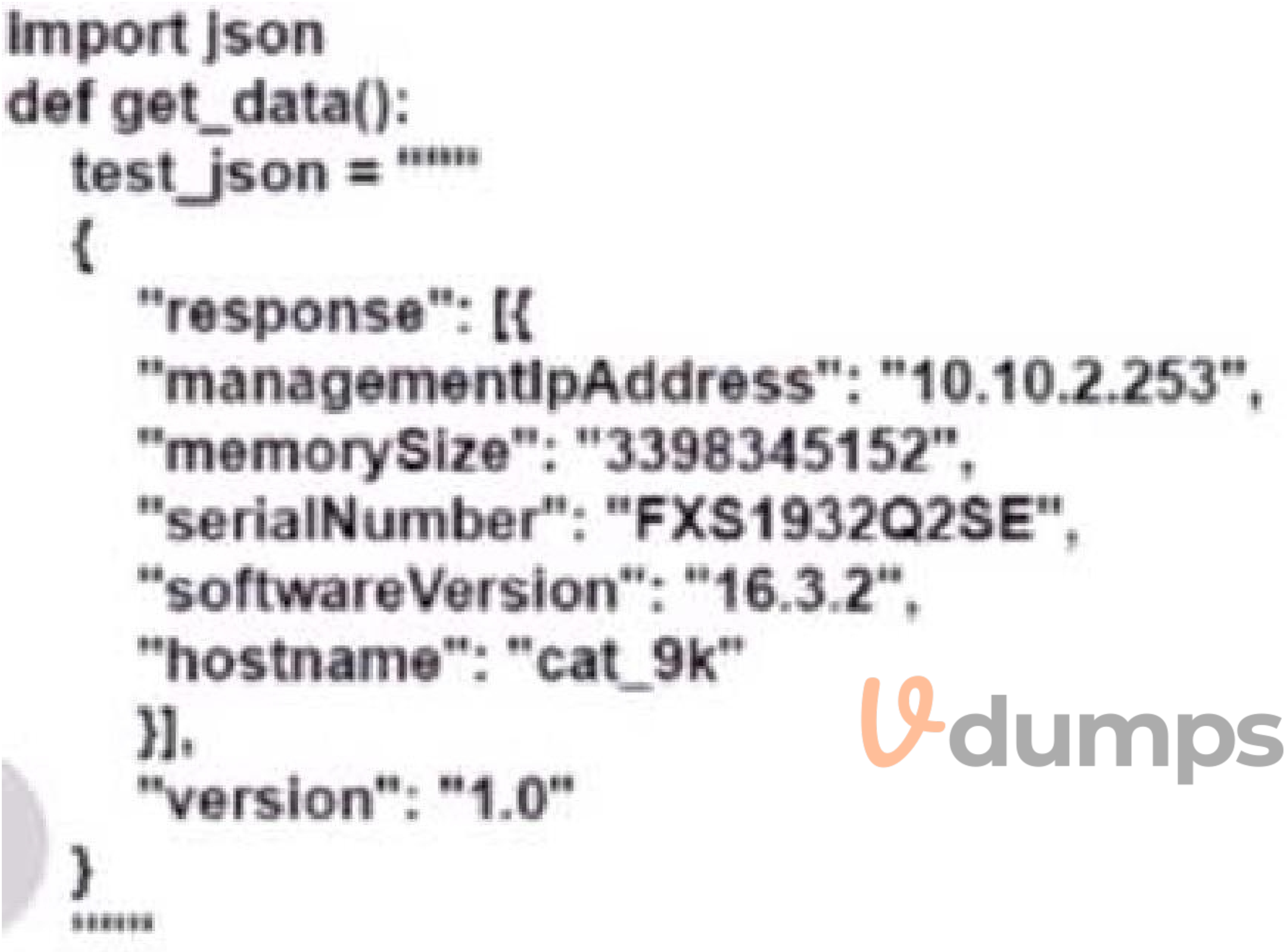
There are three ways for you to discover devices:

- Use Cisco Discovery Protocol (CDP) and provide a seed IP address.
- Specify a range of IP addresses. (A maximum range of 4096 devices is supported.)
- Use Link Layer Discovery Protocol (LLDP) and provide a seed IP address.

QUESTION 22

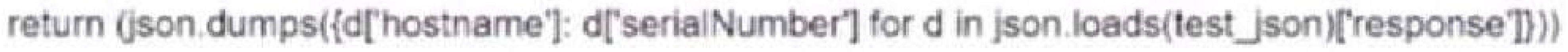
Which line must be added in the Python function to return the JSON object {"cat_9k":

"FXS193202SE")?



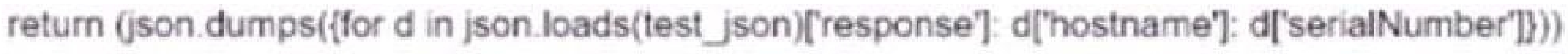
```
Import json
def get_data():
    test_json = """"""
    {
        "response": [{
        "managementIpAddress": "10.10.2.253",
        "memorySize": "3398345152",
        "serialNumber": "FXS1932Q2SE",
        "softwareVersion": "16.3.2",
        "hostname": "cat_9k"
        }],
        "version":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

A.



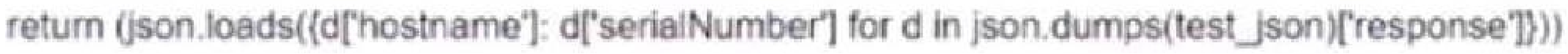
```
return (json.dumps({d['hostname']: d['serialNumber'] for d in json.loads(test_json)['response']}))
```

B.



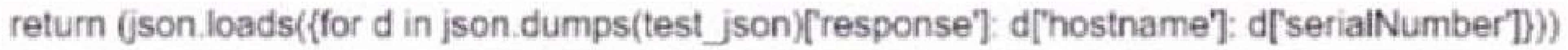
```
return (json.dumps({for d in json.loads(test_json)['response']: d['hostname']: d['serialNumber']}))
```

C.



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

D.



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

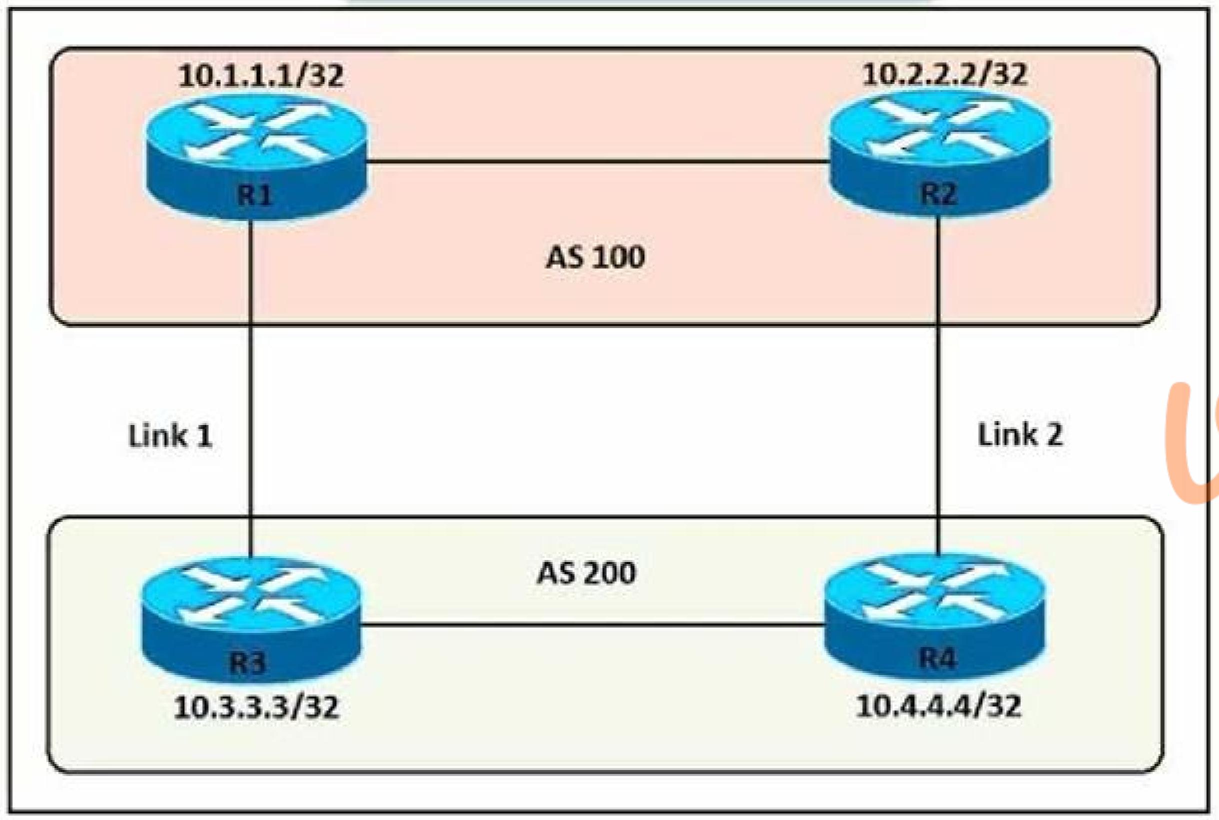
Correct Answer: D
Section:

QUESTION 23
What is a characteristic of a virtual machine?

A. It must be aware of other virtual machines, in order to allocate physical resources for them
B. It is deployable without a hypervisor to host it
C. It must run the same operating system as its host
D. It relies on hypervisors to allocate computing resources for it

Correct Answer: D
Section:

QUESTION 24
Refer to the exhibit.



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

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

Correct Answer: A
Section:
Explanation:
Local preference is an indication to the AS about which path has preference to exit the AS in order to reach a certain network. A path with a higher local preference is preferred. The default value for local preference is 100. Unlike the weight attribute, which is only relevant to the local router, local preference is an attribute that routers exchange in the same AS. The local preference is set with the "bgp default local-preference value" command. In this case, both R3 & R4 have exit links but R4 has higher local-preference so R4 will be chosen as the preferred exit point from AS 200.

QUESTION 25

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

A. mobility MAC on the 5520 cluster

B. mobility MAC on the 9800 WLC

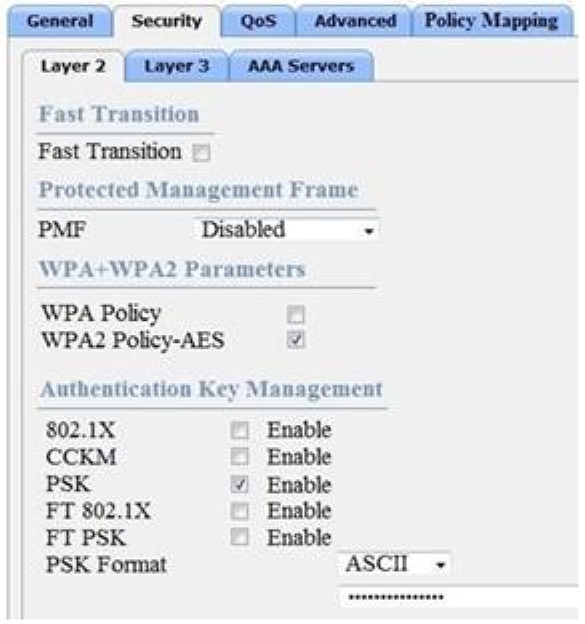
C. new mobility on the 5520 cluster

D. new mobility on the 9800 WLC

Correct Answer: B
Section:

QUESTION 26

Refer to the exhibit.



Fast Transition

Fast Transition □

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy-AES ☑

Authentication Key Management

802.1X	□	Enable
CCKM	□	Enable
PSK	☑	Enable
FT 802.1X	□	Enable
FT PSK	□	Enable
PSK Format		ASCII
		••••••••••••••••

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

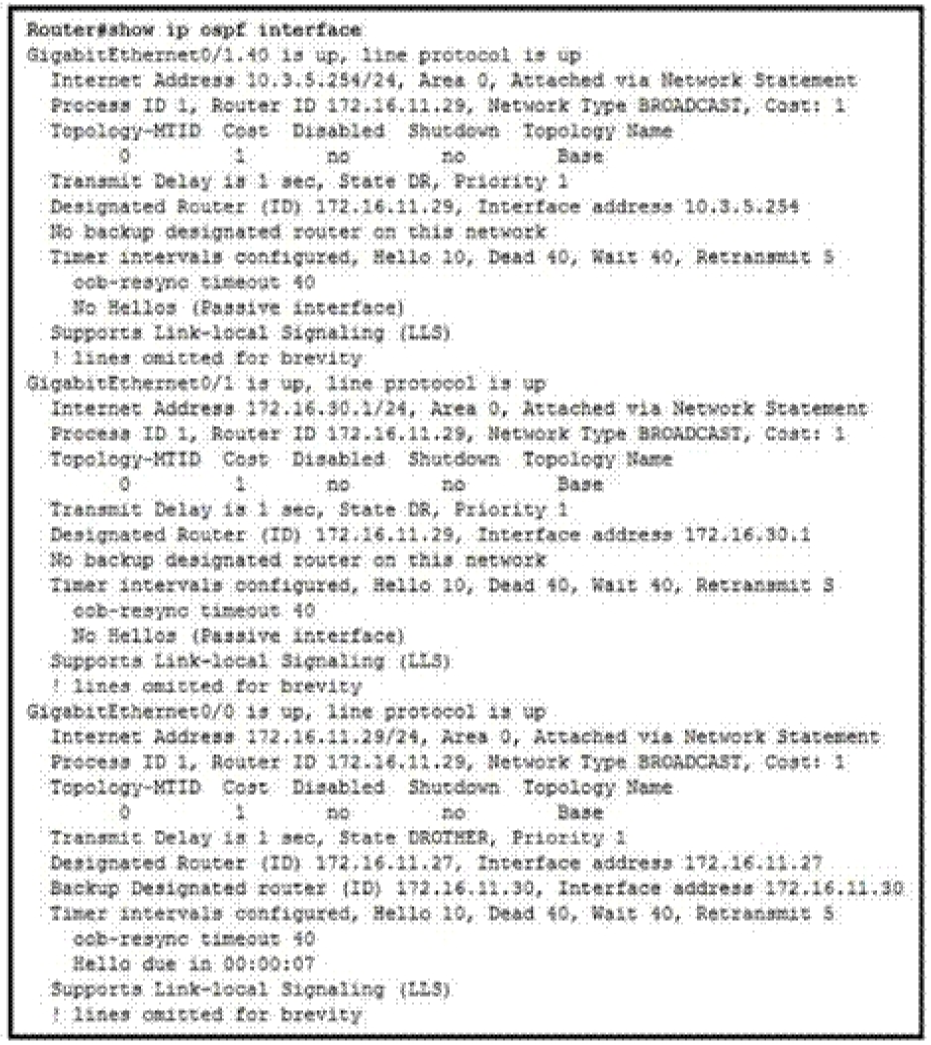
C. certificate

D. RADIUS token

Correct Answer: A
Section:

QUESTION 27

Refer to the exhibit.



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

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

A. GigabitEthemet0/1 and GigabitEthernet0/1.40

B. only GigabitEthernet0/1

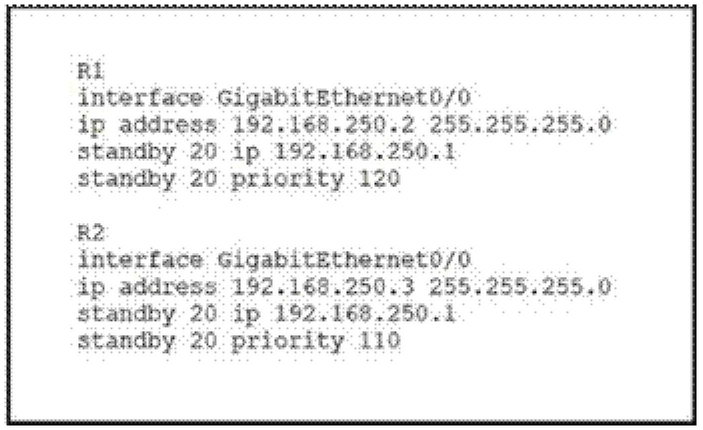
C. only GigabttEthernet0/0

D. Gigabit Ethernet0/0 and GigabitEthemet0/1

Correct Answer: C
Section:

QUESTION 28

Refer to the exhibit.



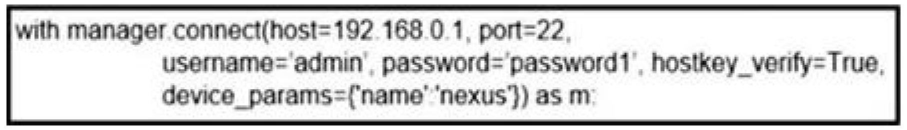
```
R1
interface GigabitEthernet0/0
ip address 192.168.250.2 255.255.255.0
standby 20 ip 192.168.250.1
standby 20 priority 120

R2
interface GigabitEthernet0/0
ip address 192.168.250.3 255.255.255.0
standby 20 ip 192.168.250.1
standby 20 priority 110
```

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

A. R1 becomes the active router.
B. R1 becomes the standby router.
C. If R2 goes down, R1 becomes active but reverts to standby when R2 comes back online.
D. If R1 goes down. R2 becomes active and remains the active device when R1 comes back online.
E. If R1 goes down, R2 becomes active but reverts to standby when R1 comes back online.

Correct Answer: A, D
Section:

QUESTION 29
Refer to the exhibit.



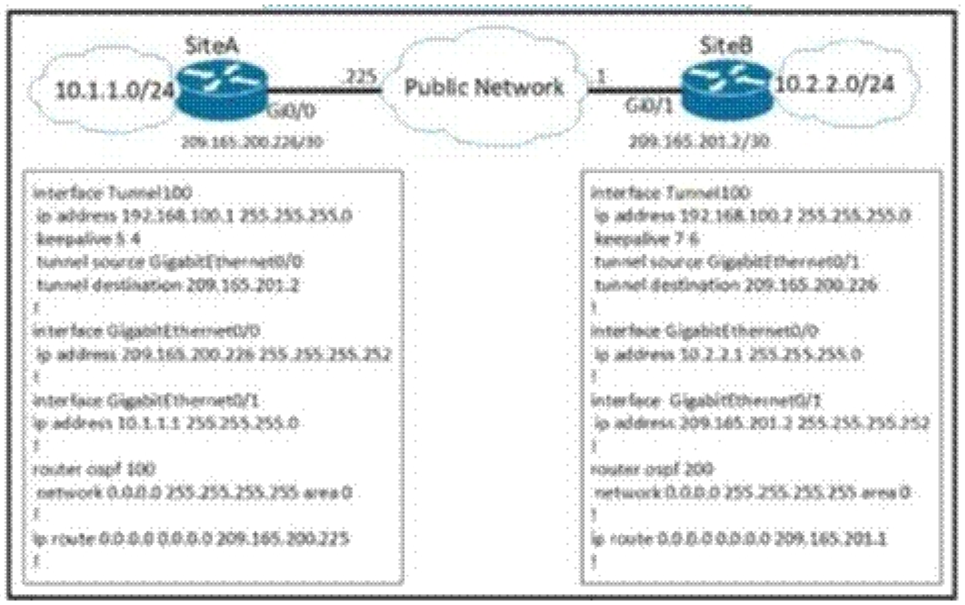
```
with manager.connect(host=192.168.0.1, port=22,
             username='admin', password='password1', hostkey_verify=True,
             device_params={'name':'nexus'}) as m:
```

What does the snippet of code achieve?

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

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

QUESTION 30



```
interface Tunnel100
 ip address 192.168.100.1 255.255.255.0
 keepalive 5 4
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.201.2
!
interface GigabitEthernet0/0
 ip address 209.165.200.226 255.255.255.252
!
interface GigabitEthernet0/1
ip address 10.1.1.1 255.255.255.0
!
router ospf 100
 network 0.0.0.0 255.255.255.255 area 0
!
ip route 0.0.0.0 0.0.0.0 209.165.200.225
!
```

```
interface Tunnel100
 ip address 192.168.100.2 255.255.255.0
 keepalive 7 6
 tunnel source GigabitEthernet0/1
 tunnel destination 209.165.200.226
!
interface GigabitEthernet0/0
 ip address 10.2.2.1 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 209.165.201.2 255.255.255.252
!
router ospf 200
 network 0.0.0.0 255.255.255.255 area 0
!
ip route 0.0.0.0 0.0.0.0 209.165.201.1
!
```

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

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

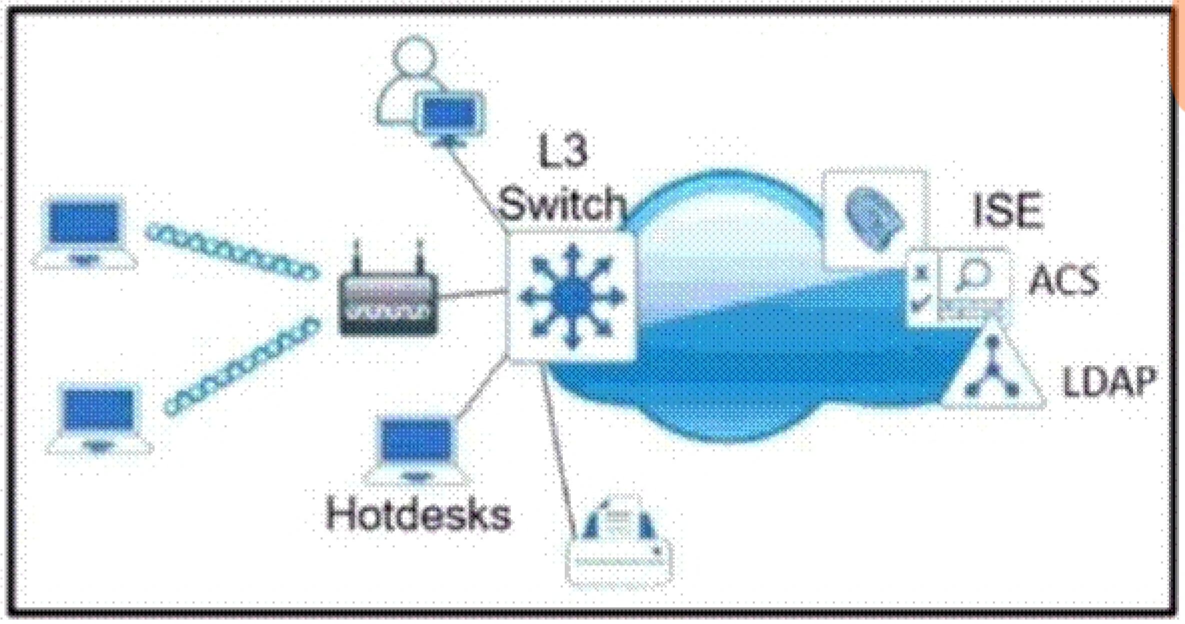
Correct Answer: C
Section:

QUESTION 31
A network engineer configures a new GRE tunnel and enters the show run command. What does the output verify?

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

Correct Answer: B
Section:

QUESTION 32

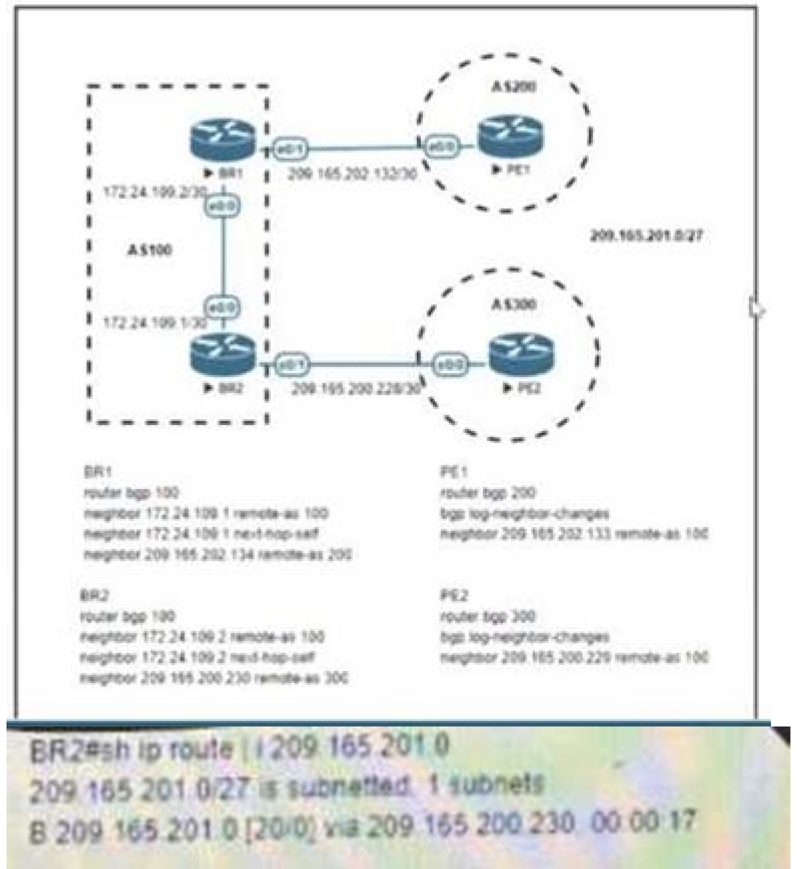


Refer to the exhibit Which single security feature is recommended to provide Network Access Control in the enterprise?

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

Correct Answer: B
Section:

QUESTION 33



```
BR1
router bgp 100
neighbor 172.24.109.1 remote-as 100
neighbor 172.24.109.1 next-hop-self
neighbor 209.165.202.134 remote-as 200

BR2
router bgp 100
neighbor 172.24.109.2 remote-as 100
neighbor 172.24.109.2 next-hop-self
neighbor 209.165.200.230 remote-as 300
```

```
PE1
router bgp 200
bgp log-neighbor-changes
neighbor 209.165.202.133 remote-as 100

PE2
router bgp 300
bgp log-neighbor-changes
neighbor 209.165.200.229 remote-as 100
```

```
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.

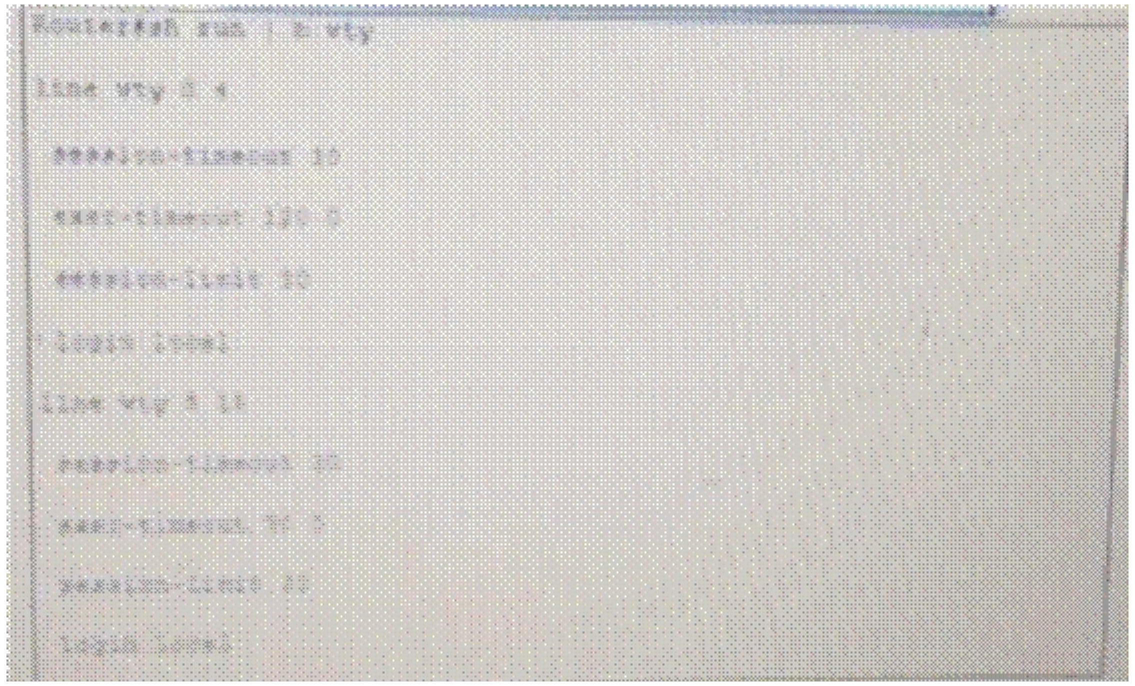
Correct Answer: C
Section:
Explanation:
MED Attribute:
+ Optional nontransitive attribute (nontransitive means that we can only advertise MED to routers that are one AS away) + Sent through ASes to external BGP neighbors + Lower value is preferred (it can be considered the external metric of a route)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

QUESTION 34
Which two methods are used to reduce the AP coverage area? (Choose two)

A. Reduce channel width from 40 MHz to 20 MHz
B. Disable 2.4 GHz and use only 5 GHz.
C. Reduce AP transmit power.
D. Increase minimum mandatory data rate
E. Enable Fastlane

Correct Answer: C, D
Section:

QUESTION 35
Refer to the exhibit.



```
Router#sh run | b vty
line vty 0 4
 session-timeout 10
 exec-timeout 120 0
 session-limit 10
 login local
line vty 5 15
 session-timeout 10
 exec-timeout 30 0
 session-limit 10
 login local
```

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

A. line vty 0 15 absolute-timeout 600

B. line vty 0 15 exec-timeout

C. line vty 01 5 exec-timeout 10 0

D. line vty 0 4 exec-timeout 600

Correct Answer: C
Section:

QUESTION 36
Which two threats does AMP4E have the ability to block? (Choose two.)

A. DDoS

B. ransomware

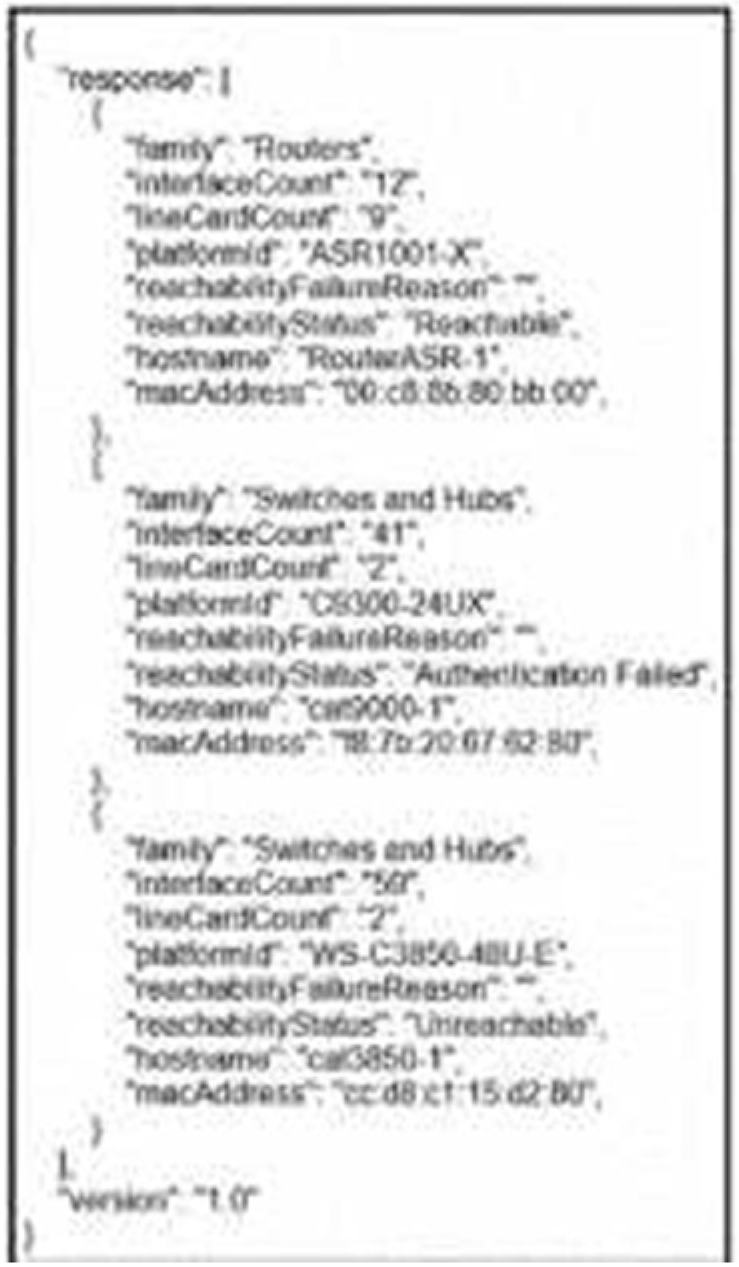
C. Microsoft Word macro attack

D. SQL injection

E. email phishing

Correct Answer: B, C
Section:
Explanation:
https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/c11-742008- 00-cisco-amp-for-endpoints-wp-v2a.pdf

QUESTION 37



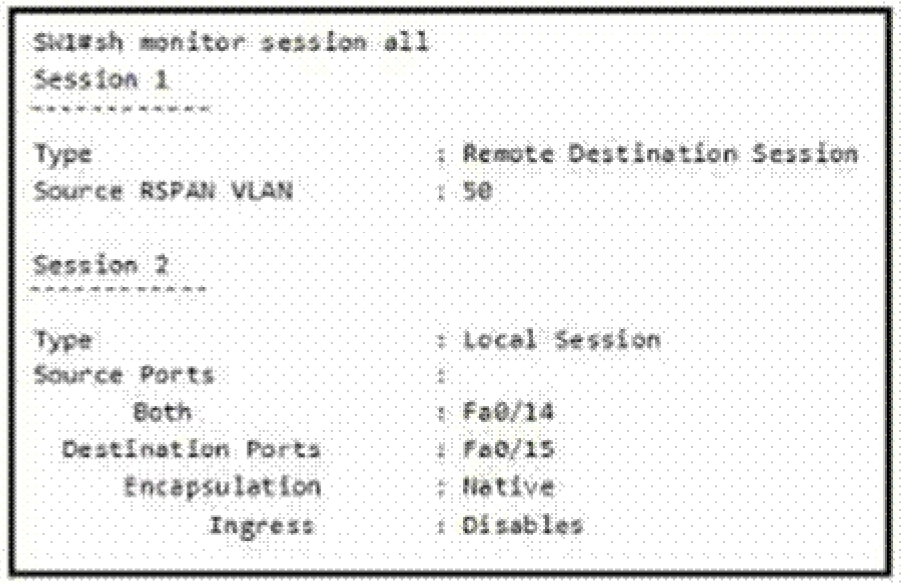
```
{
   "response": [
      {
         "family": "Routers",
         "interfaceCount": "12",
         "lineCardCount": "9",
         "platformId": "ASR1001-X",
         "reachabilityFailureReason": "",
         "reachabilityStatus": "Reachable",
         "hostname": "RouterASR-1",
         "macAddress": "00:c8:8b:80:bb:00",
      },
      {
         "family": "Switches and Hubs",
         "interfaceCount": "41",
         "lineCardCount": "2",
         "platformId": "C9300-24UX",
         "reachabilityFailureReason": "",
         "reachabilityStatus": "Authentication Failed",
         "hostname": "cat9000-1",
         "macAddress": "f8:7b:20:67:62:80",
      },
      {
         "family": "Switches and Hubs",
         "interfaceCount": "59",
         "lineCardCount": "2",
         "platformId": "WS-C3850-48U-E",
         "reachabilityFailureReason": "",
         "reachabilityStatus": "Unreachable",
         "hostname": "cat3850-1",
         "macAddress": "cc:d8:c1:15:d2:80",
      }
   ],
   "version": "1.0"
}
```

What does the cisco REST response indicate?

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

Correct Answer: C
Section:

QUESTION 38
Refer to the exhibit.



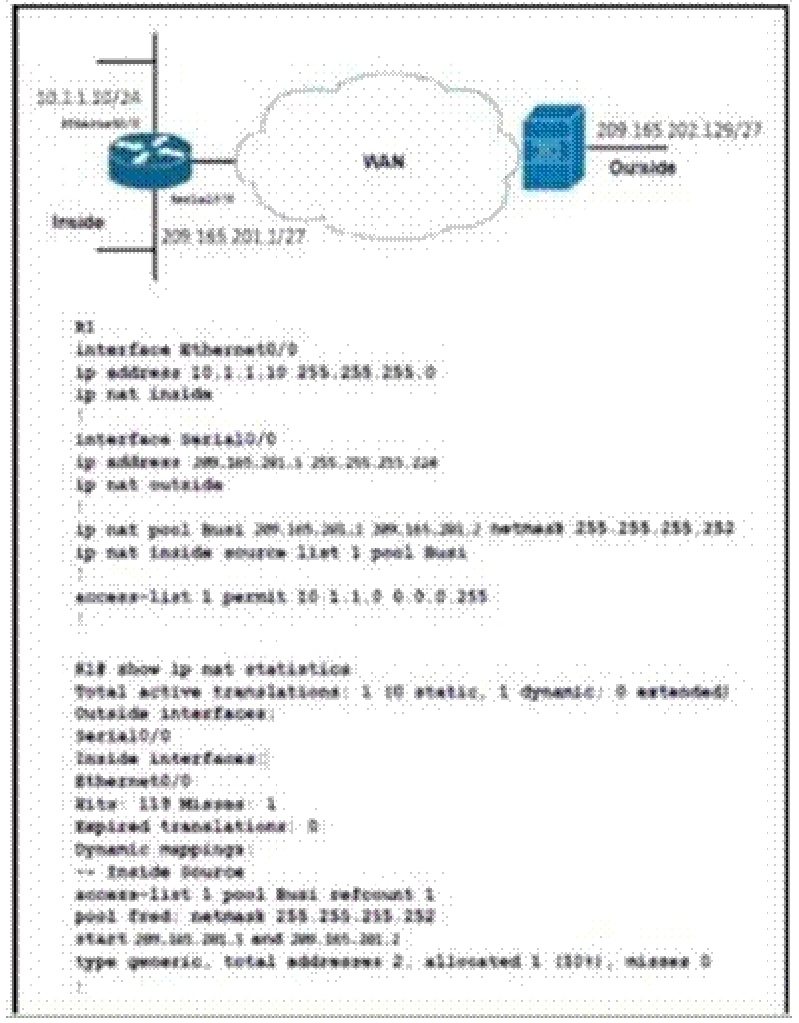
```
SW1#sh monitor session all
Session 1
------------

Type                          : Remote Destination Session
Source RSPAN VLAN             : 50

Session 2
------------

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

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

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

Correct Answer: D
Section:
Explanation:
SW1 has been configured with the following commands:
SW1(config)#monitor session 1 source remote vlan 50 SW1(config)#monitor session 2 source interface fa0/14 SW1(config)#monitor session 2 destination interface fa0/15 The session 1 on SW1 was configured for Remote SPAN (RSPAN) while session 2 was configured for local SPAN. For RSPAN we need to configure the destination port to complete the configuration.
Note: In fact we cannot create such a session like session 1 because if we only configure ?Source RSPAN VLAN 50? (with the command ?monitor session 1 source remote vlan 50?) then we will receive a ?Type: Remote Source Session?
(not ?Remote Destination Session?).

QUESTION 39



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


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

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

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

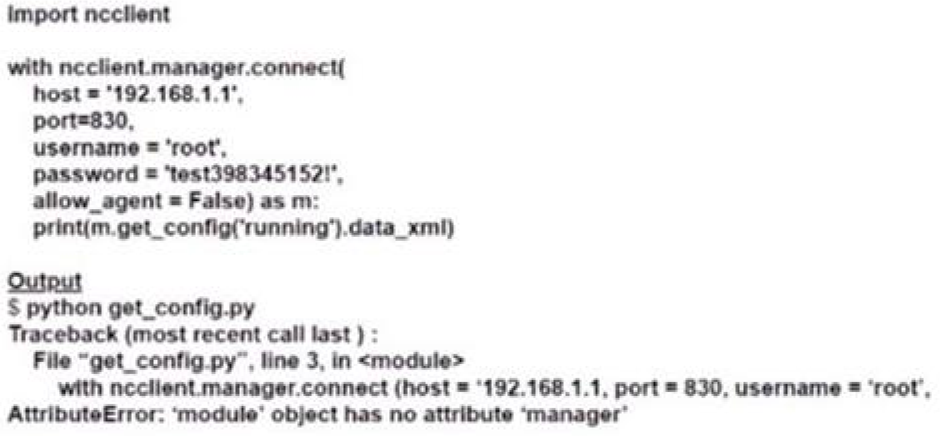
Correct Answer: A
Section:

QUESTION 40
An engineer is troubleshooting the Ap join process using DNS. Which FQDN must be resolvable on the network for the access points to successfully register to the WLC?

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

Correct Answer: B
Section:
Explanation:
DNS: If you have configured your DHCP server to provide both option 006 (DNS server address) and option 015 (domain name) information, the AP can obtain WLC addresses from the DNS server. The process works as follows:
1. The AP gets its IP address from DHCP with options 6 and 15 configured.
2. The AP can obtain the IP address of the DNS server from the DHCP option.
3. The AP uses this information to perform a hostname lookup using CISCO-CAPWAPCONTROLLER.< localdomain>, which resolves to available WLC management interface IP addresses (IPv4 or IPv6, or both).
4. The AP can then perform a directed message to associate to responsive WLCs.
To prevent all APs from joining a single controller based on a DNS name resolution, the domain name may vary; this is what is done to dispatch APs to different controllers across the enterprise network, based on different domain names that are configured in their respective DNS scopes.

QUESTION 41
Running the script causes the output in the exhibit. Which change to the first line of the script resolves the error?



```
Import ncclient

with ncclient.manager.connect(
   host = '192.168.1.1',
   port=830,
   username = 'root',
   password = 'test398345152!',
   allow_agent = False) as m:
   print(m.get_config('running').data_xml)
```

Output

```
$ python get_config.py
Traceback (most recent call last ) :
   File "get_config.py", line 3, in <module>
      with ncclient.manager.connect (host = '192.168.1.1, port = 830, username = 'root',
AttributeError: 'module' object has no attribute 'manager'
```

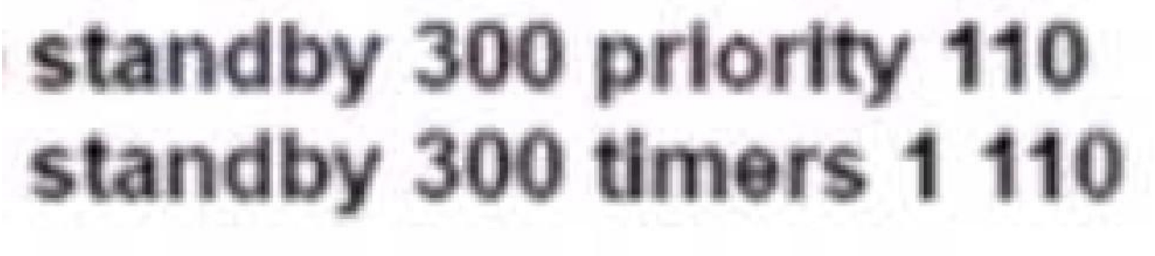
A. from ncclient import
B. import manager
C. from ncclient import*

D. import ncclient manager

Correct Answer: C
Section:

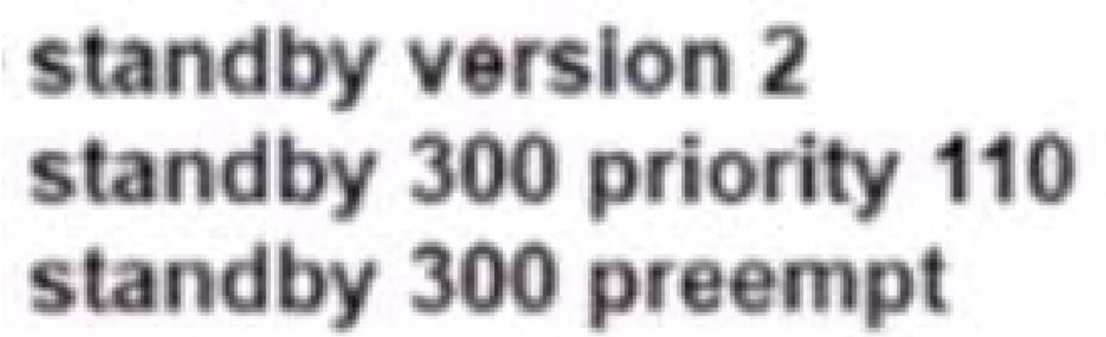
QUESTION 42
An engineer must configure HSRP group 300 on a Cisco IOS router. When the router is functional, it must be the must be the active HSRP router. The peer router has been configured using the default priority value. Which command set is required?

A.



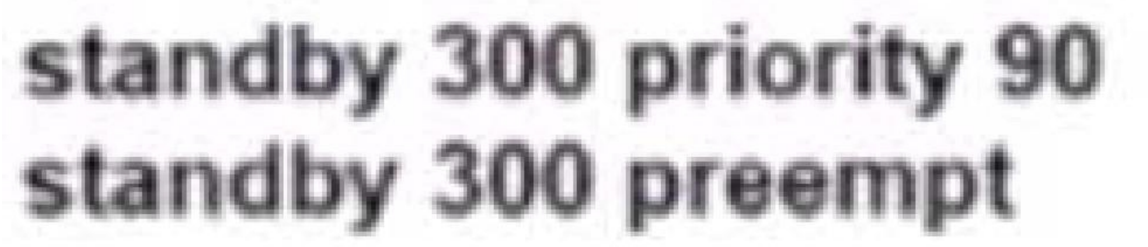
```
standby 300 priority 110
standby 300 timers 1 110
```

B.



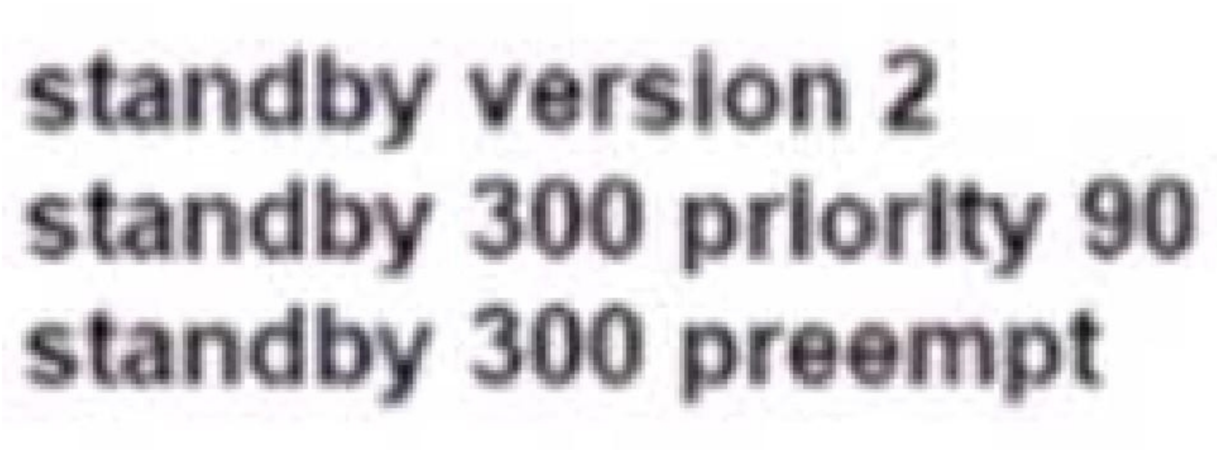
```
standby version 2
standby 300 priority 110
standby 300 preempt
```

C.



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

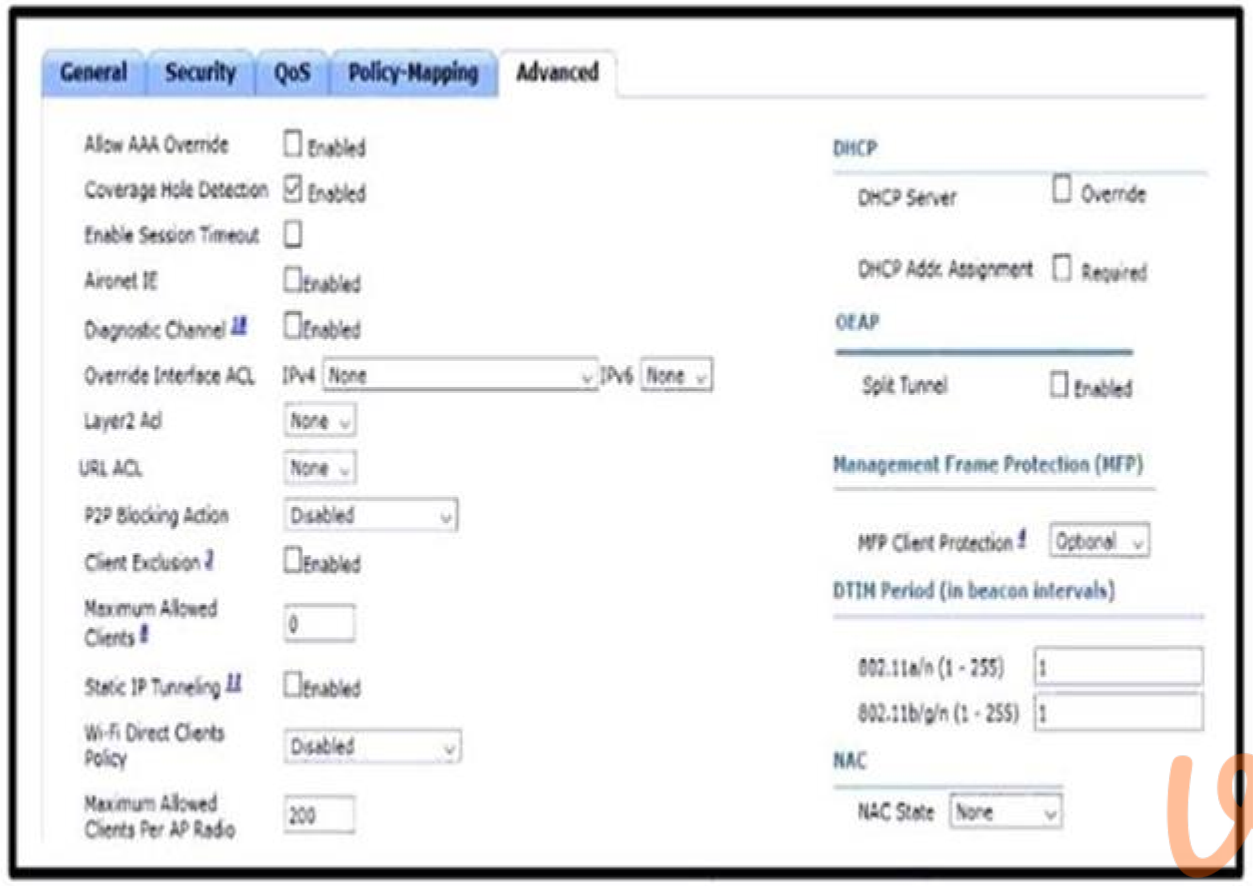
D.



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

Correct Answer: B
Section:

QUESTION 43



Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout □
Aironet IE □ Enabled
Diagnostic Channel □ Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
URL ACL None
P2P Blocking Action Disabled
Client Exclusion □ Enabled
Maximum Allowed Clients 0
Static IP Tunneling □ Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

OEAP
Split Tunnel □ Enabled

Management Frame Protection (MFP)
MFP Client Protection Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
NAC State None

Refer to the exhibit. An engineer is investigating why guest users are able to access other guest user devices when the users are connected to the customer guest WLAN. What action resolves this issue?

A. implement MFP client protection
B. implement split tunneling
C. implement P2P blocking
D. implement Wi-Fi direct policy

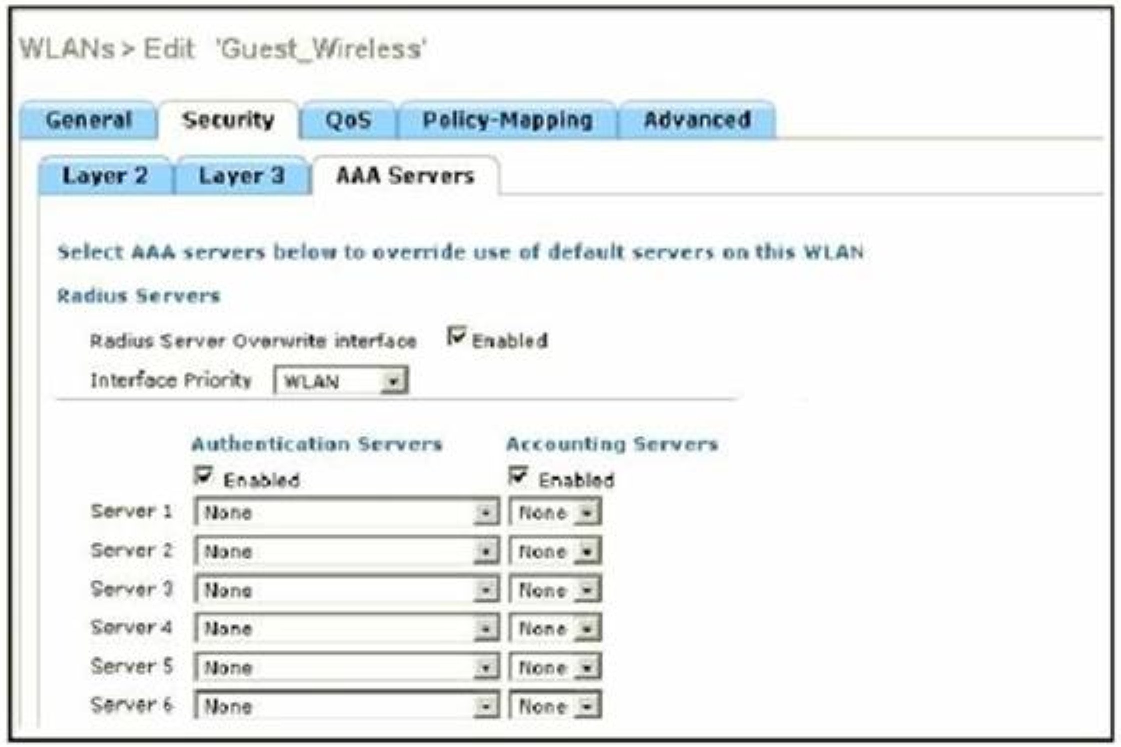
Correct Answer: C
Section:
Explanation:
This control determines whether the Wireless LAN Controller is configured to prevent clients connected to the same Wireless Local Area Controller from communicating with each other.
Wireless Client Isolation prevents wireless clients from communicating with each other over the RF.
Packets that arrive on the wireless interface are forwarded only out the wired interface of an Access Point. One wireless client could potentially compromise another client sharing the same wireless network.

QUESTION 44
Which characteristic distinguishes Ansible from Chef?

A. Ansible lacs redundancy support for the master server. Chef runs two masters in an active/active mode.
B. Ansible uses Ruby to manage configurations. Chef uses YAML to manage configurations.
C. Ansible pushes the configuration to the client. Chef client pulls the configuration from the server.
D. The Ansible server can run on Linux, Unix or Windows. The Chef server must run on Linux or Unix.

Correct Answer: C
Section:

QUESTION 45
Refer to the exhibit.



WLANs > Edit 'Guest_Wireless'

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface ☑ Enabled

Interface Priority WLAN

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	None	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

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

Correct Answer: A
Section:

QUESTION 46
In an SD-Access solution what is the role of a fabric edge node?

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

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

QUESTION 47

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

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

Correct Answer: A
Section:

QUESTION 48
When using TLS for syslog, which configuration allows for secure and reliable transportation of messages to its default port?

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

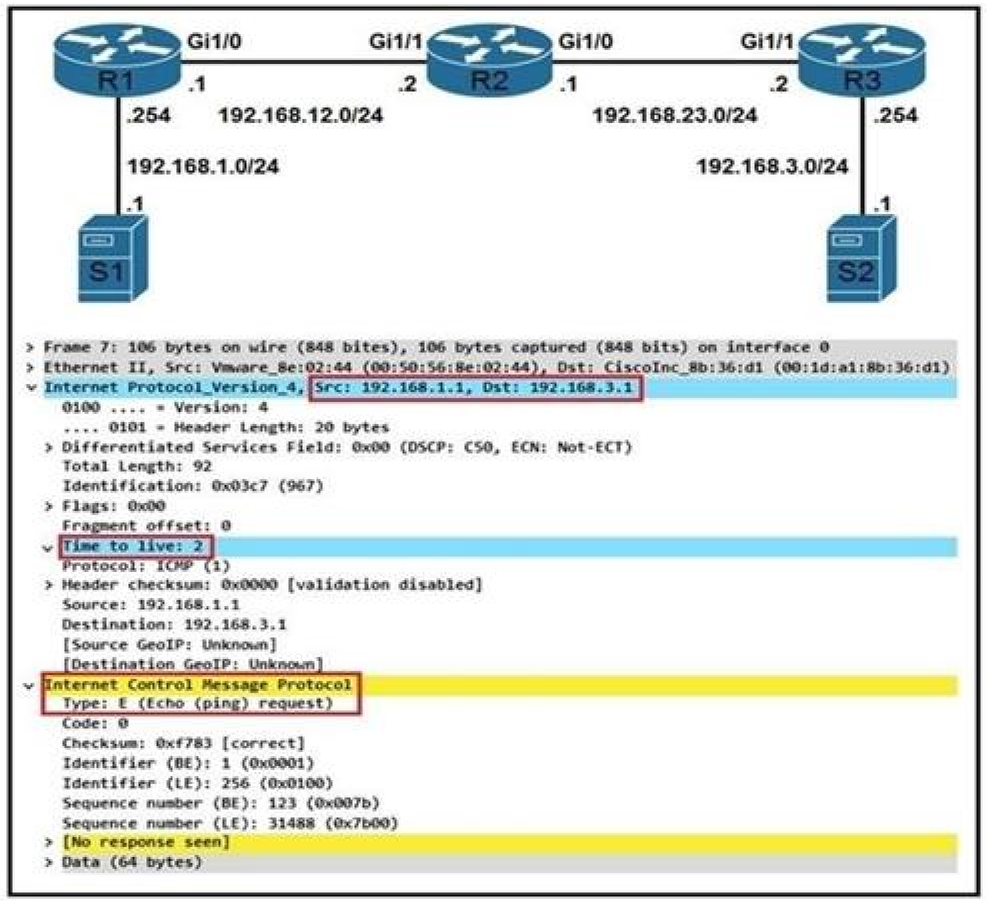
Correct Answer: A
Section:
Explanation:
The TCP port 6514 has been allocated as the default port for syslog over Transport Layer Security (TLS).
Reference: https://tools.ietf.org/html/rfc5425

QUESTION 49
At which Layer does Cisco DNA Center support REST controls?

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

Correct Answer: D
Section:

QUESTION 50
Refer to the exhibit.



```
> Frame 7: 106 bytes on wire (848 bites), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: Vmware_8e:02:44 (00:50:56:8e:02:44), Dst: CiscoInc_8b:36:d1 (00:1d:a1:8b:36:d1)
v Internet Protocol_Version_4, Src: 192.168.1.1, Dst: 192.168.3.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x03c7 (967)
  > Flags: 0x00
    Fragment offset: 0
  v Time to live: 2
    Protocol: ICMP (1)
  > Header checksum: 0x0000 [validation disabled]
    Source: 192.168.1.1
    Destination: 192.168.3.1
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
v Internet Control Message Protocol
    Type: E (Echo (ping) request)
    Code: 0
    Checksum: 0xf783 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 123 (0x007b)
    Sequence number (LE): 31488 (0x7b00)
  > [No response seen]
  > Data (64 bytes)
```

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

A. The packet reaches R3, and the TTL expires
B. R2 replies with a TTL exceeded message
C. R3 replies with a TTL exceeded message.
D. The packet reaches R2 and the TTL expires
E. R1 replies with a TTL exceeded message
F. The packet reaches R1 and the TTL expires.

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

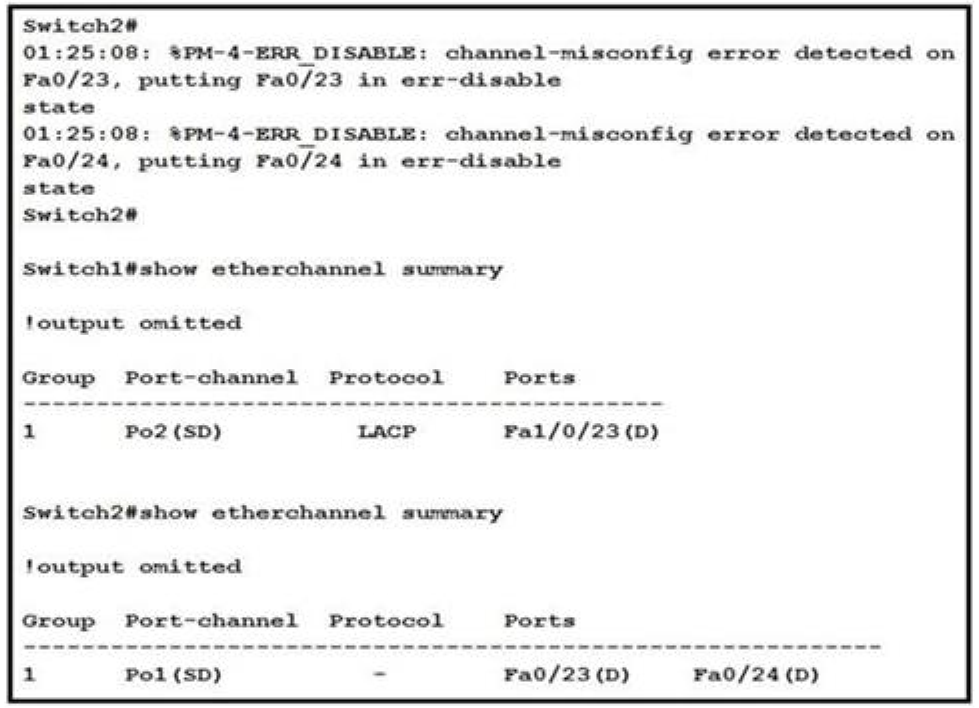
QUESTION 51
Which technology provides a secure communication channel for all traffic at Layer 2 of the OSI model?

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

Correct Answer: A
Section:

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

QUESTION 52



```
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.

Correct Answer: C
Section:
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 occuring by disabling all the ports bundled in the EtherChannel.

QUESTION 53
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

Correct Answer: C
Section:
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

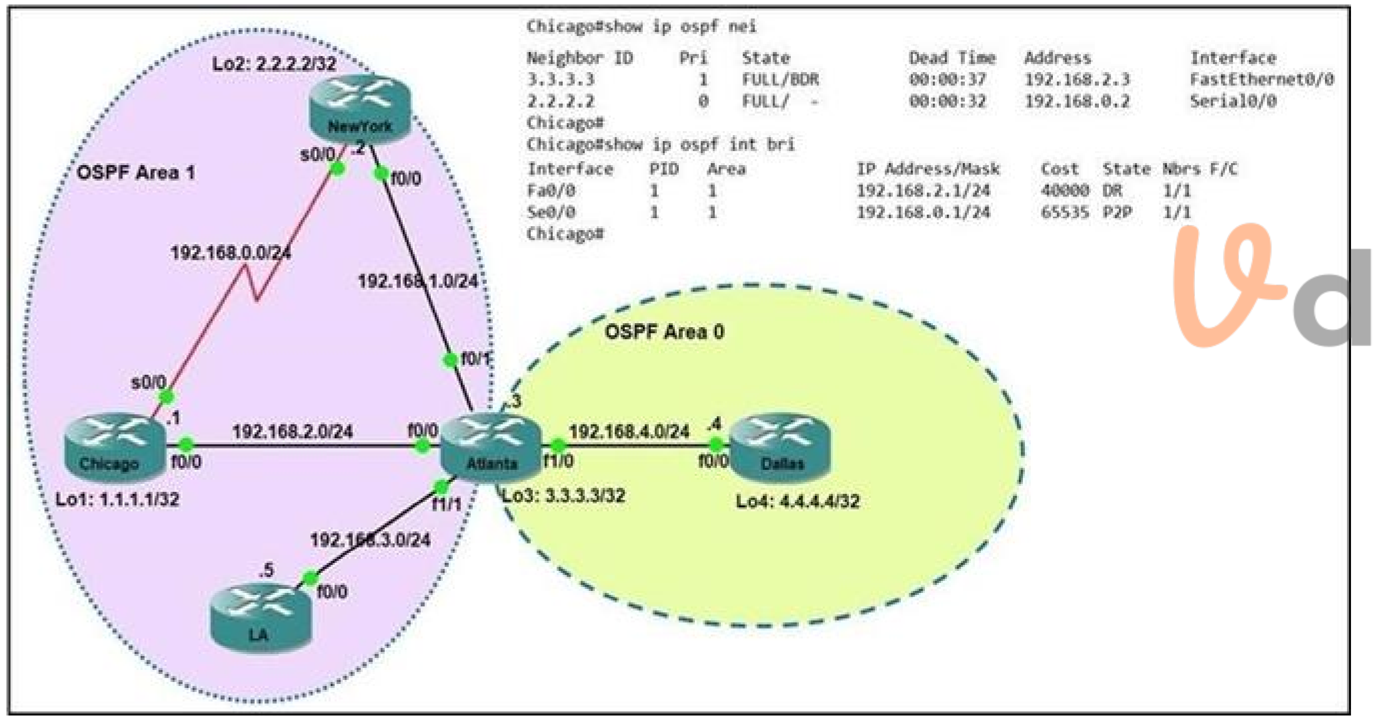
VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments.
Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/vxlan/configuration/guide/b_Cisco_Nexus_9000_Series_NXOS_VXLAN_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NXOS_VXLAN_Configuration_Guide_7x_chapter_010.html

QUESTION 54
Which DHCP option helps lightweight APs find the IP address of a wireless LAN controller?

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

Correct Answer: A
Section:

QUESTION 55
Refer the exhibit.



```
Chicago#show ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           1   FULL/BDR        00:00:37    192.168.2.3     FastEthernet0/0
2.2.2.2           0   FULL/  -        00:00:32    192.168.0.2     Serial0/0
Chicago#
Chicago#show ip ospf int bri
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Fa0/0        1     1               192.168.2.1/24     40000 DR    1/1
Se0/0        1     1               192.168.0.1/24     65535 P2P   1/1
Chicago#
```

Which router is the designated router on the segment 192.168.0.0/24?

A. This segment has no designated router because it is a nonbroadcast network type.
B. This segment has no designated router because it is a p2p network type.
C. Router Chicago because it has a lower router ID
D. Router NewYork because it has a higher router ID

Correct Answer: B
Section:

QUESTION 56
What are two differences between the RIB and the FIB? (Choose two.)

A. The FIB is derived from the data plane, and the RIB is derived from the FIB.

B. The RIB is a database of routing prefixes, and the FIB is the Information used to choose the egress interface for each packet.

C. FIB is a database of routing prefixes, and the RIB is the information used to choose the egress interface for each packet.

D. The FIB is derived from the control plane, and the RIB is derived from the FIB.

E. The RIB is derived from the control plane, and the FIB is derived from the RIB.

Correct Answer: B, E
Section:

QUESTION 57
Which algorithms are used to secure REST API from brute attacks and minimize the impact?

A. SHA-512 and SHA-384

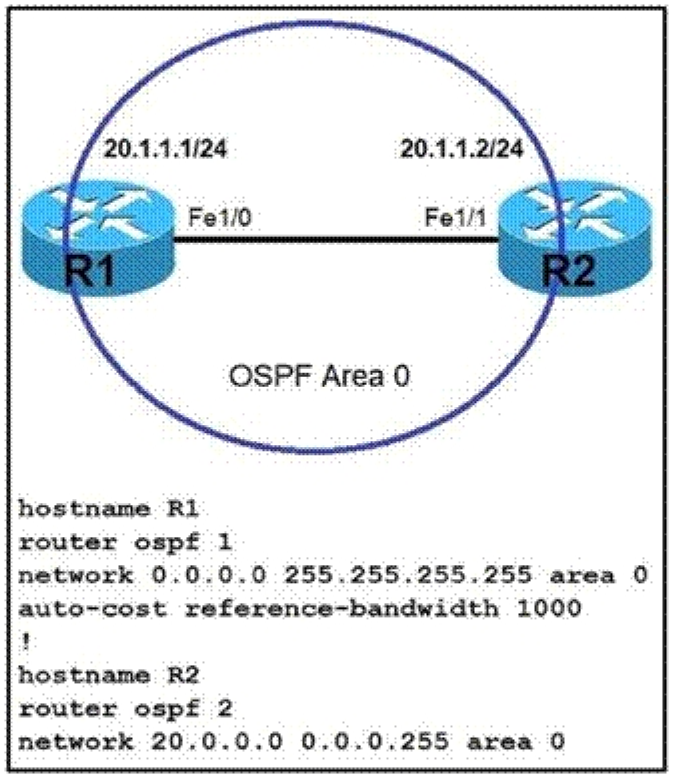
B. MD5 algorithm-128 and SHA-384

C. SHA-1, SHA-256, and SHA-512

D. PBKDF2, BCrypt, and SCrypt

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

QUESTION 58



```
hostname R1
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
auto-cost reference-bandwidth 1000
!
hostname R2
router ospf 2
network 20.0.0.0 0.0.0.255 area 0
```

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

A. network 20.1.1.2.0.0.0.0 area 0

B. network 20.1.1.2 255.255.0.0. area 0

C. network 20.1.1.2.0.0.255.255 area 0

D. network 20.1.1.2 255.255.255 area 0

Correct Answer: A
Section:
Explanation:
The ?network 20.0.0.0 0.0.0.255 area 0? command on R2 did not cover the IP address of Fa1/1 interface of R2 so OSPF did not run on this interface. Therefore we have to use the command ?network 20.1.1.2 0.0.255.255 area 0? to turn on OSPF on this interface.
Note: The command ?network 20.1.1.2 0.0.255.255 area 0? can be used too so this answer is also correct but answer C is the best answer here.
The ?network 0.0.0.0 255.255.255.255 area 0? command on R1 will run OSPF on all active

QUESTION 59
Which two operations are valid for RESTCONF? (Choose two.)

A. HEAD

B. REMOVE

C. PULL

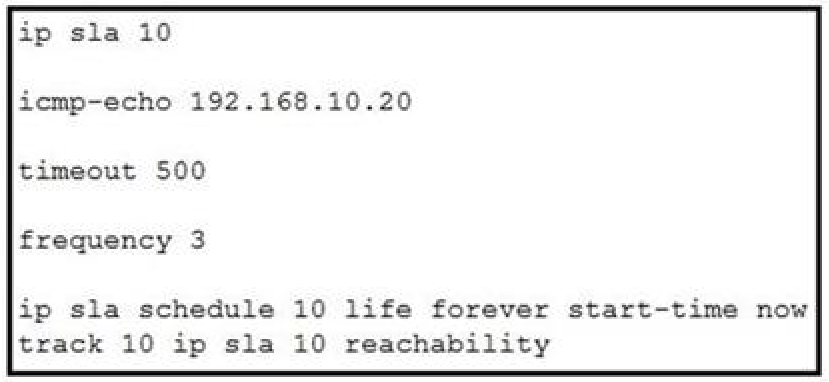
D. PATCH

E. ADD

F. PUSH

Correct Answer: A, D
Section:
Explanation:
RESTCONF operations include OPTIONS, HEAD, GET, POST, PATCH, DELETE.

QUESTION 60
Refer to the exhibit.



```
ip sla 10

icmp-echo 192.168.10.20

timeout 500

frequency 3

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

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

A. event manager applet EEM_IP_SLA event track 10 state down

B. event manager applet EEM_IP_SLA event track 10 state unreachable

C. event manager applet EEM_IP_SLA event sla 10 state unreachable

D. event manager applet EEM_IP_SLA event sla 10 state down

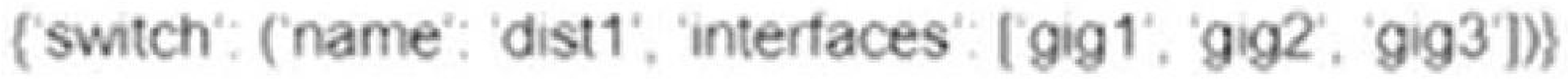
Correct Answer: A
Section:
Explanation:
The ?ip sla 10? will ping the IP 192.168.10.20 every 3 seconds to make sure the connection is still up. We can configure an EEM applet if there is any problem with this IP SLA via the command ?event track 10 state down?.
Reference: https://www.theroutingtable.com/ip-sla-and-cisco-eem/

QUESTION 61
Which JSON syntax is valid?

A.

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

B.

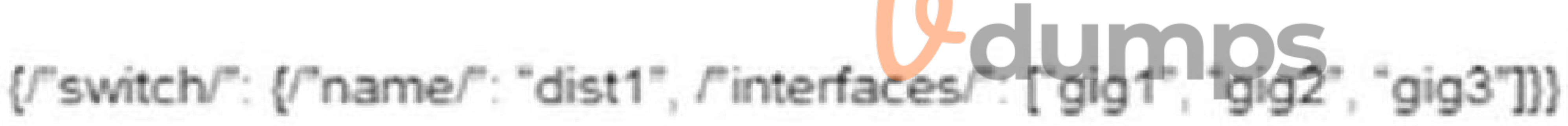


```
{'switch': ('name': 'dist1', 'interfaces': ['gig1', 'gig2', 'gig3'])}
```

C.

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

D.

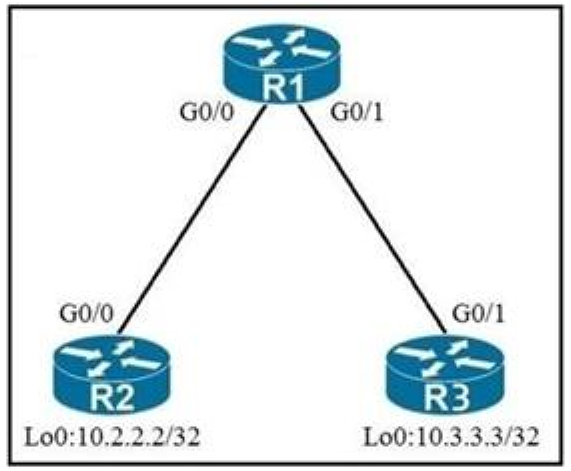


```
{/"switch/": {/"name/": "dist1", /"interfaces/": ["gig1", "gig2", "gig3"]}}
```

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

QUESTION 62

Refer to the exhibit.


R1
G0/0
G0/1
G0/0
G0/1
R2
R3
Lo0:10.2.2.2/32
Lo0:10.3.3.3/32

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

A.
```
R3(config)#time-range WEEKEND
R3(config-time-range)#periodic Saturday Sunday 00:00 to 23:59
R3(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R3(config)#access-list 150 permit ip any any time-range WEEKEND
R3(config)#interface G0/1
R3(config-if)#ip access-group 150 out
```

B.
```
R1(config)#time-range WEEKEND
R1(config-time-range)#periodic 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
```

C.
```
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
```

D.
```
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
```

Correct Answer: C
Section:
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.

QUESTION 63
When configuration WPA2 Enterprise on a WLAN, which additional security component configuration is required?

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

Correct Answer: C
Section:

QUESTION 64
Which devices does Cisco DNA Center configure when deploying an IP-based access control policy?

A. All devices integrating with ISE

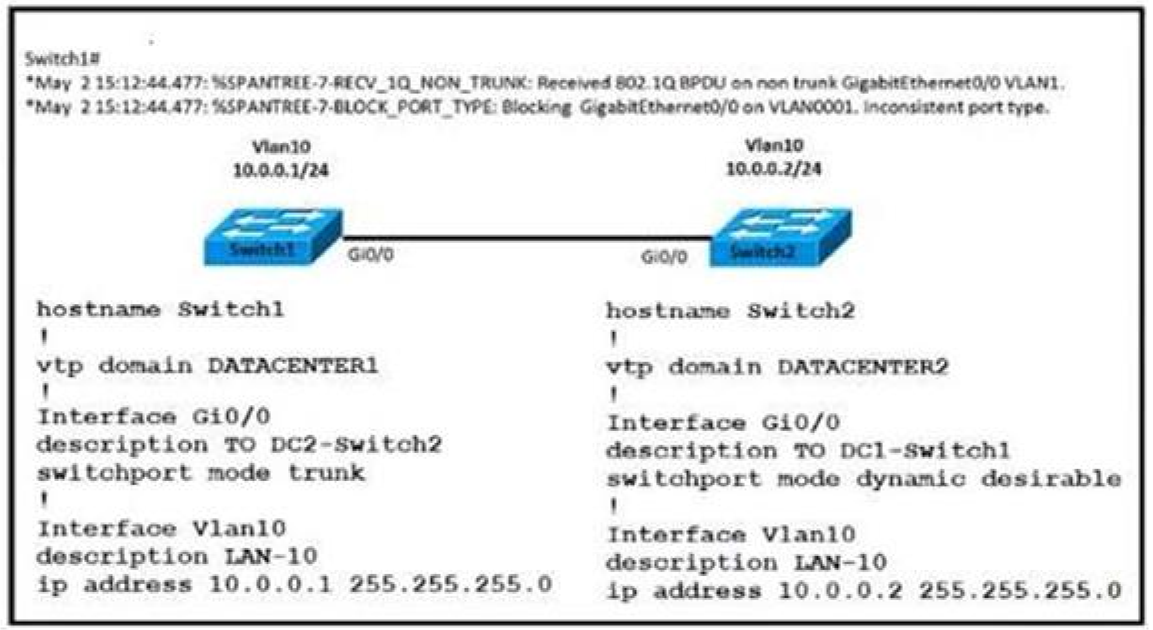
B. selected individual devices

C. all devices in selected sites

D. all wired devices

Correct Answer: C
Section:
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.

QUESTION 65
Refer to the exhibit.



```
Switch1#
*May  2 15:12:44.477: %SPANTREE-7-RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non trunk GigabitEthernet0/0 VLAN1.
*May  2 15:12:44.477: %SPANTREE-7-BLOCK_PORT_TYPE: Blocking  GigabitEthernet0/0 on VLAN0001. Inconsistent port type.
```

```
hostname Switch1
!
vtp domain DATACENTER1
!
Interface Gi0/0
description TO DC2-Switch2
switchport mode trunk
!
Interface Vlan10
description LAN-10
ip address 10.0.0.1 255.255.255.0
```

```
hostname Switch2
!
vtp domain DATACENTER2
!
Interface Gi0/0
description TO DC1-Switch1
switchport mode dynamic desirable
!
Interface Vlan10
description LAN-10
ip address 10.0.0.2 255.255.255.0
```

An engineer implemented several configuration changes and receives the logging message on switch1. Which action should the engineer take to resolve this issue?

A. Change the VTP domain to match on both switches

B. Change Switch2 to switch port mode dynamic auto

C. Change Switch1 to switch port mode dynamic auto

D. Change Switch1 to switch port mode dynamic desirable

Correct Answer: A
Section:

QUESTION 66
Which AP mode allows an engineer to scan configured channels for rogue access points?

A. sniffer

B. monitor

C. bridge

D. local

Correct Answer: B
Section:

QUESTION 67
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

Correct Answer: B
Section:

QUESTION 68
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

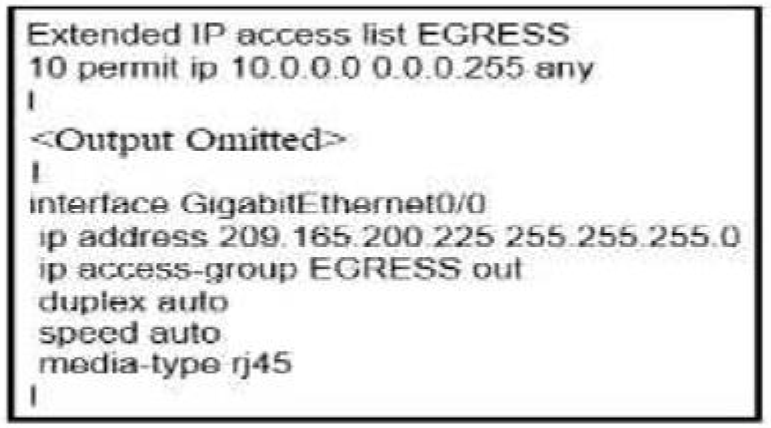
Correct Answer: B
Section:

QUESTION 69
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

Correct Answer: A
Section:

QUESTION 70
Refer to the exhibit.



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

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

A. Access control lists that are applied outbound to a router interface do not affect traffic that is sourced from the router.

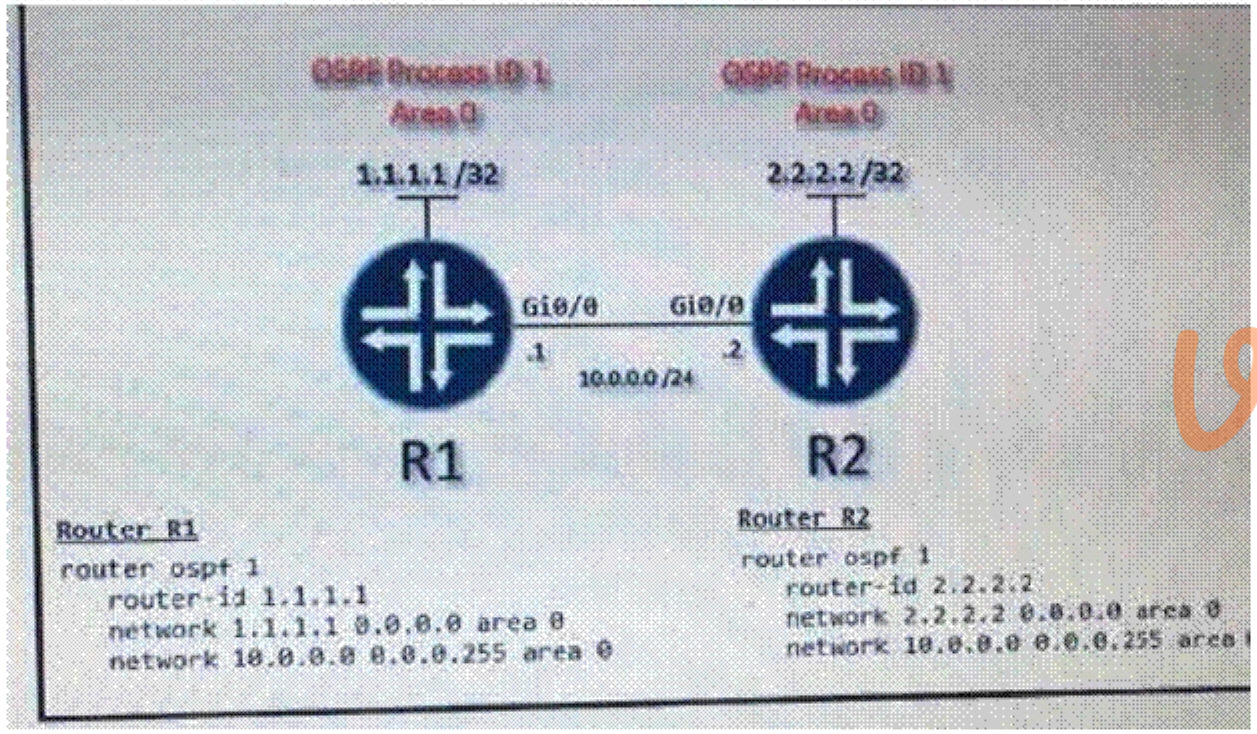
B. Only standard access control lists can block traffic from a source IP address.

C. After an access control list is applied to an interface, that interface must be shut and no shut for the access control list to take effect.

D. The access control list must contain an explicit deny to block traffic from the router.

Correct Answer: A
Section:

QUESTION 71
Refer to the exhibit.

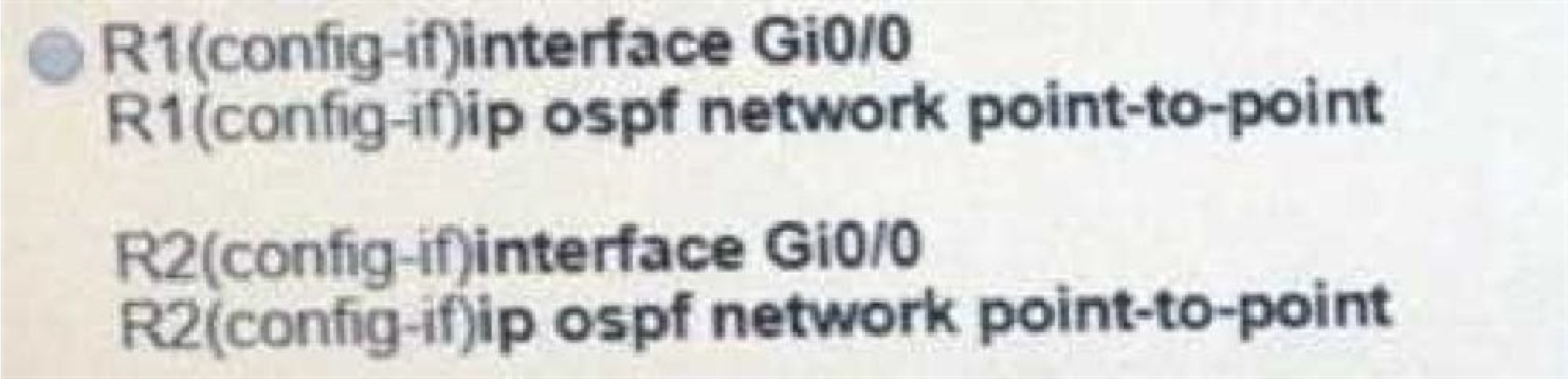


```
Router R1
router ospf 1
   router-id 1.1.1.1
   network 1.1.1.1 0.0.0.0 area 0
   network 10.0.0.0 0.0.0.255 area 0
```

```
Router R2
router ospf 1
   router-id 2.2.2.2
   network 2.2.2.2 0.0.0.0 area 0
   network 10.0.0.0 0.0.0.255 area
```

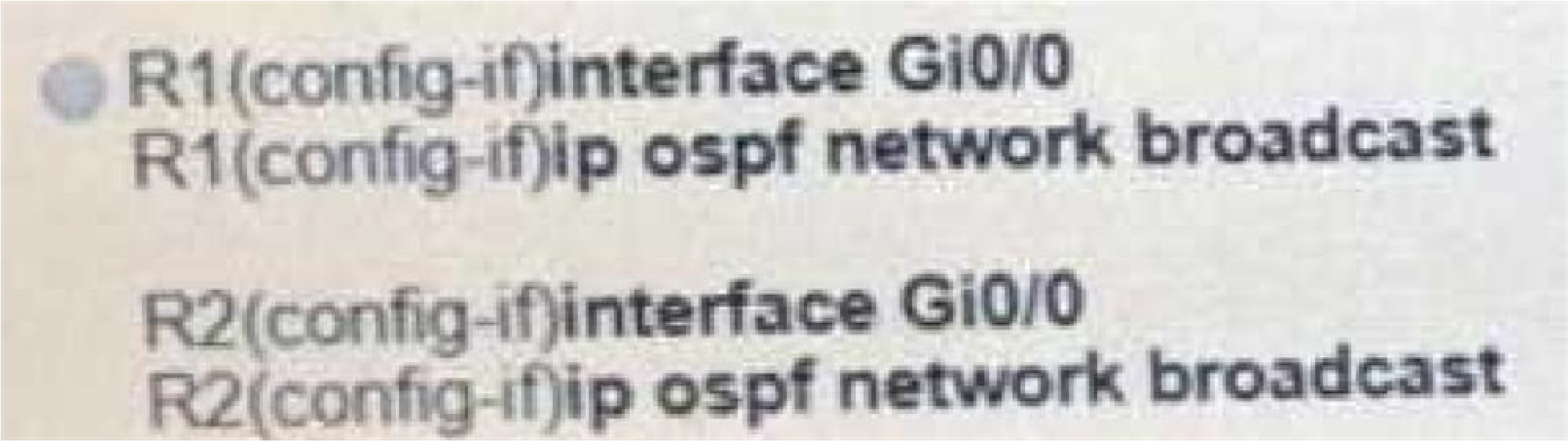
A network engineer is configuring OSPF between router R1 and router R2. The engineer must ensure that a DR/BDR election does not occur on the Gigabit Ethernet interfaces in area 0. Which configuration set accomplishes this goal?

A.



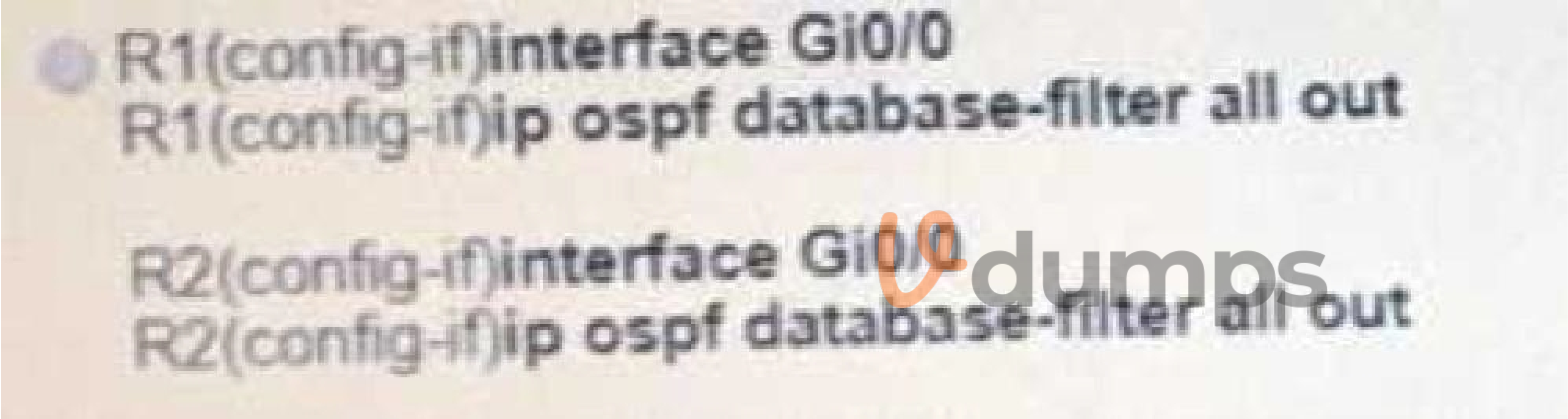
```
R1(config-if)interface Gi0/0
R1(config-if)ip ospf network point-to-point

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

B.



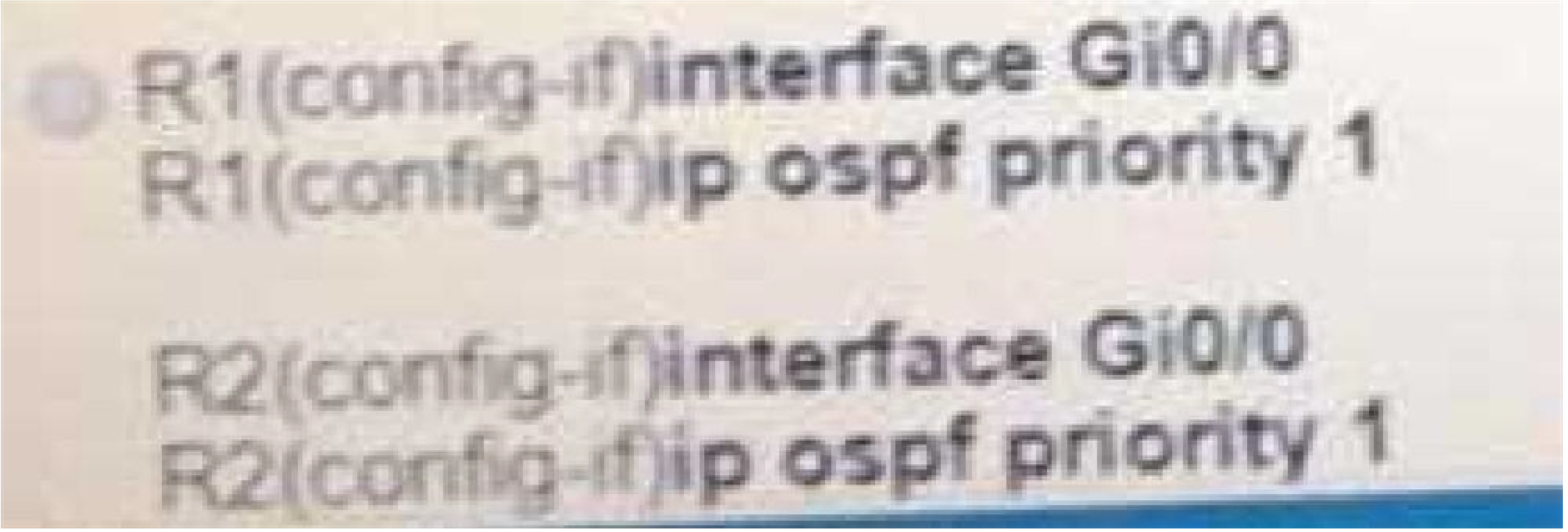
```
R1(config-if)interface Gi0/0
R1(config-if)ip ospf network broadcast

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

C.



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

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

D.



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

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

Correct Answer: A

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

QUESTION 72
Which design principle slates that a user has no access by default to any resource, and unless a resource is explicitly granted, it should be denied?

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

Correct Answer: B
Section:

QUESTION 73
Which congestion queuing method on Cisco IOS based routers uses four static queues?

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

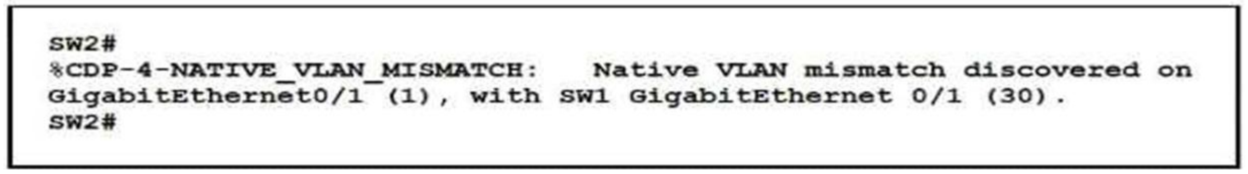
Correct Answer: A
Section:

QUESTION 74
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

Correct Answer: B
Section:

QUESTION 75
Refer to the exhibit.



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

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

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

Correct Answer: C
Section:

QUESTION 76
Which IPv4 packet field carries the QoS IP classification marking?

A. ID
B. TTL
C. FCS
D. ToS

Correct Answer: D
Section:
Explanation:
The classification is carried in the IP packet header, using 6 bits from the deprecated IP type of service (ToS) field to carry the classification (class) information. Classification can also be carried in the Layer 2 frame.

QUESTION 77
Which Cisco FlexConnect state allows wireless users that are connected to the network to continue working after the connection to the WLC has been lost?

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

Correct Answer: C
Section:
Explanation:
Operation Modes
There are two modes of operation for the FlexConnect AP.
Connected mode: The WLC is reachable. In this mode the FlexConnect AP has CAPWAP connectivity with its WLC.
Standalone mode: The WLC is unreachable. The FlexConnect has lost or failed to establish CAPWAP connectivity with its WLC. A WAN-link outage between a branch and its central site is a example of such a mode of operation.
FlexConnect States
A FlexConnect WLAN, depending on its configuration and network connectivity, is classified as being in one of the following defined states.
Authentication-Central/Switch-Central: This state represents a WLAN that uses a centralized authentication method such as 802.1X, VPN, or web. User traffic is sent to the WLC via CAPWAP (Central switching). This state is supported only when FlexConnect is in connected mode.
Authentication Down/Switching Down: Central switched WLANs no longer beacon or respond to probe requests when the FlexConnect AP is in standalone mode. Existing clients are disassociated.
Authentication-Central/Switch-Local: This state represents a WLAN that uses centralized authentication, but user traffic is switched locally. This state is supported only when the FlexConnect AP is in connected mode.
Authentication-Down/Switch-Local: A WLAN that requires central authentication rejects new users.
Existing authenticated users continue to be switched locally until session time-out if configured. The WLAN continues to beacon and respond to probes until there are no more existing users associated to the WLAN. This state occurs as a result of the AP going into standalone mode.
Authentication-local/switch-local: This state represents a WLAN that uses open, static WEP, shared, or WPA2 PSK security methods. User traffic is switched locally. These are the only security methods supported locally if a FlexConnect goes into standalone mode. The WLAN continues to beacon and respond to probes. Existing users remain connected and new user associations are accepted. If the AP is in connected mode, authentication information for these security types is forwarded to the WLC.

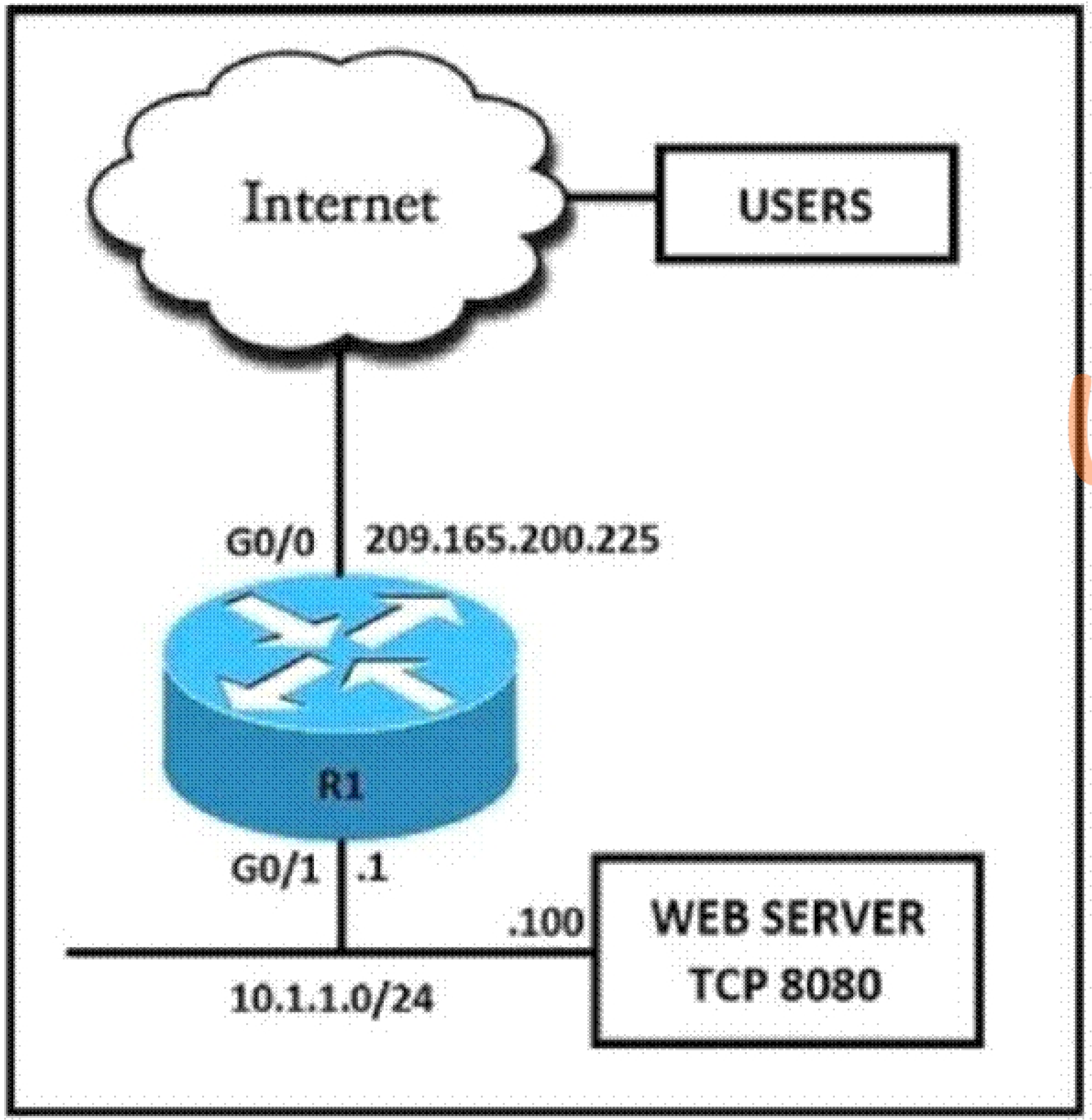
QUESTION 78

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

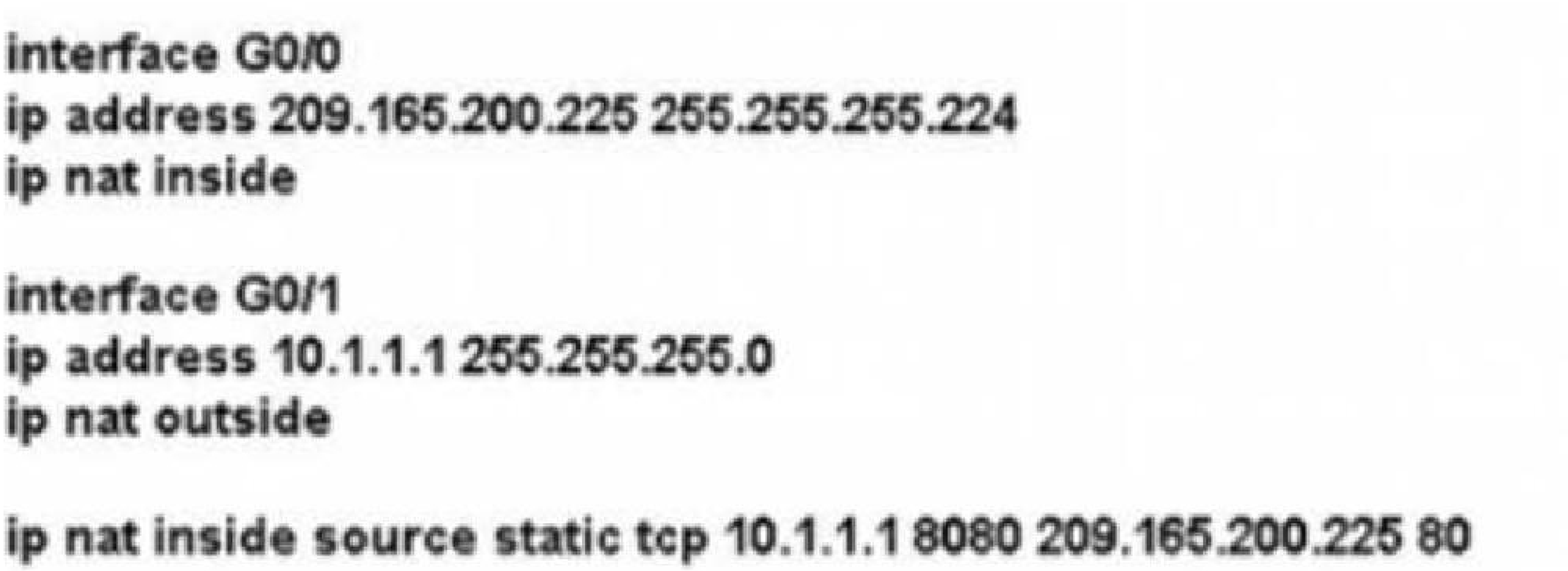
Correct Answer: B
Section:

QUESTION 79



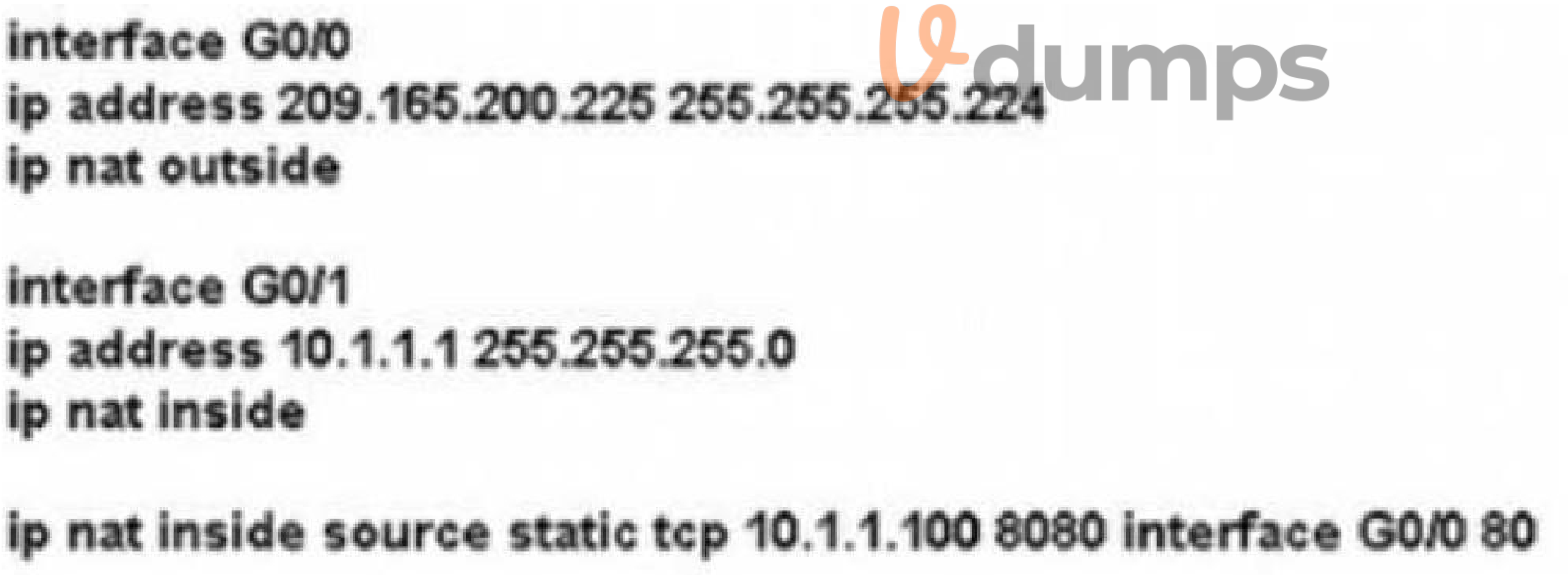
Refer to the exhibit. External users require HTTP connectivity to an internal company web server thatis listening on TCP port 8080. Which command set accomplishes this requirement?

A.



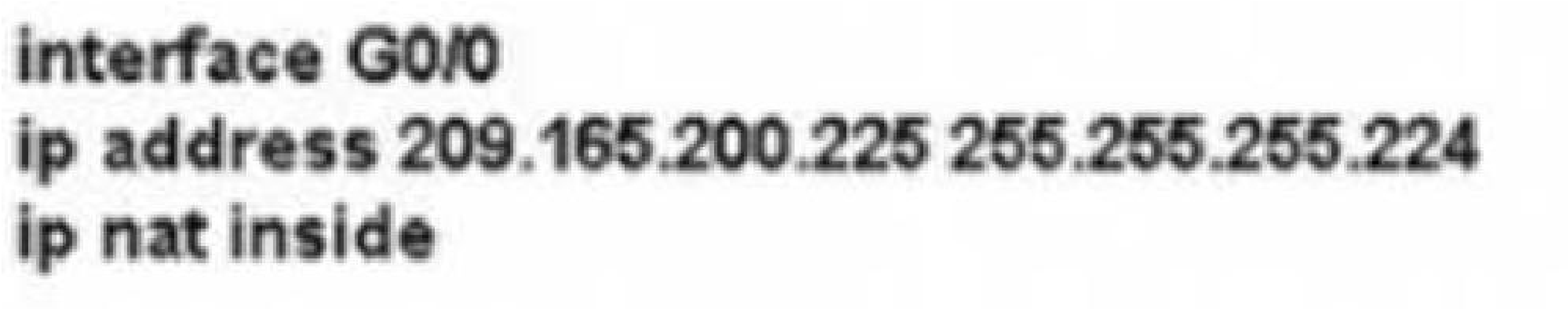
```
interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat inside

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.



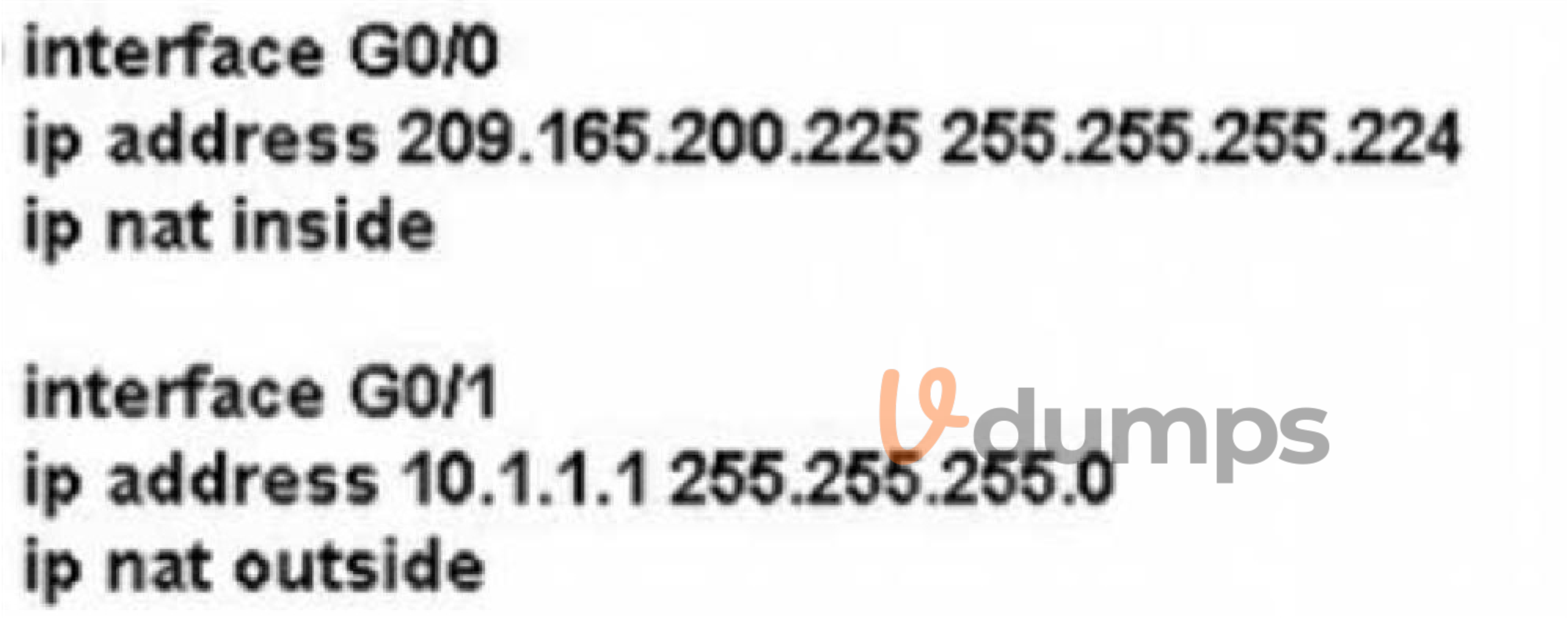
```
interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat outside

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.



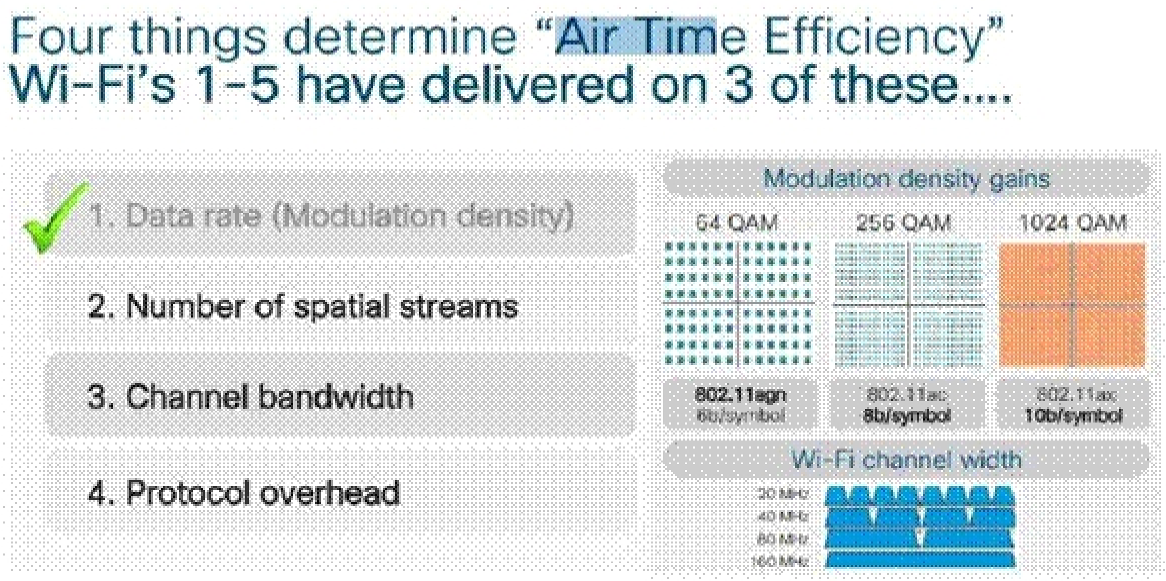
```
interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat inside

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

Correct Answer: B
Section:

QUESTION 80
Which three elements determine Air Time efficiency? (Choose three)

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

Correct Answer: B, C, D
Section:
Explanation:
https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKEWN-3010.pdf



Four things determine "Air Time Efficiency"
Wi-Fi's 1-5 have delivered on 3 of these....

✓ 1. Data rate (Modulation density)

2. Number of spatial streams

3. Channel bandwidth

4. Protocol overhead

QUESTION 81
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.

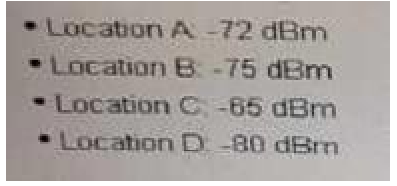
Correct Answer: A, C
Section:

QUESTION 82
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

Correct Answer: D
Section:

QUESTION 83
An engineer measures the Wi-Fi coverage at a customer site. The RSSI values are recorded as follows:



- Location A: -72 dBm
- Location B: -75 dBm
- Location C: -65 dBm
- Location D: -80 dBm

Which two statements does the engineer use to explain these values to the customer? (Choose two)

A. The signal strength at location C is too weak to support web surfing

B. Location D has the strongest RF signal strength

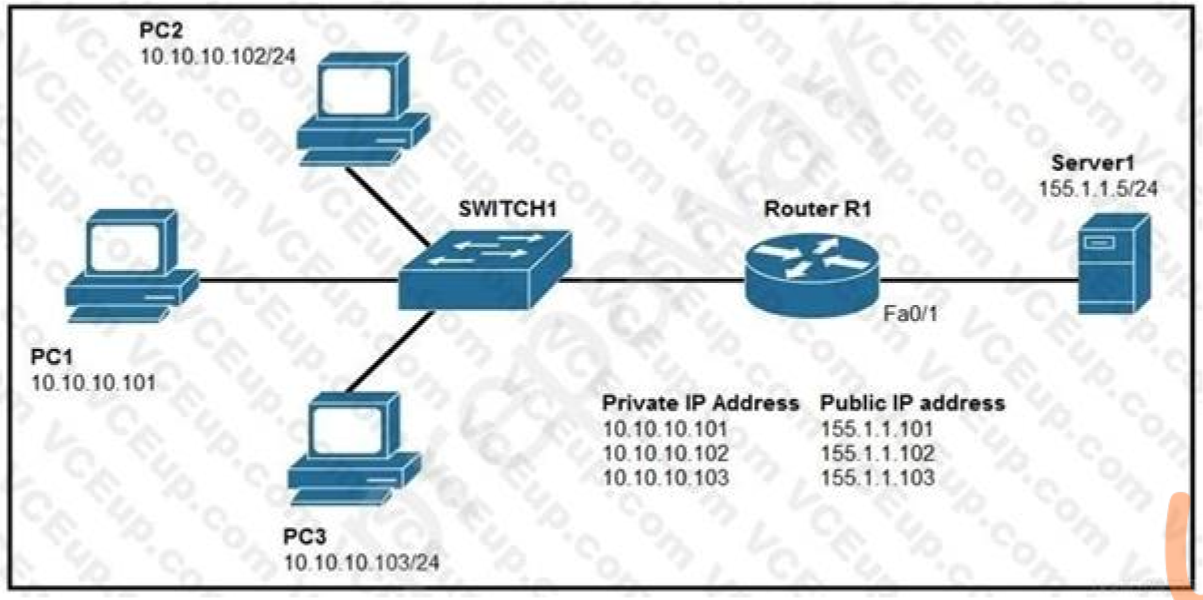
C. The RF signal strength at location B is 50% weaker than location A

D. The signal strength at location B is 10 dB better than location C

E. The RF signal strength at location C is 10 times stronger than location B

Correct Answer: C, E
Section:

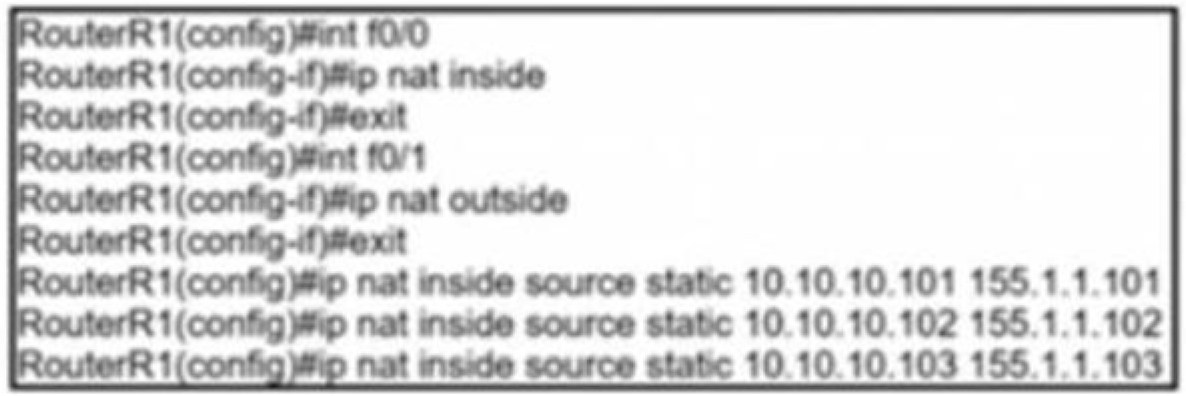
QUESTION 84



Private IP Address	Public IP address
10.10.10.101	155.1.1.101
10.10.10.102	155.1.1.102
10.10.10.103	155.1.1.103

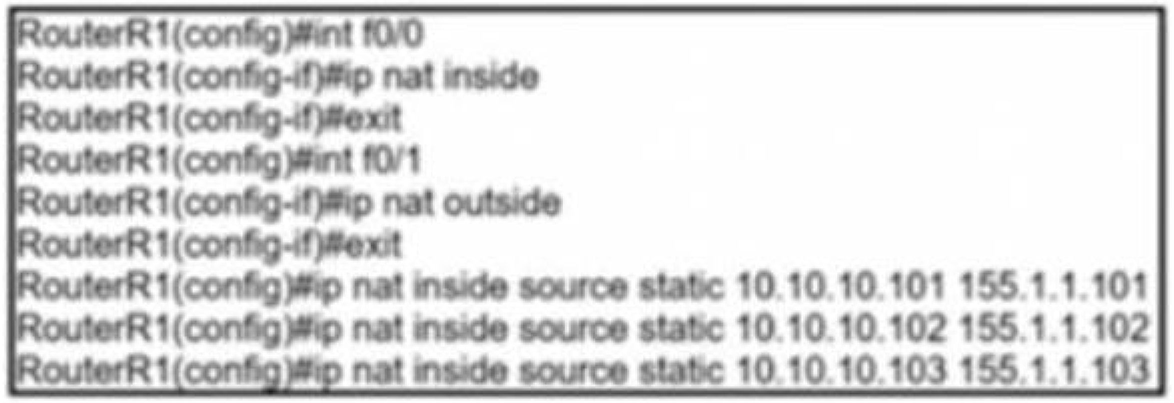
Refer to the exhibit. Which set of commands on router r R1 Allow deterministic translation of private hosts PC1, PC2, and PC3 to addresses in the public space?

A.



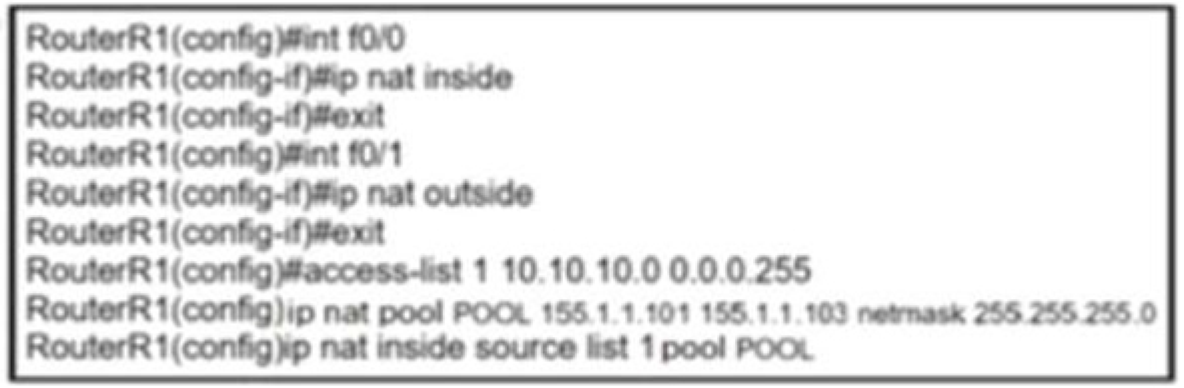
```
RouterR1(config)#int f0/0
RouterR1(config-if)#ip nat inside
RouterR1(config-if)#exit
RouterR1(config)#int f0/1
RouterR1(config-if)#ip nat outside
RouterR1(config-if)#exit
RouterR1(config)#ip nat inside source static 10.10.10.101 155.1.1.101
RouterR1(config)#ip nat inside source static 10.10.10.102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

B.



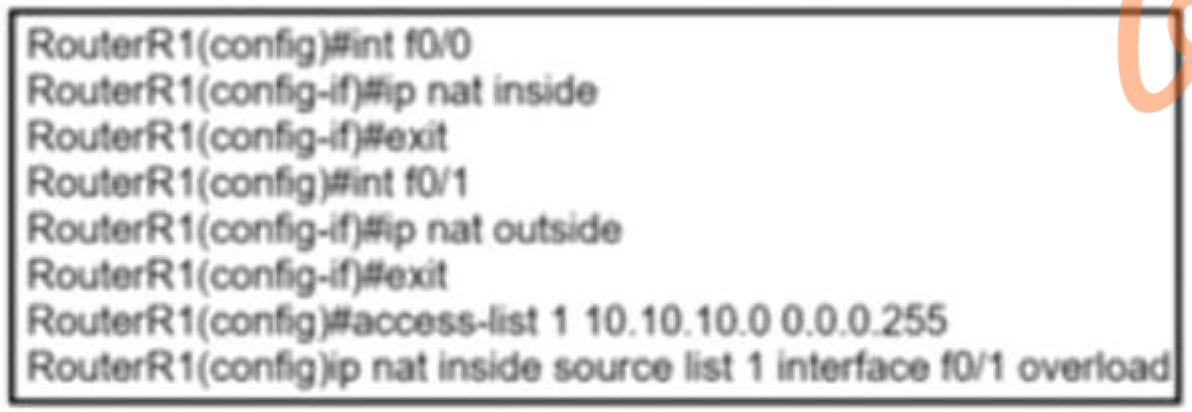
```
RouterR1(config)#int f0/0
RouterR1(config-if)#ip nat inside
RouterR1(config-if)#exit
RouterR1(config)#int f0/1
RouterR1(config-if)#ip nat outside
RouterR1(config-if)#exit
RouterR1(config)#ip nat inside source static 10.10.10.101 155.1.1.101
RouterR1(config)#ip nat inside source static 10.10.10.102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

C.



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

D.



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

Correct Answer: A
Section:

QUESTION 85
What is a characteristic of YANG?

A. It is a Cisco proprietary language that models NETCONF data
B. It allows model developers to create custom data types
C. It structures data in an object-oriented fashion to promote model reuse
D. It provides loops and conditionals to control now within models

Correct Answer: C
Section:

QUESTION 86

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

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

Correct Answer: A, B
Section:

QUESTION 87

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

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

Correct Answer: D
Section:

QUESTION 88

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

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

Correct Answer: A
Section:

QUESTION 89

What is one difference between saltstack and ansible?

A. SaltStack uses an API proxy agent to program Cisco boxes on agent mode, whereas Ansible uses a Telnet connection
B. SaltStack uses the Ansible agent on the box, whereas Ansible uses a Telnet server on the box
C. SaltStack is constructed with minion, whereas Ansible is constructed with YAML
D. SaltStack uses SSH to interact with Cisco devices, whereas Ansible uses an event bus

Correct Answer: C
Section:

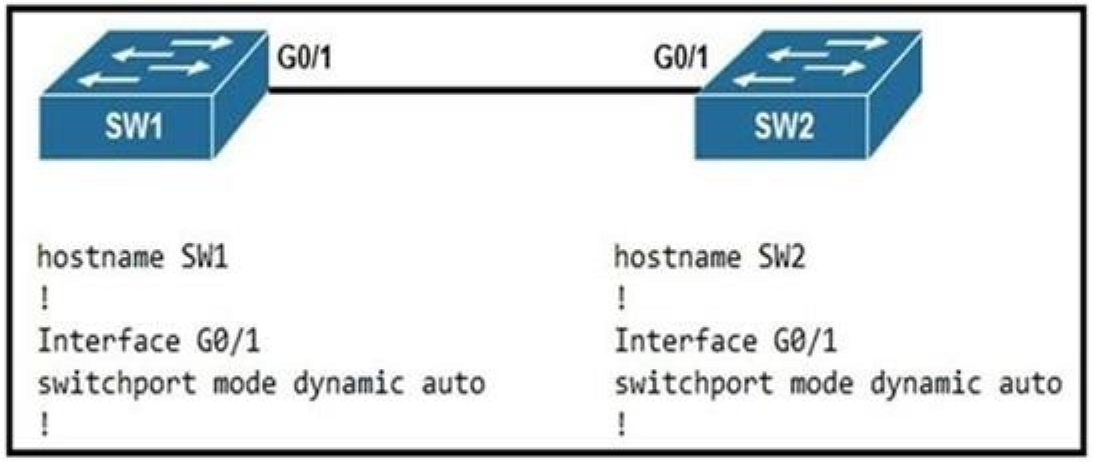
QUESTION 90

A network administrator has designed a network with two multilayer switches on the distribution layer, which act as default gateways for the end hosts. Which two technologies allow every end host in a VLAN to use both gateways? (Choose two)

A. GLBP
B. HSRP
C. MHSRP
D. VSS
E. VRRP

Correct Answer: A, C
Section:

QUESTION 91



```
hostname SW1
!
Interface G0/1
switchport mode dynamic auto
!
```

```
hostname SW2
!
Interface G0/1
switchport mode dynamic auto
!
```

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

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

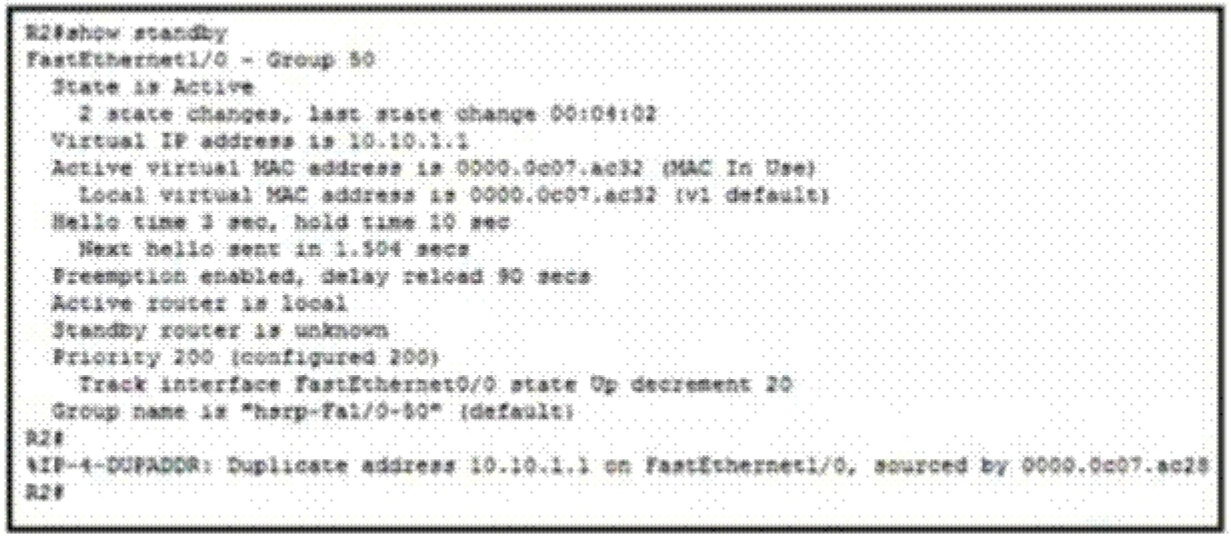
Correct Answer: A
Section:

QUESTION 92
In cisco SD_WAN, which protocol is used to measure link quality?

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

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

QUESTION 93



```
R2#show standby
FastEthernet1/0 - Group 50
  State is Active
    2 state changes, last state change 00:04:02
  Virtual IP address is 10.10.1.1
  Active virtual MAC address is 0000.0c07.ac32 (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac32 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.504 secs
  Preemption enabled, delay reload 90 secs
  Active router is local
  Standby router is unknown
  Priority 200 (configured 200)
    Track interface FastEthernet0/0 state Up decrement 20
  Group name is "hsrp-Fa1/0-50" (default)
R2#
%IP-4-DUPADDR: Duplicate address 10.10.1.1 on FastEthernet1/0, sourced by 0000.0c07.ac28
R2#
```

Refer to the exhibit. An engineer configures a new HSRP group. While reviewing the HSRP status, the engineer sees the logging message generated on R2. Which is the cause of the message?

A. The same virtual IP address has been configured for two HSRP groups
B. The HSRP configuration has caused a spanning-tree loop
C. The HSRP configuration has caused a routing loop
D. A PC is on the network using the IP address 10.10.1.1

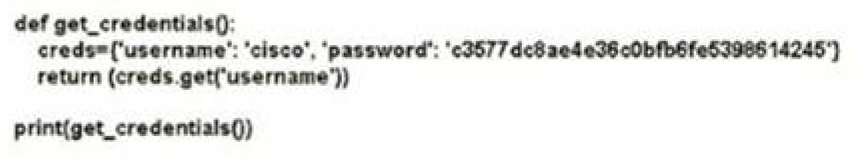
Correct Answer: A
Section:

QUESTION 94
Which measure is used by an NTP server to indicate its closeness to the authoritative time source?

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

Correct Answer: D
Section:

QUESTION 95
What is the output of this code?

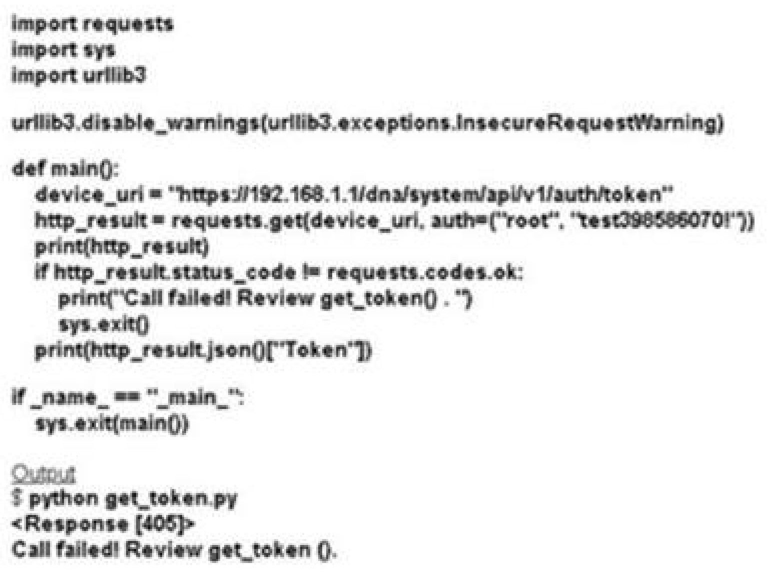


```
def get_credentials():
    creds={'username': 'cisco', 'password': 'c3577dc8ae4e36c0bfb6fe5398614245'}
    return (creds.get('username'))

print(get_credentials())
```

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

Correct Answer: D
Section:

QUESTION 96
An engineer runs the code against an API of Cisco DMA Center, and the platform returns this output What does the response indicate?



```
import requests
import sys
import urllib3

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

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

if _name_ == "_main_":
   sys.exit(main())
```

Output

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

A. The authentication credentials are incorrect

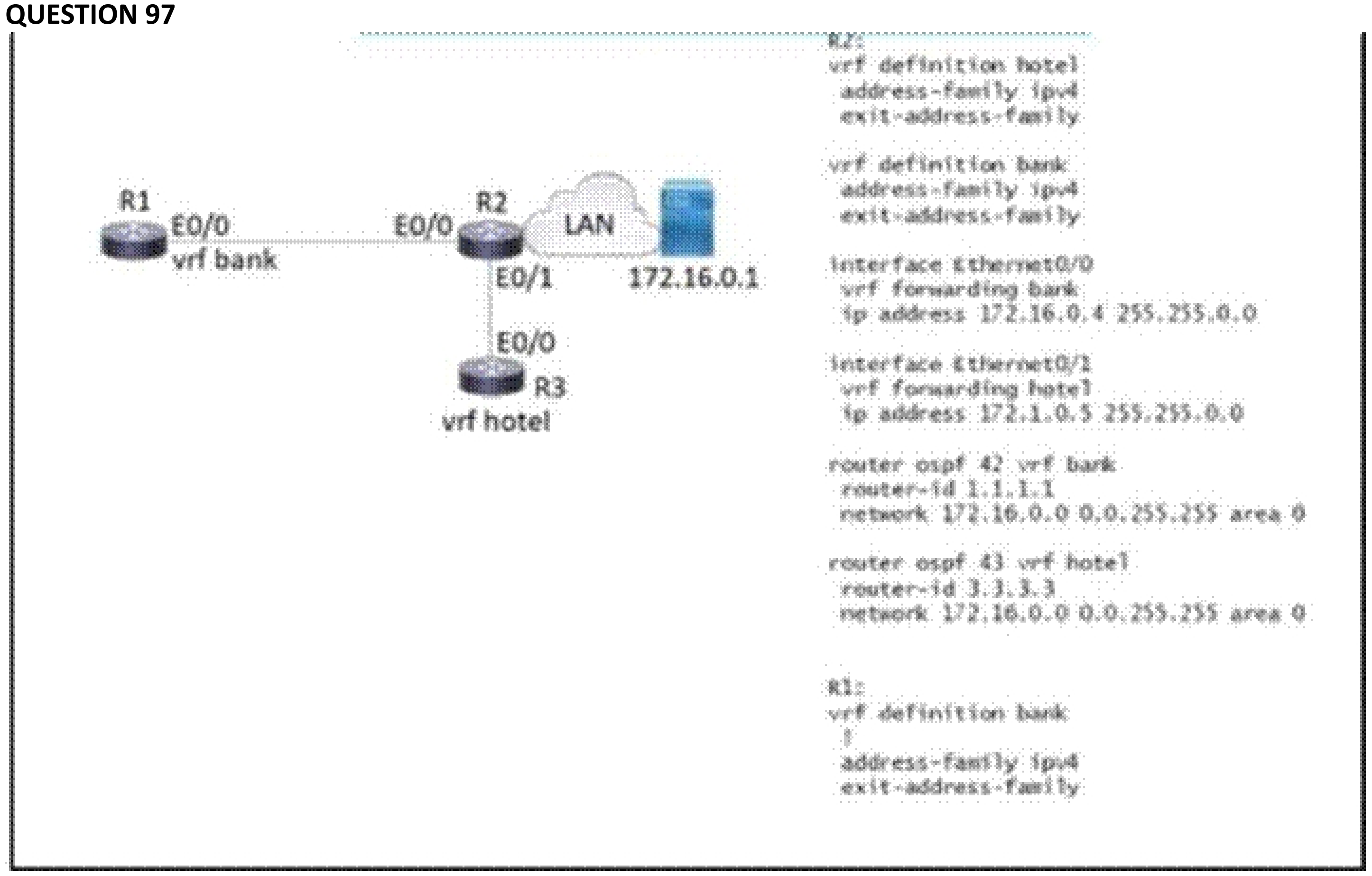
B. The URl string is incorrect.

C. The Cisco DNA Center API port is incorrect

D. The HTTP method is incorrect

Correct Answer: D
Section:
Explanation:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status

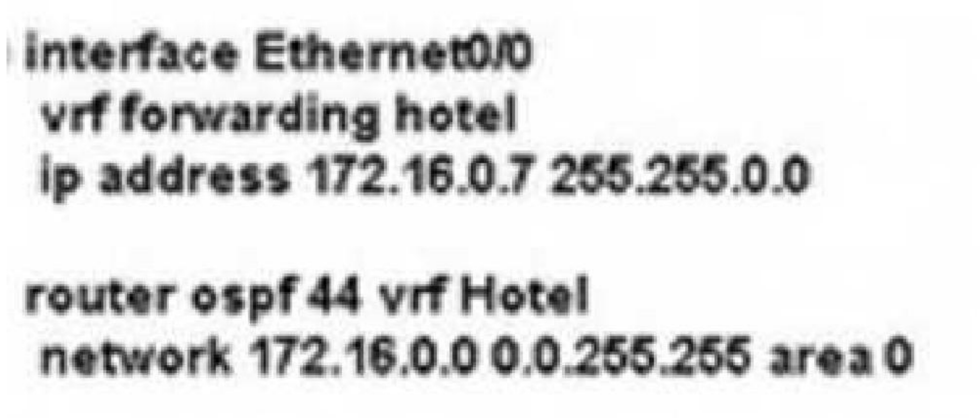
QUESTION 97



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

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

interface Ethernet0/0
 vrf forwarding bank
 ip address 172.16.0.4 255.255.0.0

interface Ethernet0/1
 vrf forwarding hotel
 ip address 172.1.0.5 255.255.0.0

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

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


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

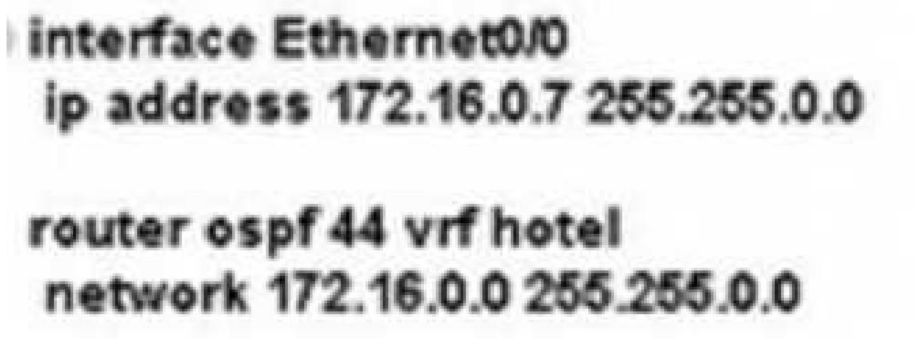
Refer to the exhibit. Which configuration must be applied to R to enable R to reach the server at 172.16.0.1?

A.



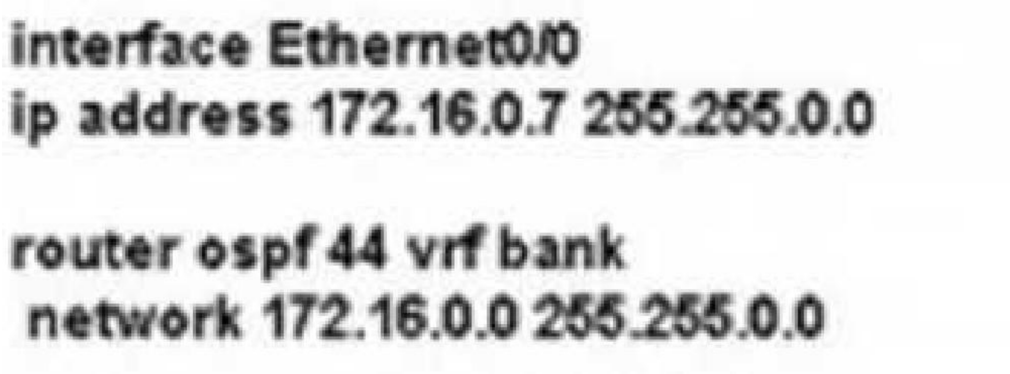
```
interface Ethernet0/0
 vrf forwarding hotel
 ip address 172.16.0.7 255.255.0.0

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

B.



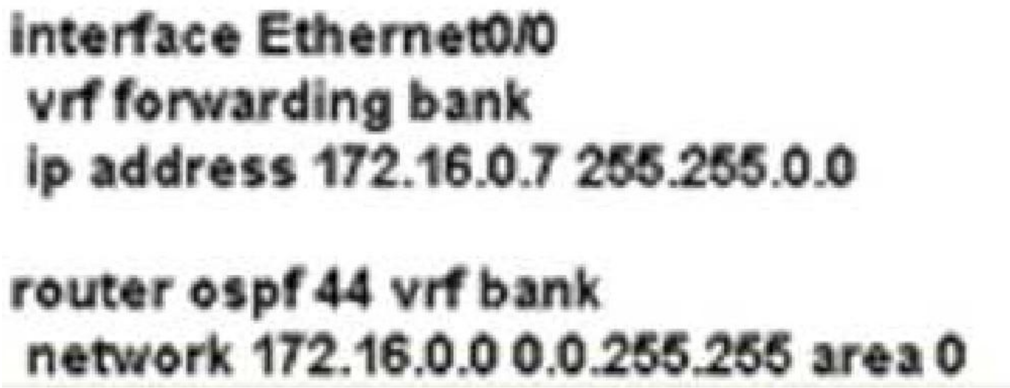
```
interface Ethernet0/0
 ip address 172.16.0.7 255.255.0.0

router ospf 44 vrf hotel
 network 172.16.0.0 255.255.0.0
```

C.



```
interface Ethernet0/0
ip address 172.16.0.7 255.255.0.0

router ospf 44 vrf bank
 network 172.16.0.0 255.255.0.0
```

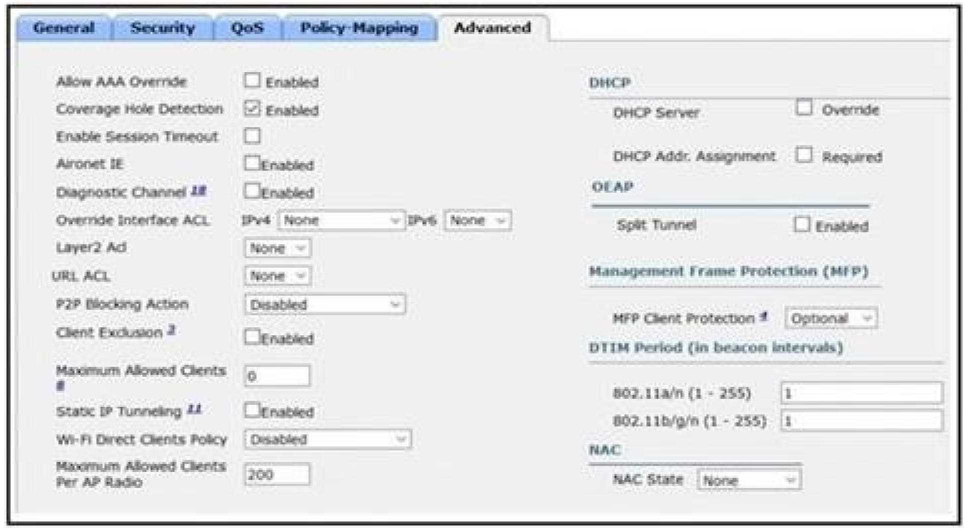
D.



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

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

Correct Answer: D
Section:

QUESTION 98



General | Security | QoS | Policy-Mapping | Advanced

Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout □
Aironet IE □ Enabled
Diagnostic Channel [18] □ Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
URL ACL None
P2P Blocking Action Disabled
Client Exclusion [2] □ Enabled
Maximum Allowed Clients [8] 0
Static IP Tunneling [11] □ Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

OEAP
Split Tunnel □ Enabled

Management Frame Protection (MFP)
MFP Client Protection [4] Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
NAC State None

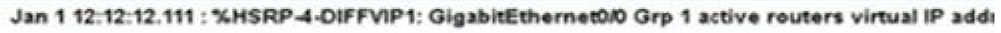
Refer to the exhibit. An engineer has configured Cisco ISE to assign VLANs to clients based on their method of authentication, but this is not working as expected. Which action will resolve this issue?

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

Correct Answer: B
Section:

QUESTION 99

While configuring an IOS router for HSRP with a virtual IP of 10 1.1.1. an engineer sees this log message.



```
Jan 1 12:12:12.111 : %HSRP-4-DIFFVIP1: GigabitEthernet0/0 Grp 1 active routers virtual IP add
```

Which configuration change must the engineer make?

A. Change the HSRP group configuration on the local router to 1.
B. Change the HSRP virtual address on the local router to 10.1.1.1.
C. Change the HSRP virtual address on the remote router to 10.1.1.1.
D. Change the HSRP group configuration on the remote router to 1.

Correct Answer: B
Section:

QUESTION 100

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

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

Correct Answer: B
Section:

QUESTION 101

A network engineer configures BGP between R1 and R2. Both routers use BGP peer group CORP and are set up to use MD5 authentication. This message is logged to the console of router R1:
"May 5 39:85:55.469: %TCP-6-BADAUTH" Invalid MD5 digest from 10.10.10.1 (29832) to 10.120.10.1 (179) tebleid -0
Which two configuration allow peering session to from between R1 and R2? Choose two.)

A. R1(config-router)#neighbor 10.10.10.1 peer-group CORP R1(config-router)#neighbor CORP password Cisco
B. R2(config-router)#neighbor 10.120.10.1 peer-group CORP R2(config-router)#neighbor CORP password Cisco
C. R2(config-router)#neighbor 10.10.10.1 peer-group CORP R2(config-router)#neighbor PEER password Cisco
D. R1(config-router)#neighbor 10.120.10.1 peer-group CORP R1(config-router)#neighbor CORP password Cisco
E. R2(config-router)#neighbor 10.10.10.1 peer-group CORP R2(config-router)#neighbor CORP password Cisco

Correct Answer: A, B
Section:

QUESTION 102

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

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

Correct Answer: D, E
Section:

QUESTION 103

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

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

Correct Answer: C, D
Section:

QUESTION 104

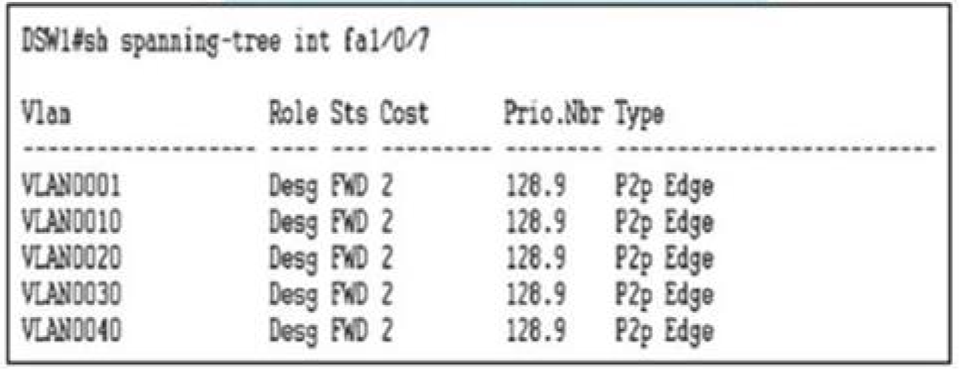
which entity is a Type 1 hypervisor?

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

Correct Answer: C

Section:

QUESTION 105



```
DSW1#sh spanning-tree int fa1/0/7

Vlan                Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
VLAN0001            Desg FWD 2         128.9    P2p Edge
VLAN0010            Desg FWD 2         128.9    P2p Edge
VLAN0020            Desg FWD 2         128.9    P2p Edge
VLAN0030            Desg FWD 2         128.9    P2p Edge
VLAN0040            Desg FWD 2         128.9    P2p Edge
```

Refer to the exhibit How was spanning-tree configured on this interface?

A. By entering the command spanning-tree portfast trunk in the interface configuration mode.

B. By entering the command spanning-tree portfast in the interface configuration mode

C. By entering the command spanning-tree mst1 vlan 10,20,30,40 in the global configuration mode

D. By entering the command spanning-tree vlan 10,20,30,40 root primary in the interface configuration mode

Correct Answer: A
Section:

QUESTION 106
What is a characteristic of a next-generation firewall?

A. only required at the network perimeter

B. required in each layer of the network

C. filters traffic using Layer 3 and Layer 4 information only

D. provides intrusion prevention

Correct Answer: D
Section:
Explanation:
The feature set for NGFWs build upon traditional firewall features by including critical security functions like intrusion prevention, VPN, and anti-virus, and even encrypted web traffic inspection to help prevent packets containing malicious content from entering the network

QUESTION 107
which features does Cisco EDR use to provide threat detection and response protection?

A. containment, threat intelligence, and machine learning

B. firewalling and intrusion prevention

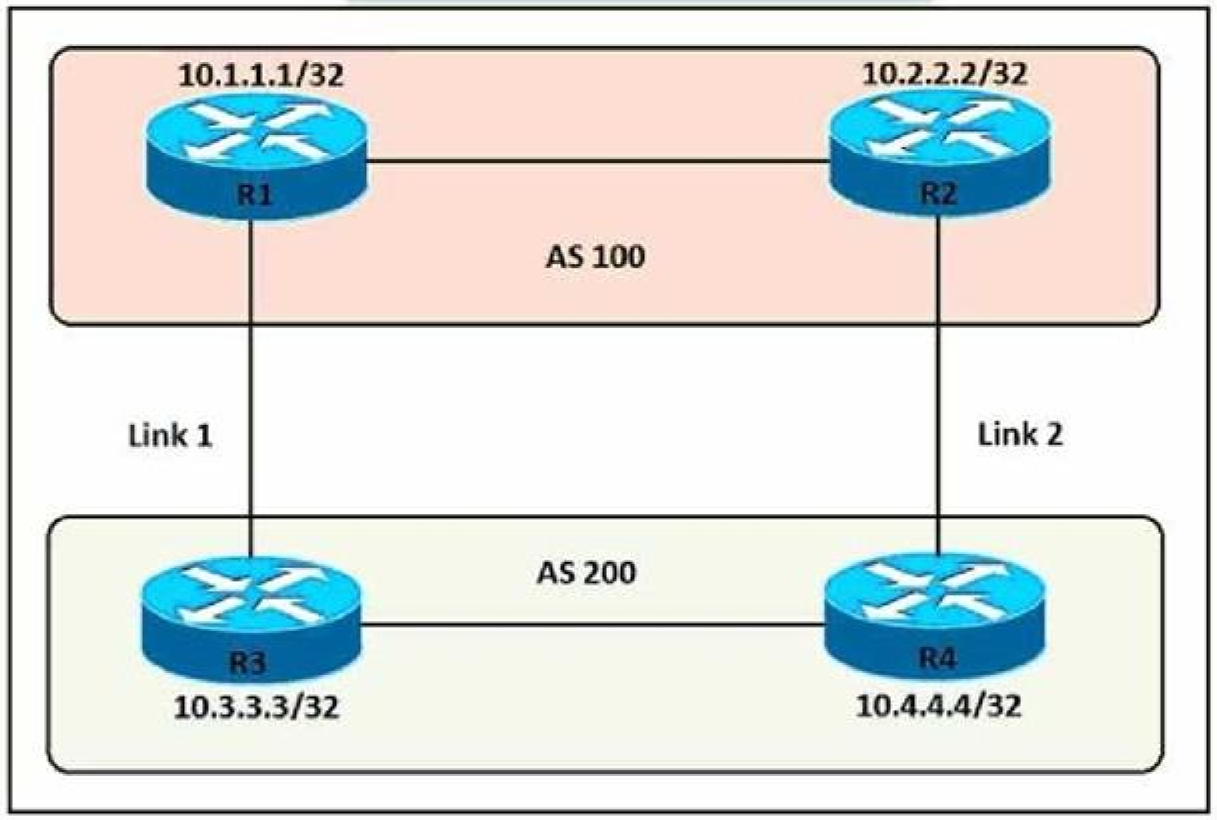
C. container-based agents

D. cloud analysis and endpoint firewall controls

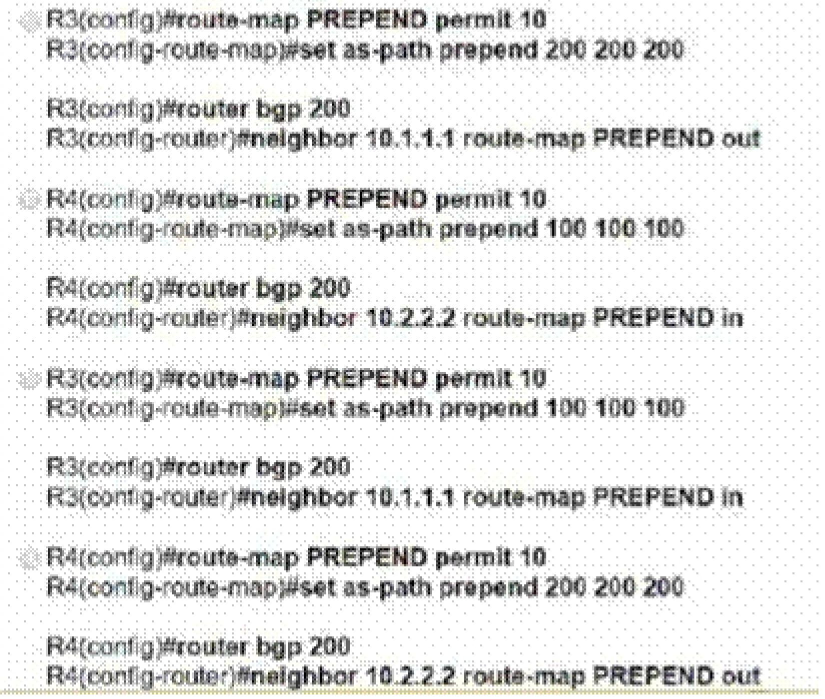
Correct Answer: B
Section:

QUESTION 108

Refer to the exhibit.



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



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

  R3(config)#router bgp 200
  R3(config-router)#neighbor 10.1.1.1 route-map PREPEND out

○ R4(config)#route-map PREPEND permit 10
  R4(config-route-map)#set as-path prepend 100 100 100

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

○ R3(config)#route-map PREPEND permit 10
  R3(config-route-map)#set as-path prepend 100 100 100

  R3(config)#router bgp 200
  R3(config-router)#neighbor 10.1.1.1 route-map PREPEND in

○ R4(config)#route-map PREPEND permit 10
  R4(config-route-map)#set as-path prepend 200 200 200

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

A. Option A

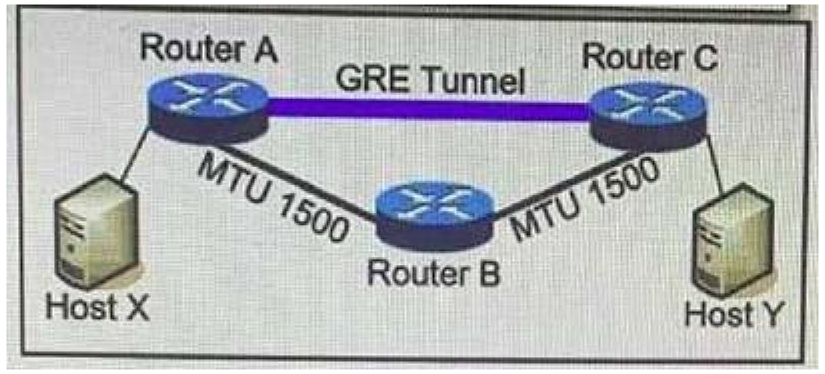
B. Option B

C. Option C

D. Option D

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

QUESTION 109
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.

Correct Answer: D
Section:

QUESTION 110
What is one benefit of implementing a VSS architecture?

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

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

QUESTION 111
What does Call Admission Control require the client to send in order to reserve the bandwidth?

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

Correct Answer: C
Section:

QUESTION 112
Which function in handled by vManage in the cisco SD-WAN fabric?

A. Establishes BFD sessions to test liveliness of links and nodes.
B. Distributes polices that govern data forwarding.
C. Performs remote software upgrades for WAN Edge vSmart and vBond.
D. Establishes iPsec tunnels with nodes

Correct Answer: C
Section:

QUESTION 113
Where is radio resource management performed in a cisco SD-access wireless solution?

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

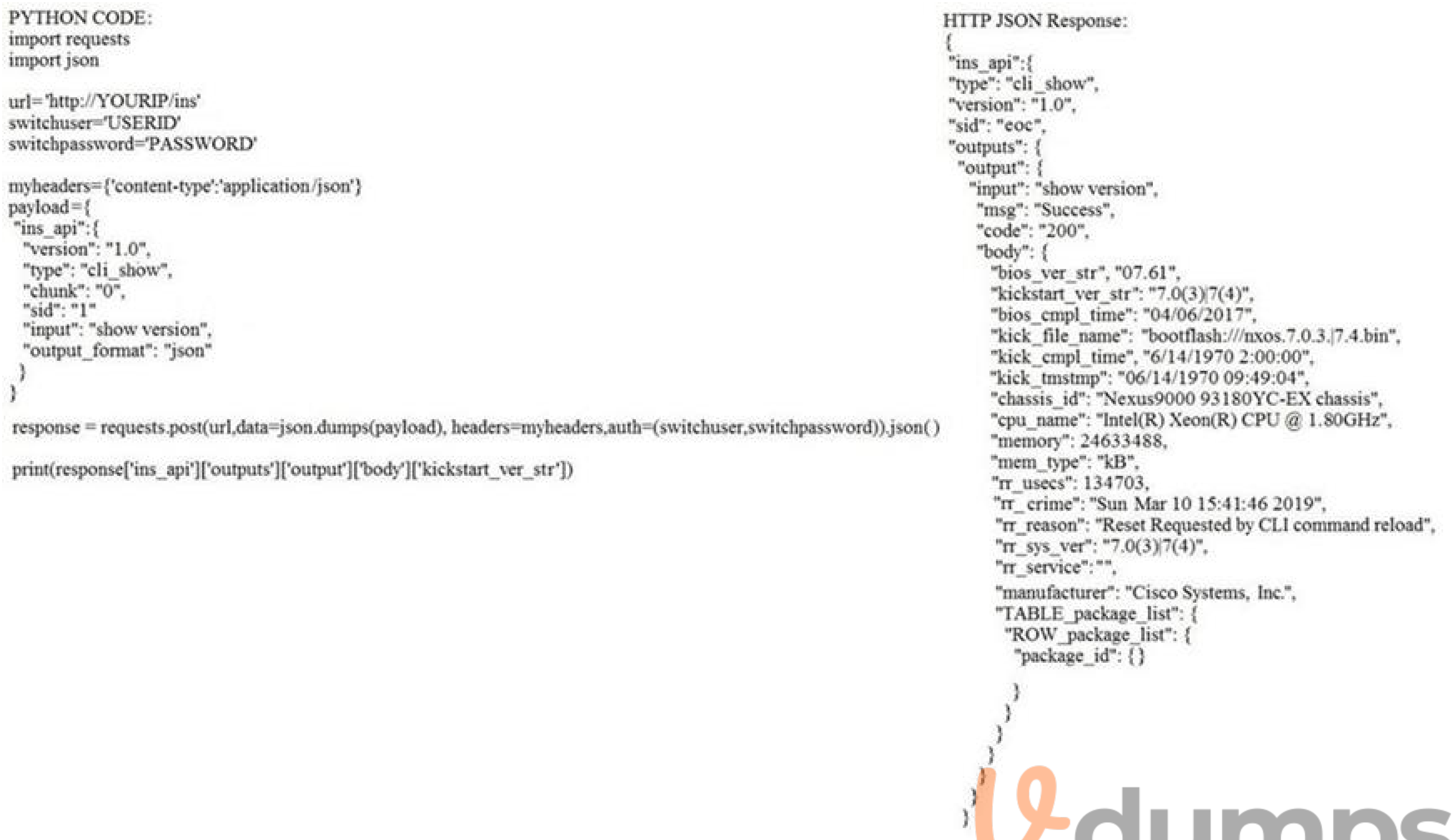
Correct Answer: C
Section:
Explanation:
Fabric wireless controllers manage and control the fabric-mode APs using the same general model as the traditional local-mode controllers which offers the same operational advantages such as mobility control and radio resource management. A significant difference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

QUESTION 114
How does EIGRP differ from OSPF?

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

Correct Answer: B
Section:

QUESTION 115
Refer to the exhibit.



```
PYTHON CODE:
import requests
import json

url='http://YOURIP/ins'
switchuser='USERID'
switchpassword='PASSWORD'

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

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

```
HTTP JSON Response:
{
 "ins_api":{
 "type": "cli_show",
 "version": "1.0",
 "sid": "eoc",
 "outputs": {
  "output": {
    "input": "show version",
     "msg": "Success",
     "code": "200",
     "body": {
       "bios_ver_str", "07.61",
       "kickstart_ver_str": "7.0(3)|7(4)",
       "bios_cmpl_time": "04/06/2017",
       "kick_file_name": "bootflash:///nxos.7.0.3.|7.4.bin",
       "kick_cmpl_time", "6/14/1970 2:00:00",
       "kick_tmstmp": "06/14/1970 09:49:04",
       "chassis_id": "Nexus9000 93180YC-EX chassis",
       "cpu_name": "Intel(R) Xeon(R) CPU @ 1.80GHz",
       "memory": 24633488,
       "mem_type": "kB",
       "rr_usecs": 134703,
       "rr_ crime": "Sun Mar 10 15:41:46 2019",
       "rr_reason": "Reset Requested by CLI command reload",
       "rr_sys_ver": "7.0(3)|7(4)",
       "rr_service": "",
       "manufacturer": "Cisco Systems, Inc.",
       "TABLE_package_list": {
        "ROW_package_list": {
         "package_id": {}

        }
       }
      }
     }
    }
   }
  }
```

Which HTTP JSON response does the python code output give?

A. NameError: name 'json' is not defined

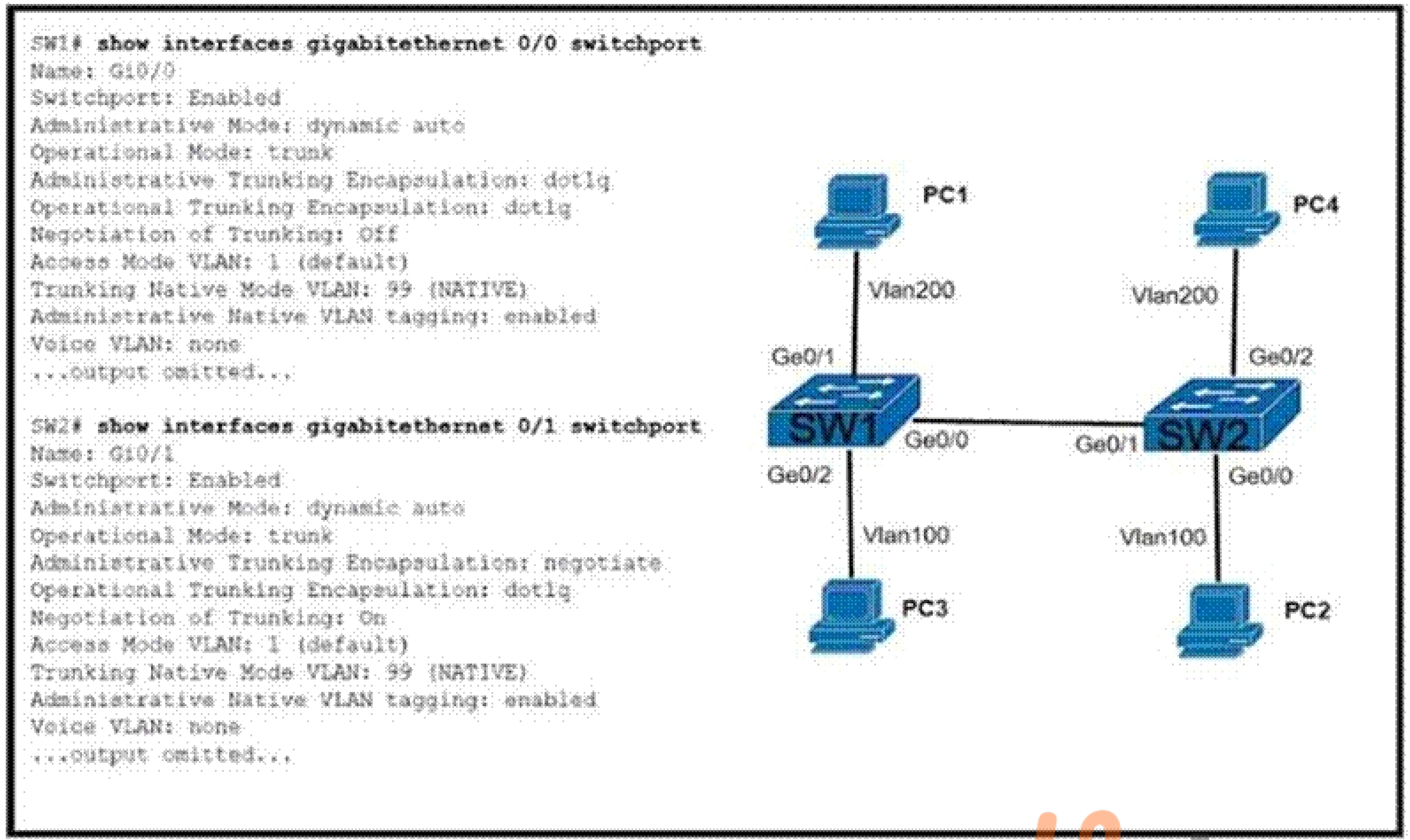
B. KeyError 'kickstart_ver_str'

C. 7.61

D. 7.0(3)I7(4)

Correct Answer: D
Section:

QUESTION 116



```
SW1# show interfaces gigabitethernet 0/0 switchport
Name: Gi0/0
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (NATIVE)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
...output omitted...

SW2# show interfaces gigabitethernet 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (NATIVE)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
...output omitted...
```

Refer to the exhibit. The connecting between SW1 and SW2 is not operational. Which two actions resolve the issue? (Choose two)

A. configure switchport mode access on SW2

B. configure switchport nonegotiate on SW2

C. configure switchport mode trunk on SW2

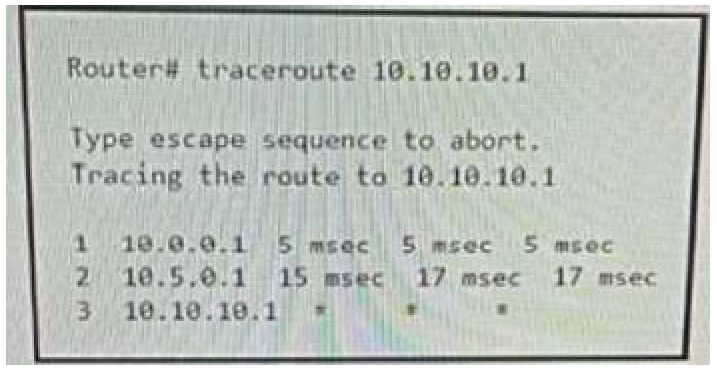
D. configure switchport nonegotiate on SW1

E. configure switchport mode dynamic desirable on SW2

Correct Answer: C, E
Section:

QUESTION 117

Refer to the exhibit.



```
Router# traceroute 10.10.10.1

Type escape sequence to abort.
Tracing the route to 10.10.10.1

1  10.0.0.1   5 msec   5 msec   5 msec
2  10.5.0.1   15 msec  17 msec  17 msec
3  10.10.10.1   *       *       *
```

An engineer is troubleshooting a connectivity issue and executes a 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

Correct Answer: D
Section:
Explanation:

In Cisco routers, the codes for a traceroute command reply are:
! - success
* - time out
N - network unreachable
H - host unreachable
P - protocol unreachable
A - admin denied
Q - source quench received (congestion)
? - unknown (any other ICMP message)In Cisco routers, the codes for a traceroute command reply are:
! - success
* - time out
N - network unreachable
H - host unreachable
P - protocol unreachable
A - admin denied
Q - source quench received (congestion)
? - unknown (any other ICMP message)

QUESTION 118
Which device makes the decision for a wireless client to roam?

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

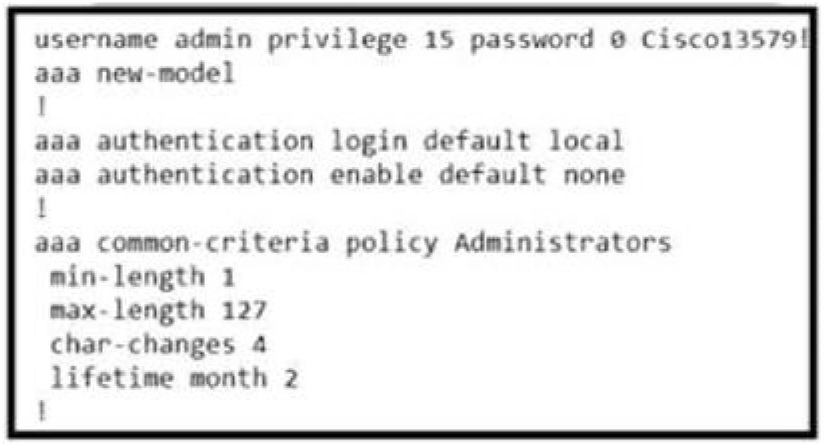
Correct Answer: A
Section:

QUESTION 119
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

Correct Answer: A
Section:

QUESTION 120



```
username admin privilege 15 password 0 Cisco13579!
aaa new-model
!
aaa authentication login default local
aaa authentication enable default none
!
aaa common-criteria policy Administrators
 min-length 1
 max-length 127
 char-changes 4
 lifetime month 2
!
```

Refer to the exhibit. A network engineer must configure a password expiry mechanism on the gateway router for all local passwords to expire after 60 days. What is required to complete this task?

A. The password expiry mechanism is on the AAA server and must be configured there.
B. Add the aaa authentication enable default Administrators command.
C. Add the username admin privilege 15 common-criteria*policy Administrators password 0 Cisco13579! command.
D. No further action Is required. The configuration is complete.

Correct Answer: C
Section:
Explanation:
Perform this task to create a password security policy and to apply the policy to a specific user profile.
Device> enable
Device# configure terminal
Device(config)# aaa new-model

```
Device(config)# aaa common-criteria policy policy1
Device(config-cc-policy)# char-changes 4
Device(config-cc-policy)# max-length 20
Device(config-cc-policy)# min-length 6
Device(config-cc-policy)# numeric-count 2
Device(config-cc-policy)# special-case 2
Device(config-cc-policy)# exit
Device(config)# username user1 common-criteria-policy policy1 password password1 Device(config)# end
```

QUESTION 121

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

A. handle, maintain, and gather configuration and status for nodes within the SD-WAN fabric

B. distribute policies that govern data forwarding performed within the SD-WAN fabric

C. gather telemetry data from vEdge routers

D. onboard vEdge nodes into the SD-WAN fabric

Correct Answer: B

Section:

QUESTION 122

What is the function of the LISP map resolver?

A. to send traffic to non-LISP sites when connected to a service provider that does not accept nonroutable EIDs as packet sources

B. to connect a site to the LISP-capable part of a core network publish the EID-to-RLOC mappings for the site, and respond to map-request messages

C. to decapsulate map-request messages from ITRs and forward the messages to the MS.

D. to advertise routable non-LISP traffic from one address family to LISP sites in a different address family

Correct Answer: C

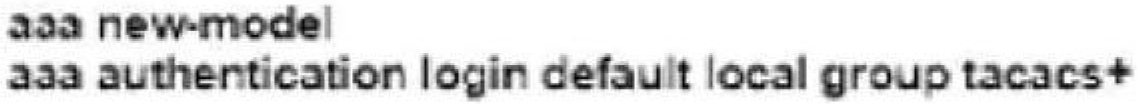
Section:

Explanation:

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

QUESTION 123

A network administrator applies the following configuration to an IOS device.



```
aaa new-model
aaa authentication login default local group tacacs+
```

What is the process of password checks when a login attempt is made to the device?

A. A TACACS+server is checked first. If that check fail, a database is checked?

B. A TACACS+server is checked first. If that check fail, a RADIUS server is checked. If that check fail. a local database is checked.

C. A local database is checked first. If that fails, a TACACS+server is checked, if that check fails, a RADUIS server is checked.

D. A local database is checked first. If that check fails, a TACACS+server is checked.

Correct Answer: D

Section:

QUESTION 124
What is the purpose of the LISP routing and addressing architecture?

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

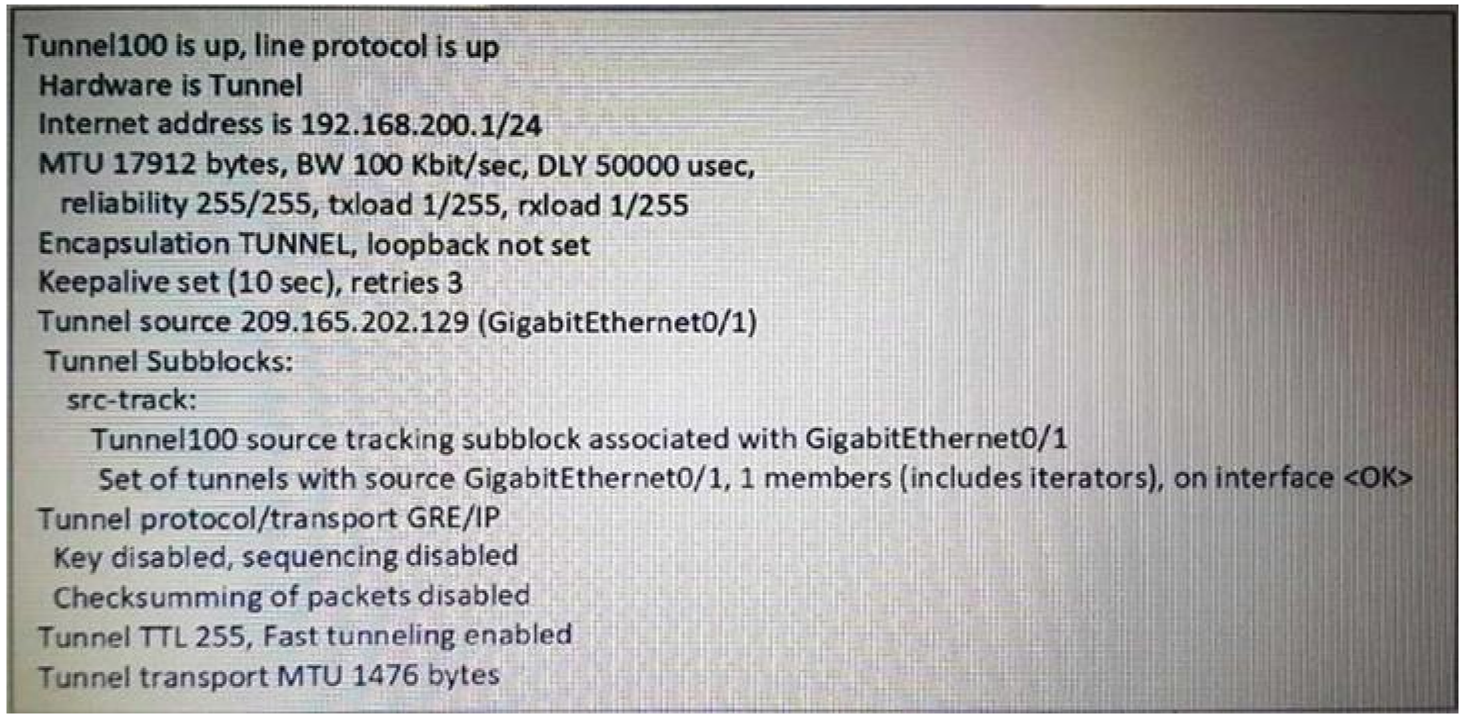
Correct Answer: A
Section:

QUESTION 125
How does Cisco Trustsec enable more access controls for dynamic networking environments and data centers?

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

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

QUESTION 126
Refer to the exhibit.



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

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

A. The keepalive value is modified from the default value.

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

Correct Answer: C
Section:

QUESTION 127
"HTTP/1.1 204 content" is returned when cur –I –x delete command is issued. Which situation hasoccurred?

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

Correct Answer: B
Section:
Explanation:
HTTP Status 204 (No Content) indicates that the server has successfully fulfilled the request and thatthere is no content to send in the response payload body.

QUESTION 128
A company plans to implement intent-based networking in its campus infrastructure. Which design facilities a migrate from a traditional campus design to a programmer fabric designer?

A. Layer 2 access
B. three-tier
C. two-tier
D. routed access

Correct Answer: C
Section:

QUESTION 129
When a wireless client roams between two different wireless controllers, a network connectivity outage is experience for a period of time. Which configuration issue would cause this problem?

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

Correct Answer: B
Section:

QUESTION 130
What is the differences between TCAM and the MAC address table?

A. The MAC address table is contained in CAM ACL and QoS information is stored in TCAM
B. The MAC address table supports partial matches. TCAM requires an exact match

C. Router prefix lookups happens in CAM. MAC address table lookups happen in TCAM.

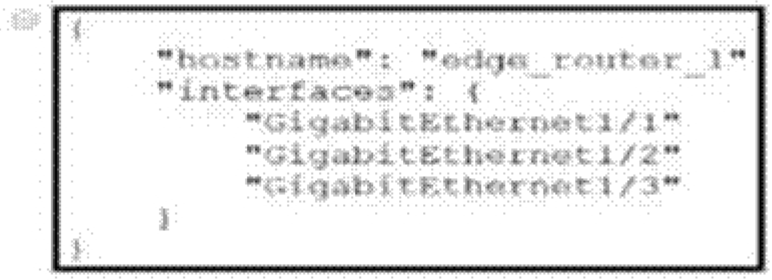
D. TCAM is used to make Layer 2 forwarding decisions CAM is used to build routing tables

Correct Answer: A
Section:
Explanation:
https://community.cisco.com/t5/networking-documents/cam-content-addressable-memory-vstcam-ternary-content/ta-p/3107938When using Ternary Content Addressable Memory (TCAM) inside routers it's used for faster addresslookup that enables fast routing.

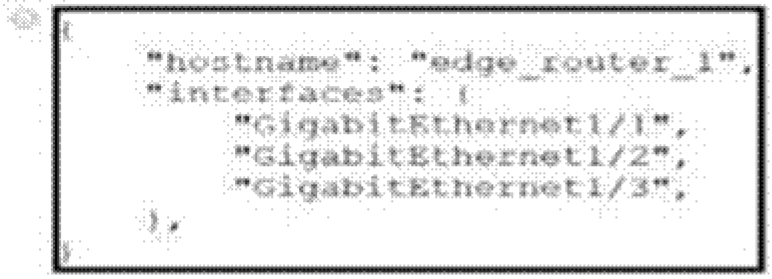
In switches Content Addressable Memory (CAM) is used for building and lookup of mac address table that enables L2 forwarding decisions.

Besides Longest-Prefix Matching, TCAM in today's routers and multilayer Switch devices are used to store ACL, QoS and other things from upper-layer processing.

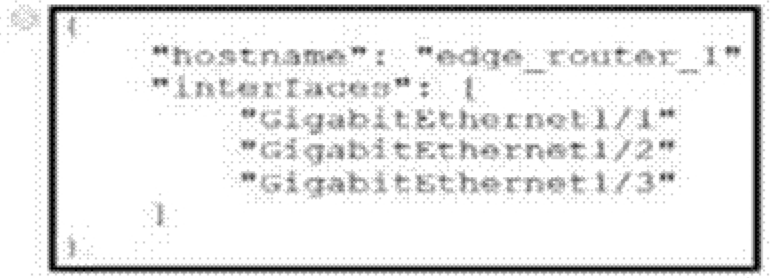
QUESTION 131
Which exhibit displays a valid JSON file?



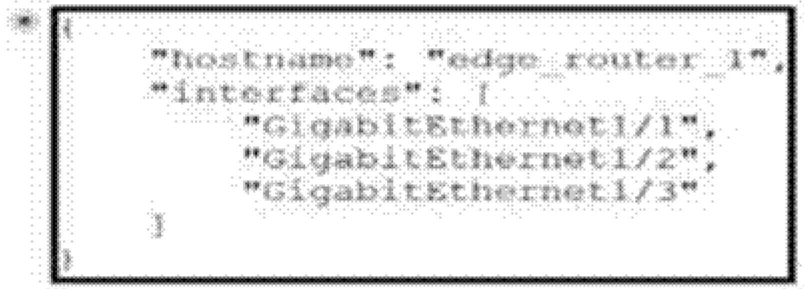
```
{
    "hostname": "edge_router_1"
    "interfaces": {
        "GigabitEthernet1/1"
        "GigabitEthernet1/2"
        "GigabitEthernet1/3"
    ]
}
```



```
{
    "hostname": "edge_router_1",
    "interfaces": {
        "GigabitEthernet1/1",
        "GigabitEthernet1/2",
        "GigabitEthernet1/3",
    },
}
```



```
{
    "hostname": "edge_router_1"
    "interfaces": [
        "GigabitEthernet1/1"
        "GigabitEthernet1/2"
        "GigabitEthernet1/3"
    ]
}
```



```
{
    "hostname": "edge_router_1",
    "interfaces": [
        "GigabitEthernet1/1",
        "GigabitEthernet1/2",
        "GigabitEthernet1/3"
    ]
}
```

A. Option A

B. Option B

C. Option C

D. Option D

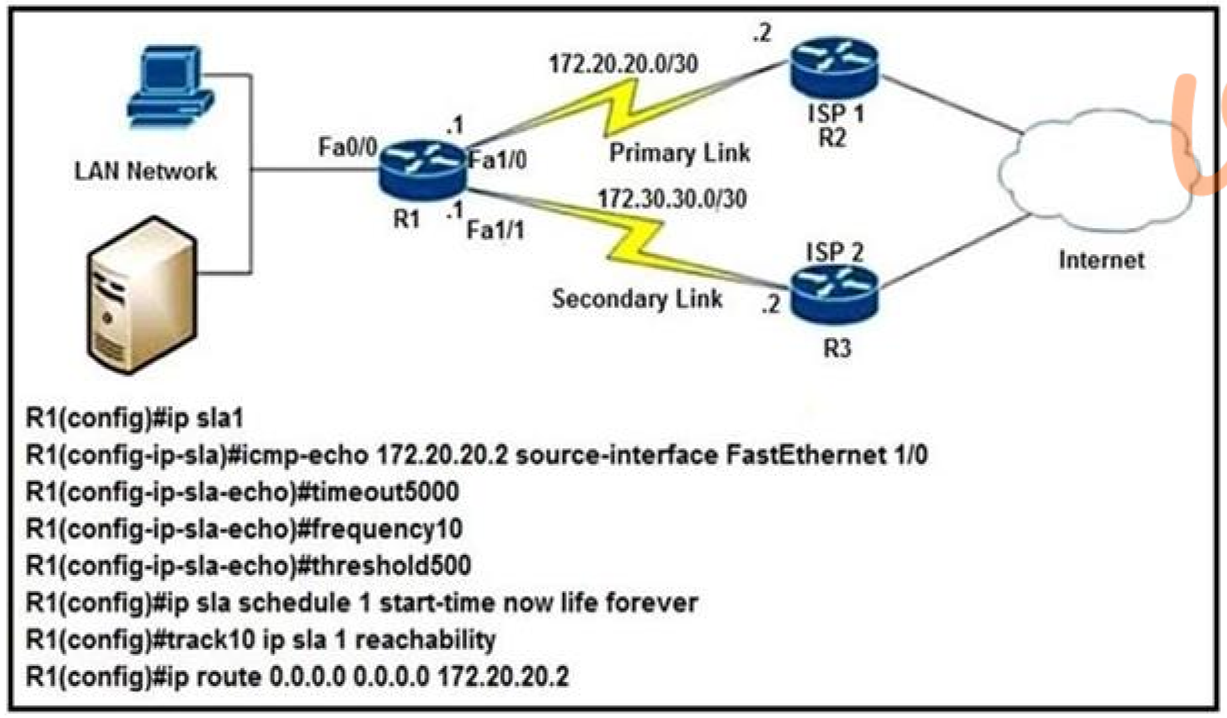
Correct Answer: D
Section:

QUESTION 132
A server running Linux is providing support for virtual machines along with DNS and DHCP services for a small business. Which technology does this represent?

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

Correct Answer: D
Section:
Explanation:
In contrast to type 1 hypervisor, a type 2 hypervisor (or hosted hypervisor) runs on top of an operating system and not the physical hardware directly. A big advantage of Type 2 hypervisors is that management console software is not required. Examples of type 2 hypervisor are VMware Workstation (which can run on Windows, Mac and Linux) or Microsoft Virtual PC (only runs on Windows).

QUESTION 133
Refer to the exhibit.



```
R1(config)#ip sla1
R1(config-ip-sla)#icmp-echo 172.20.20.2 source-interface FastEthernet 1/0
R1(config-ip-sla-echo)#timeout5000
R1(config-ip-sla-echo)#frequency10
R1(config-ip-sla-echo)#threshold500
R1(config)#ip sla schedule 1 start-time now life forever
R1(config)#track10 ip sla 1 reachability
R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2
```

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

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

Correct Answer: C
Section:

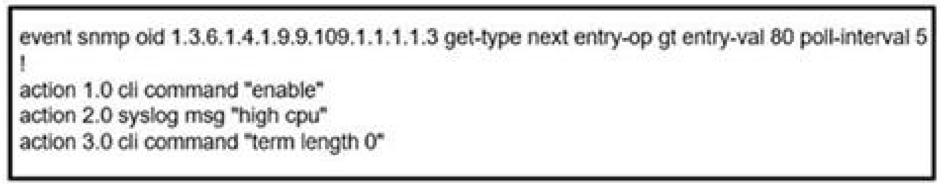
Explanation:
The last command should be "R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2 track 10".

QUESTION 134
If the noise floor is -90 dBm and wireless client is receiving a signal of -75 dBm, what is the SNR?

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

Correct Answer: A
Section:

QUESTION 135



```
event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.3 get-type next entry-op gt entry-val 80 poll-interval 5
!
action 1.0 cli command "enable"
action 2.0 syslog msg "high cpu"
action 3.0 cli command "term length 0"
```

Refer to the exhibit. An engineer must create a script that appends the output of the show process cpu sorted command to a file.

A. action 4.0 syslog command "show process cpu sorted | append flash:high-cpu-file"
B. action 4.0 publish-event "show process cpu sorted | append flash:high-cpu-file"
C. action 4.0 ens-event "show process cpu sorted | append flash:high-cpu-file"
D. action 4.0 cli command "show process cpu sorted | append flash:high-cpu-file"

Correct Answer: D
Section:

QUESTION 136
Which two mechanisms are available to secure NTP? (Choose two.)

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

Correct Answer: D, E
Section:

QUESTION 137
What is the difference between CEF and process switching?

A. CEF processes packets that are too complex for process switching to manage.
B. CEF is more CPU-intensive than process switching.

C. CEF uses the FIB and the adjacency table to make forwarding decisions, whereas process switching punts each packet.

D. Process switching is faster than CEF.

Correct Answer: C
Section:

QUESTION 138
Which AP mode allows an engineer to scan configured channels for rogue access points?

A. sniffer

B. monitor

C. bridge

D. local

Correct Answer: B
Section:

QUESTION 139
What is a characteristic of MACsec?

A. 802.1AE provides encryption and authentication services

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

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

D. 802.1AE is negotiated using Cisco AnyConnect NAM and the SAP protocol

Correct Answer: B
Section:
Explanation:
MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-ofband methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1x Extensible Authentication Protocol (EAP-TLS) or Pre Shared Key (PSK) framework.
Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-9/configuration_guide/sec/b_169_sec_9300_cg/macsec_encryption.html

QUESTION 140
Which method should an engineer use to deal with a long-standing contention issue between any two VMs on the same host?

A. Adjust the resource reservation limits

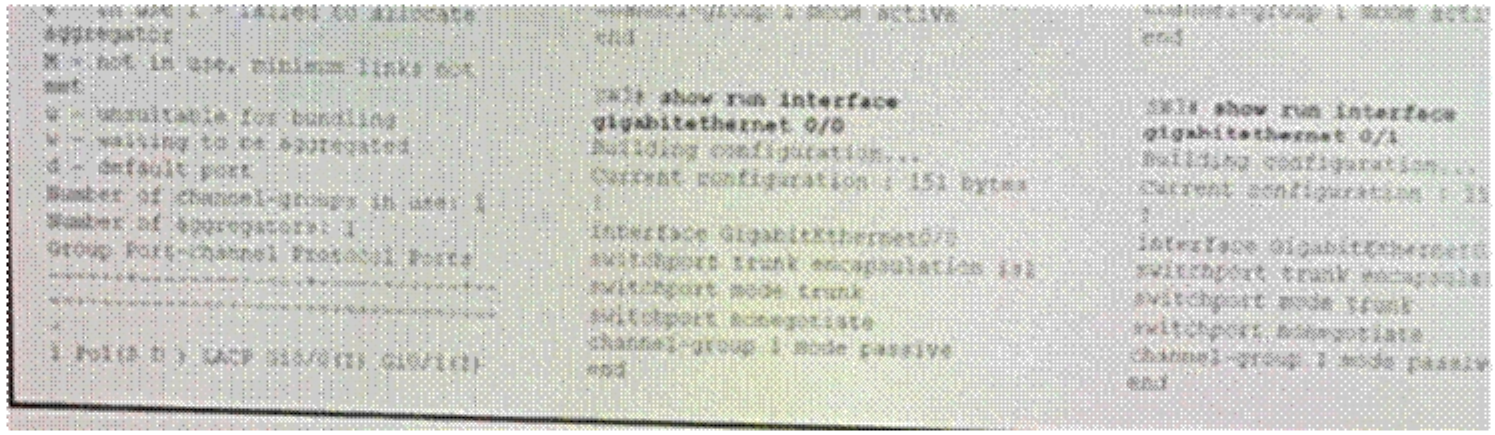
B. Live migrate the VM to another host

C. Reset the VM

D. Reset the host

Correct Answer: A
Section:

QUESTION 141
Refer to the exhibit.



```
[illegible] 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)
```

```
channel-group 1 mode active
end

SW2# show run interface
gigabitethernet 0/0
Building configuration...
Current configuration : 151 bytes
!
interface GigabitEthernet0/0
switchport trunk encapsulation isl
switchport mode trunk
switchport nonegotiate
channel-group 1 mode passive
end
```

```
channel-group 1 mode acti
end

SW3# show run interface
gigabitethernet 0/1
Building configuration...
Current configuration : 15
!
interface GigabitEthernet0
switchport trunk encapsula
switchport mode trunk
switchport nonegotiate
channel-group 1 mode passiv
end
```

The EtherChannel between SW2 and SW3 is not operational which action resolves this issue?

A. Configure the channel-group mode on SW2 Gi0/1 and Gi0/1 to on.

B. Configure the channel-group mode on SW3 Gi0/1 to active

C. Configure the mode on SW2 Gi0/0 to trunk

D. Configure the mode on SW2 Gi0/1 to access.

Correct Answer: B
Section:

QUESTION 142

```
ip nat pool Internet 10.10.10.1 10.10.10.100 netmask 255.255.255.0
ip nat inside source route-map Users pool Internet
!
ip access-list standard Users
 10 permit 192.168.1.0 0.0.0.255
!
route-map Users permit 10
 match ip address Users
```

Refer to the exhibit. Which action completes the configuration to achieve a dynamic continuous mapped NAT for all users?

A. Configure a match-host type NAT pool

B. Reconfigure the pool to use the 192.168 1 0 address range

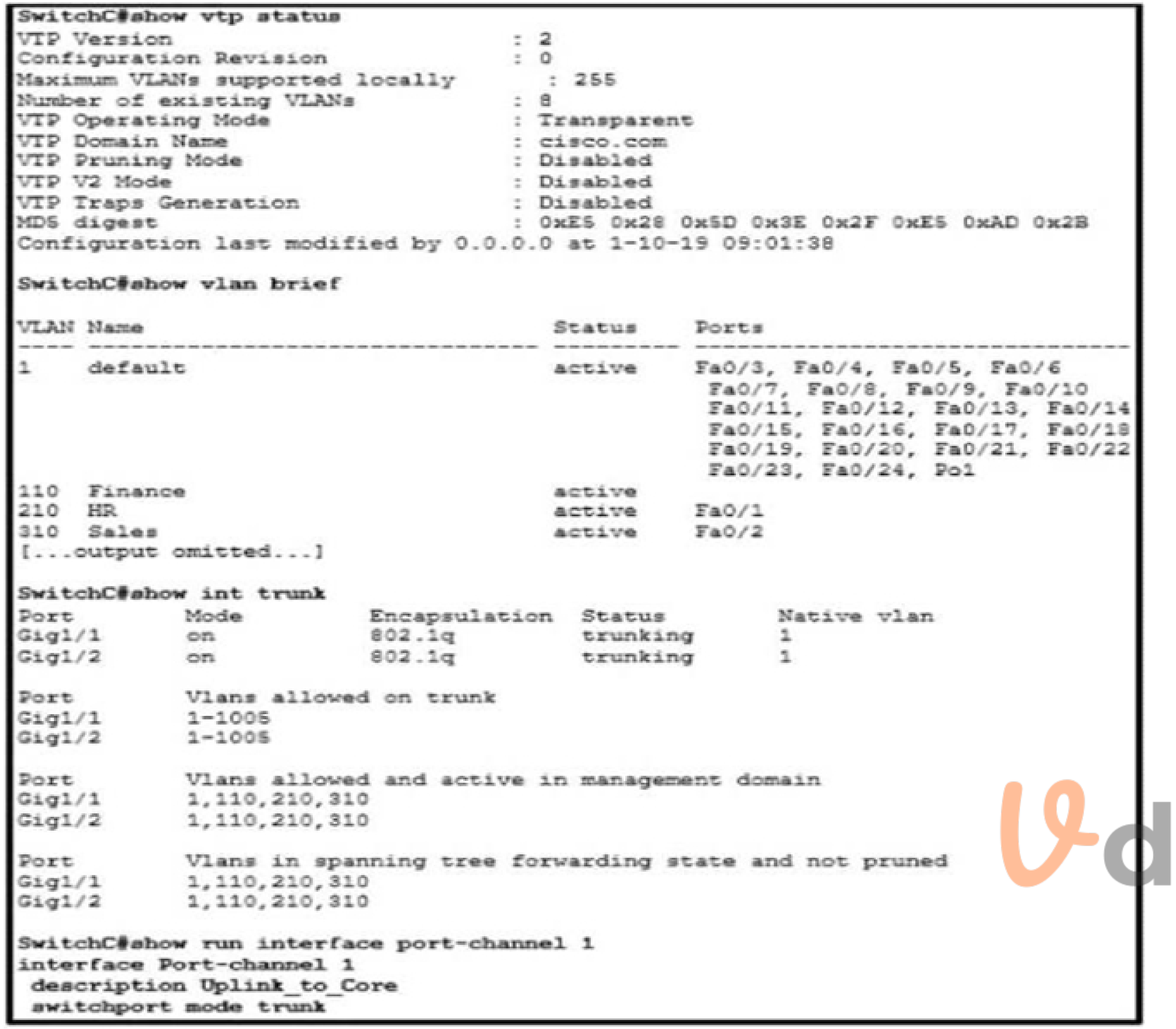
C. Increase the NAT pool size to support 254 usable addresses

D. Configure a one-to-one type NAT pool

Correct Answer: C
Section:

QUESTION 143

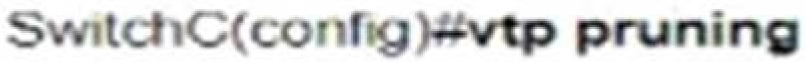
Refer to the exhibit.



```
SwitchC#show vtp status
VTP Version                            : 2
Configuration Revision                 : 0
Maximum VLANs supported locally          : 255
Number of existing VLANs               : 8
VTP Operating Mode                     : Transparent
VTP Domain Name                        : cisco.com
VTP Pruning Mode                       : Disabled
VTP V2 Mode                            : Disabled
VTP Traps Generation                   : Disabled
MD5 digest                             : 0xE5 0x28 0x5D 0x3E 0x2F 0xE5 0xAD 0x2B
Configuration last modified by 0.0.0.0 at 1-10-19 09:01:38

SwitchC#show vlan brief

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

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

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

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

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

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

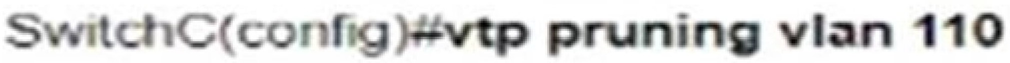
SwitchC connects HR and Sales to the Core switch However, business needs require that no traffic from the Finance VLAN traverse this switch Which command meets this requirement?

A.



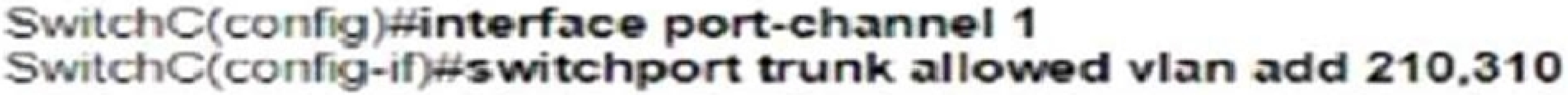
```
SwitchC(config)#vtp pruning
```

B.



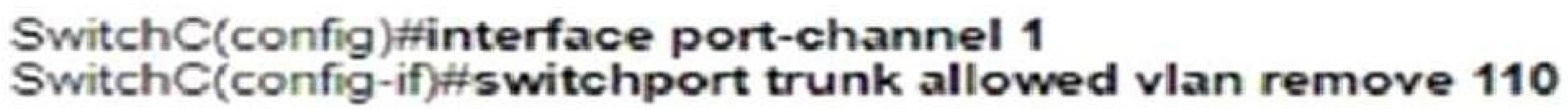
```
SwitchC(config)#vtp pruning vlan 110
```

C.



```
SwitchC(config)#interface port-channel 1
SwitchC(config-if)#switchport trunk allowed vlan add 210,310
```

D.



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

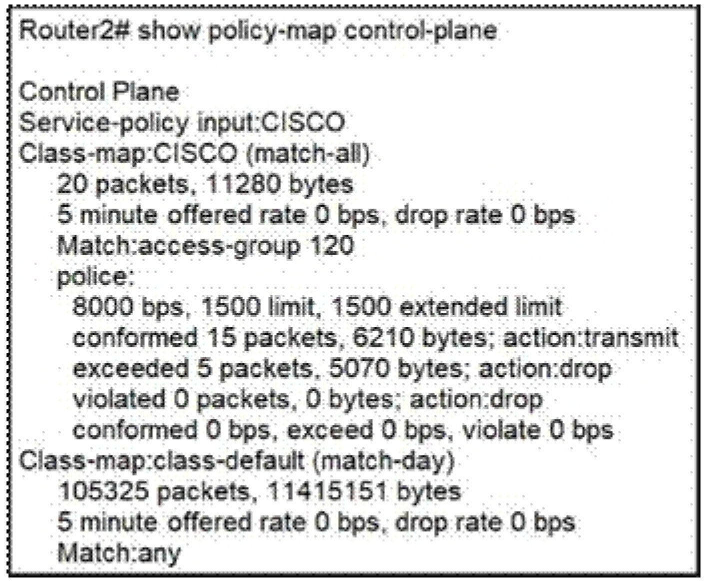
Correct Answer: D
Section:

QUESTION 144
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

Correct Answer: B
Section:

QUESTION 145



```
Router2# show policy-map control-plane

Control Plane
Service-policy input:CISCO
Class-map:CISCO (match-all)
    20 packets, 11280 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match:access-group 120
    police:
      8000 bps, 1500 limit, 1500 extended limit
      conformed 15 packets, 6210 bytes; action:transmit
      exceeded 5 packets, 5070 bytes; action:drop
      violated 0 packets, 0 bytes; action:drop
      conformed 0 bps, exceed 0 bps, violate 0 bps
Class-map:class-default (match-day)
    105325 packets, 11415151 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match:any
```

Refer to the exhibit. An engineer configures CoPP and enters the show command to verify the implementation. What is the result of the configuration?

A. All traffic will be policed based on access-list 120.
B. If traffic exceeds the specified rate, it will be transmitted and remarked.
C. Class-default traffic will be dropped.
D. ICMP will be denied based on this configuration.

Correct Answer: A
Section:

QUESTION 146
What is the function of cisco DNA center in a cisco SD-access deployment?

A. It is responsible for routing decisions inside the fabric
B. It is responsible for the design, management, deployment, provisioning and assurance of the fabric network devices.
C. It possesses information about all endpoints, nodes and external networks related to the fabric
D. It provides integration and automation for all nonfabric nodes and their fabric counterparts.

Correct Answer: B
Section:

QUESTION 147
A network administrator is implementing a routing configuration change and enables routing debugs to track routing behavior during the change. The logging output on the terminal is interrupting the command typing process. Which two actions can the network administrator take to minimize the possibility of typing commands incorrectly? (Choose two.)

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

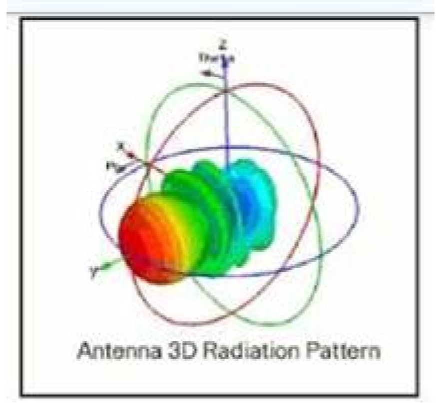
Correct Answer: C, D
Section:

QUESTION 148
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.

Correct Answer: C
Section:

QUESTION 149
Refer to the exhibit.



Which type of antenna does the radiation pattern represent?

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

Correct Answer: A
Section:

QUESTION 150
Which new enhancement was implemented in Wi-Fi 6?

A. Wi-Fi Protected Access 3
B. 4096 Quadrature Amplitude Modulation Mode
C. Channel bonding
D. Uplink and Downlink Orthogonal Frequency Division Multiple Access

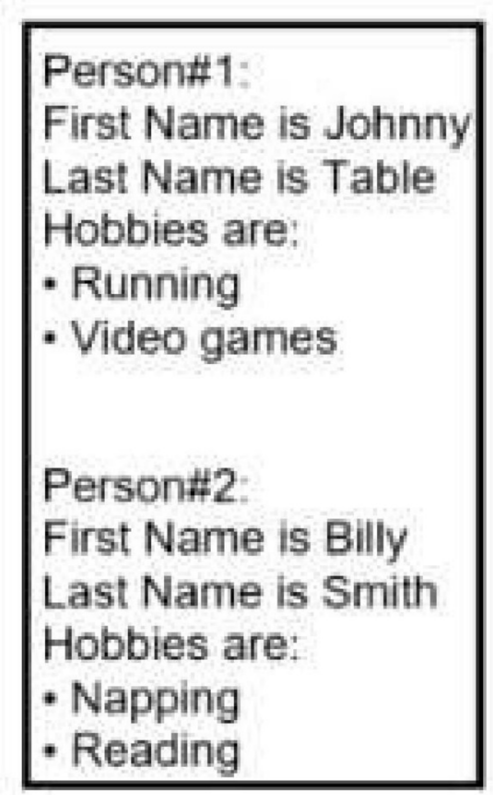
Correct Answer: D
Section:

QUESTION 151
Which cisco DNA center application is responsible for group-based accesss control permissions?

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

Correct Answer: D
Section:

QUESTION 152
Refer to the exhibit.

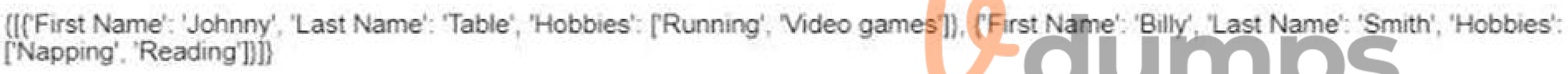


Person#1:
First Name is Johnny
Last Name is Table
Hobbies are:
- Running
- Video games

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

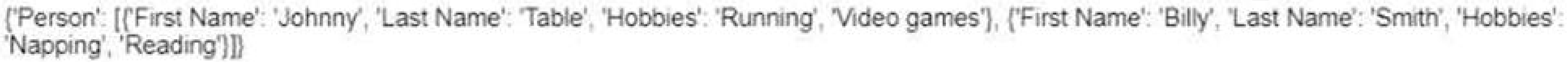
Which JSON syntax is derived from this data?

A.



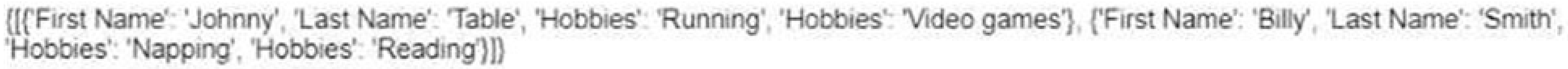
```
{[{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': ['Running', 'Video games']}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies':
['Napping', 'Reading']}]}
```

B.



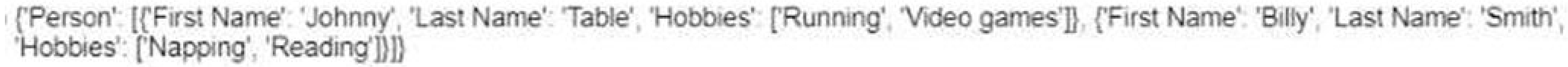
```
{'Person': [{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': 'Running', 'Video games'}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies':
'Napping', 'Reading'}]}
```

C.



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

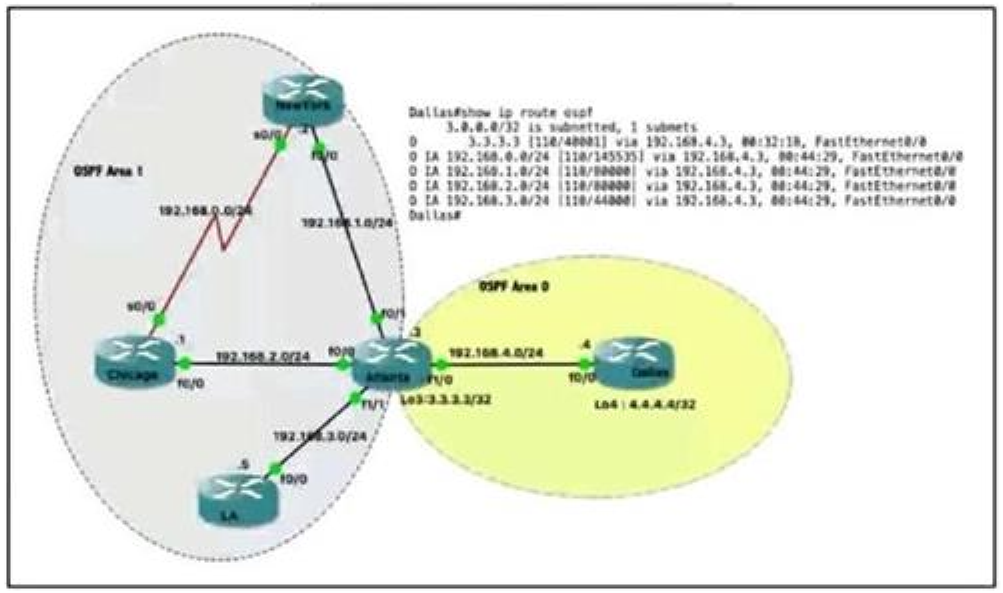
D.



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

Correct Answer: D
Section:

QUESTION 153
Refer to the exhibit.



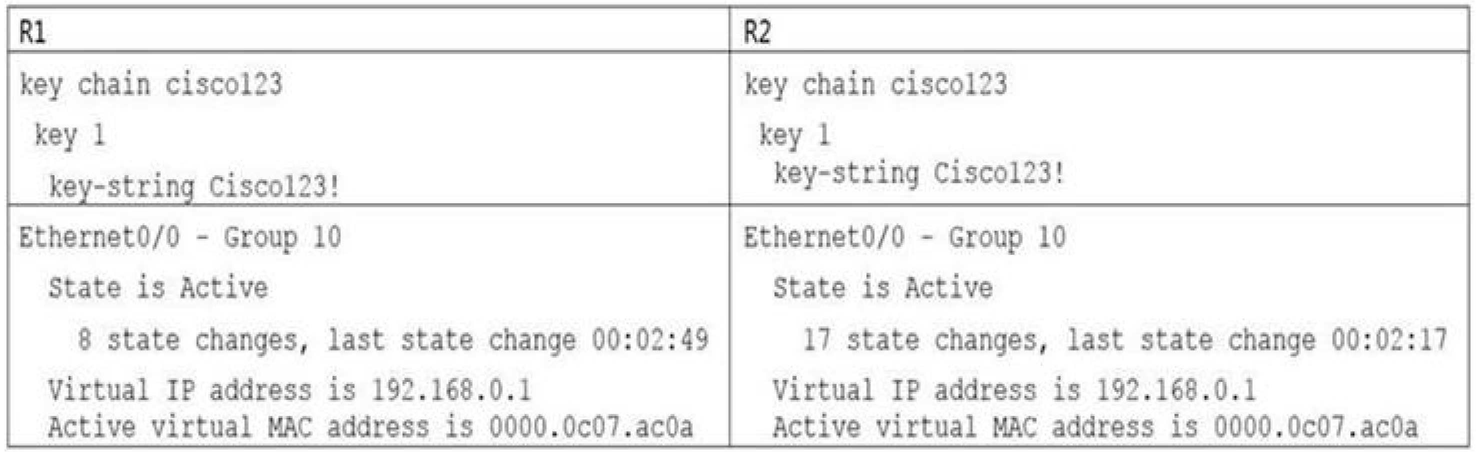
```
Dallas#show ip route ospf
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/40001] via 192.168.4.3, 00:32:18, FastEthernet0/0
O IA 192.168.0.0/24 [110/145535] via 192.168.4.3, 00:44:29, FastEthernet0/0
O IA 192.168.1.0/24 [110/80000] via 192.168.4.3, 00:44:29, FastEthernet0/0
O IA 192.168.2.0/24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

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

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

Correct Answer: C
Section:

QUESTION 154
Refer to the exhibit.



R1	R2
key chain cisco123 key 1 key-string Cisco123!	key chain cisco123 key 1 key-string Cisco123!

Ethernet0/0 - Group 10
  State is Active
   8 state changes, last state change 00:02:49
  Virtual IP address is 192.168.0.1
  Active virtual MAC address is 0000.0c07.ac0a
	Ethernet0/0 - Group 10
	  State is Active
	   17 state changes, last state change 00:02:17
	  Virtual IP address is 192.168.0.1
	  Active virtual MAC address is 0000.0c07.ac0a

An engineer is installing a new pair of routers in a redundant configuration. Which protocol ensures that traffic is not disrupted in the event of a hardware failure?

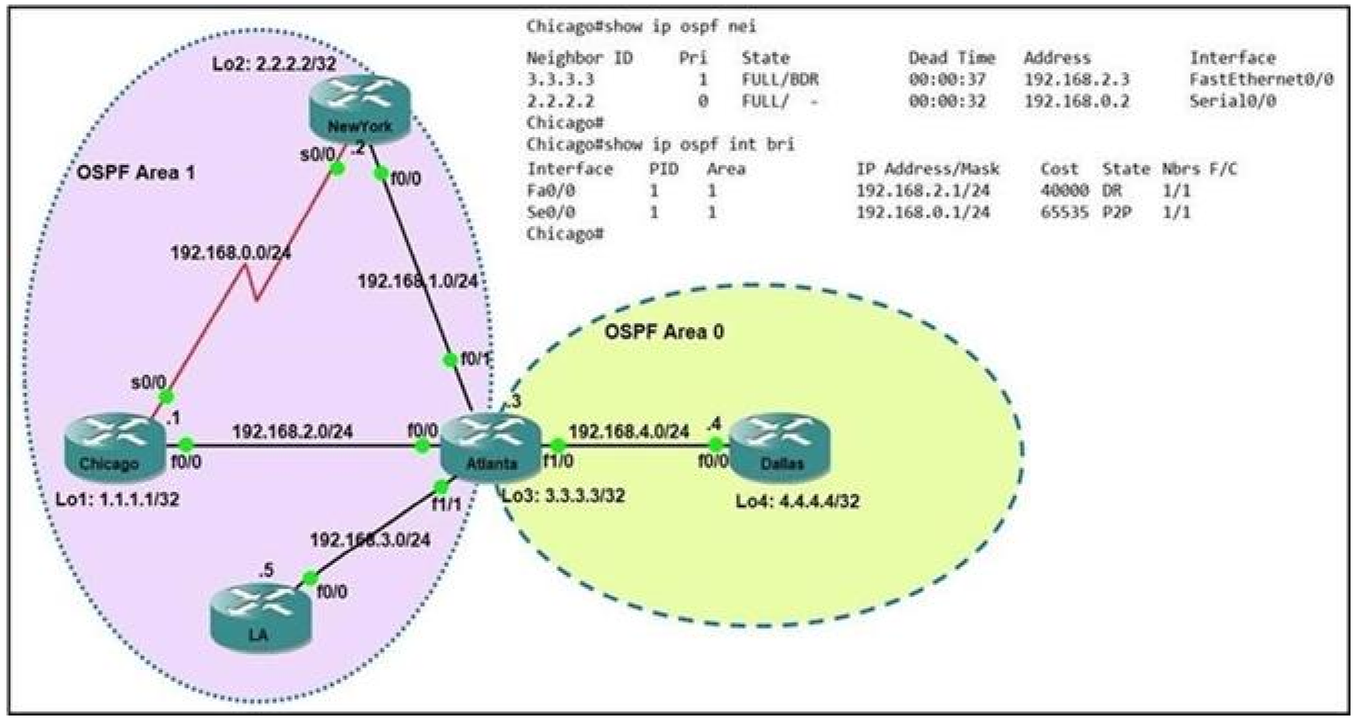
A. HSRPv1
B. GLBP
C. VRRP
D. HSRPv2

Correct Answer: A
Section:
Explanation:

The ?virtual MAC address? is 0000.0c07.acXX (XX is the hexadecimal group number) so it is using HSRPv1.
Note: HSRP Version 2 uses a new MAC address which ranges from 0000.0C9F.F000 to 0000.0C9F.FFFF.

QUESTION 155

Refer the exhibit.



```
Chicago#show ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           1   FULL/BDR        00:00:37    192.168.2.3     FastEthernet0/0
2.2.2.2           0   FULL/  -        00:00:32    192.168.0.2     Serial0/0
Chicago#
Chicago#show ip ospf int bri
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Fa0/0        1     1               192.168.2.1/24     40000 DR    1/1
Se0/0        1     1               192.168.0.1/24     65535 P2P   1/1
Chicago#
```

Which router is the designated router on the segment 192.168.0.0/24?

A. This segment has no designated router because it is a nonbroadcast network type.

B. This segment has no designated router because it is a p2p network type.

C. Router Chicago because it has a lower router ID

D. Router NewYork because it has a higher router ID

Correct Answer: B
Section:

QUESTION 156

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

A. R1#sh run | include aaa
aaa new-model
aaa authentication login VTY group tacacs+ none
aaa session-id common
R1#sh run | section vty
line vty 0 4
password 7 0202039485748
R1#sh run | include username
R1#

B. R1#sh run | include aaa
aaa new-model
aaa authentication login telnet group tacacs+ none

```
aaa session-id common
R1#sh run | section vty
line vty 0 4
R1#sh run | include username
R1#
```

C.
```
R1#sh run | include aaa
aaa new-model
aaa authentication login default group tacacs+ none
aaa session-id common
R1#sh run | section vty
line vty 0 4
password 7 0202039485748
```

D.
```
R1#sh run | include aaa
aaa new-model
aaa authentication login default group tacacs+
aaa session-id common
R1#sh run | section vty
line vty 0 4
transport input none
R1#
```

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

QUESTION 157
Which technology is used as the basis for the cisco sd-access data plane?

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

Correct Answer: C
Section:
Explanation:
A virtual network identifier (VNI) is a value that identifies a specific virtual network in the data plane.

QUESTION 158
What is YANG used for?

A. scraping data via CLI
B. processing SNMP read-only polls

C. describing data models
D. providing a transport for network configuration data between client and server

Correct Answer: C
Section:

QUESTION 159
Which method does Cisco DNA Center use to allow management of non-Cisco devices through southbound protocols?

A. It creates device packs through the use of an SDK
B. It uses an API call to interrogate the devices and register the returned data.
C. It obtains MIBs from each vendor that details the APIs available.
D. It imports available APIs for the non-Cisco device in a CSV format.

Correct Answer: A
Section:
Explanation:
Cisco DNA Center allows customers to manage their non-Cisco devices through the use of a Software Development Kit (SDK) that can be used to create Device Packages for third-party devices.
Reference: https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platformoverview/multivendor-support-southbound

QUESTION 160
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

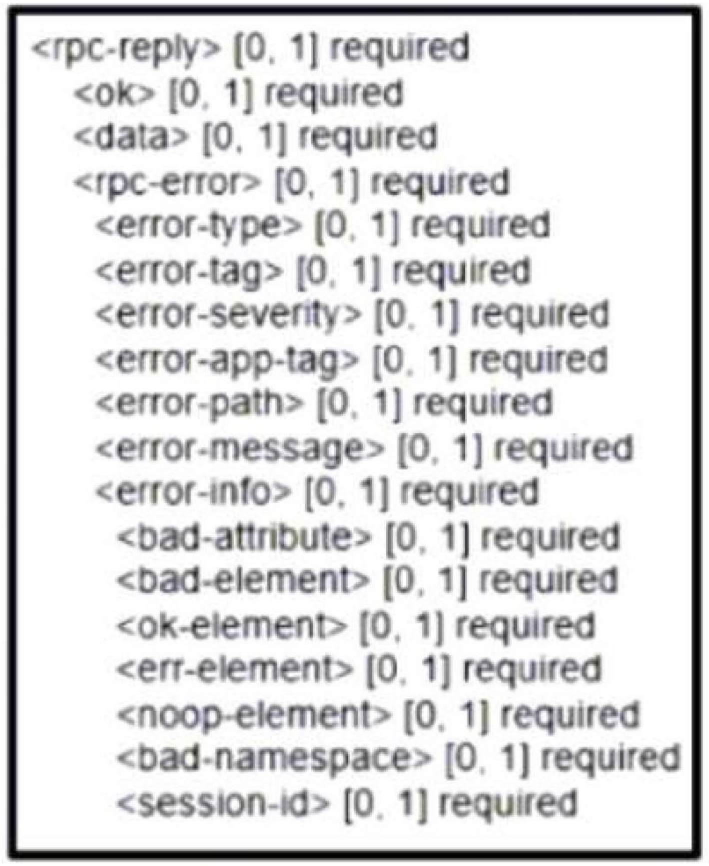
Correct Answer: B
Section:

QUESTION 161
What are two considerations when using SSO as a network redundancy feature? (Choose two)

A. both supervisors must be configured separately
B. the multicast state is preserved during switchover
C. must be combined with NSF to support uninterrupted Layer 2 operations
D. must be combined with NSF to support uninterrupted Layer 3 operations
E. requires synchronization between supervisors in order to guarantee continuous connectivity

Correct Answer: D, E
Section:
Explanation:
Cisco IOS Nonstop Forwarding(NSF) always runs with stateful switchover (SSO) and provides redundancy for Layer 3 traffic.
Reference:
https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/consolidated_guide/b_consolidated_3850_3se_cg_chapter_01101110.pdf

QUESTION 162



```
<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

Correct Answer: D
Section:

QUESTION 163

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

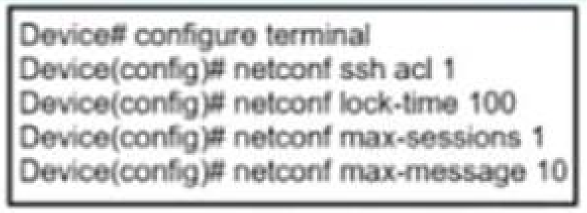
B. logging origin-id 10.10.10.1

C. logging host 10.10.10.1 transport udp port 1023

D. logging host 10.10.10.1 transport udp port 1024

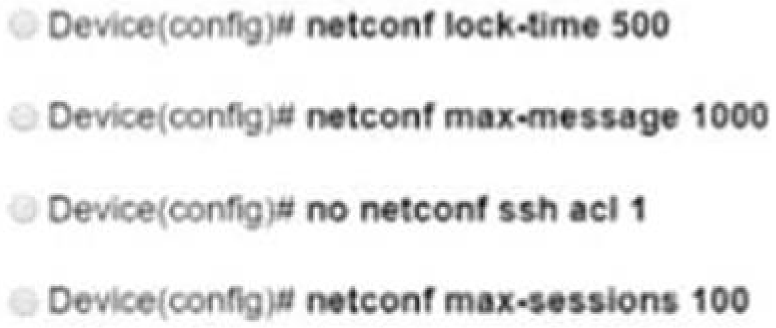
Correct Answer: A
Section:

QUESTION 164



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

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



○ Device(config)# **netconf lock-time 500**

○ Device(config)# **netconf max-message 1000**

○ Device(config)# **no netconf ssh acl 1**

○ Device(config)# **netconf max-sessions 100**

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

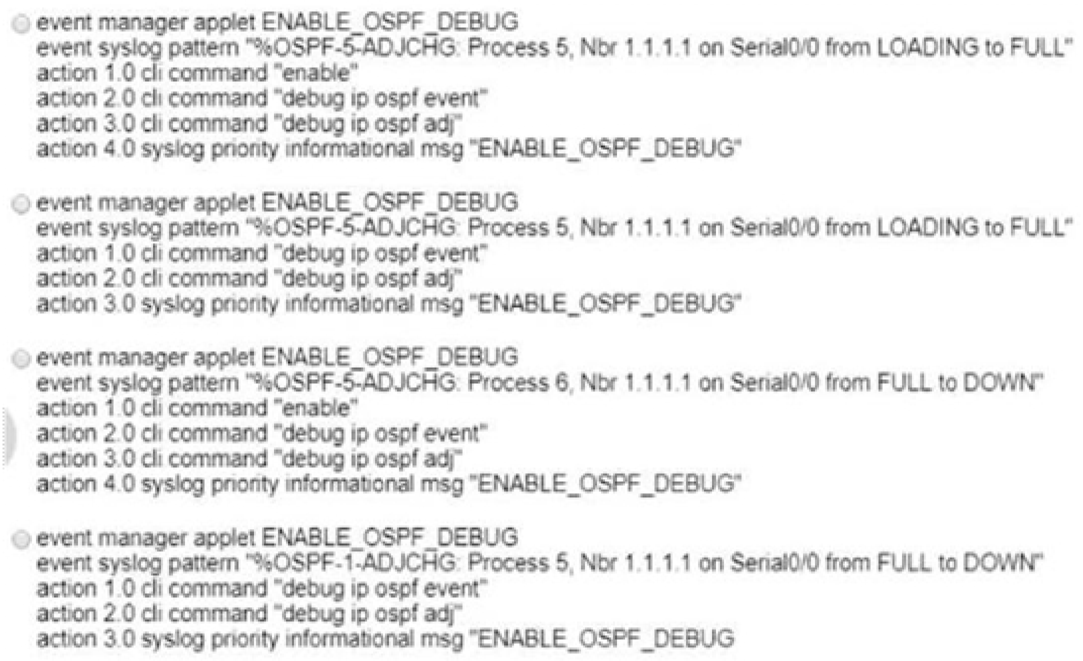
Correct Answer: C
Section:

QUESTION 165
An engineer is configuring a new SSID to present users with a splash page for authentication. Which WLAN Layer 3 setting must be configured to provide this functionally?

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

Correct Answer: D
Section:

QUESTION 166
An engineer must create an EEM script to enable OSPF debugging in the event the OSPF neighborship goes down. Which script must the engineer apply?

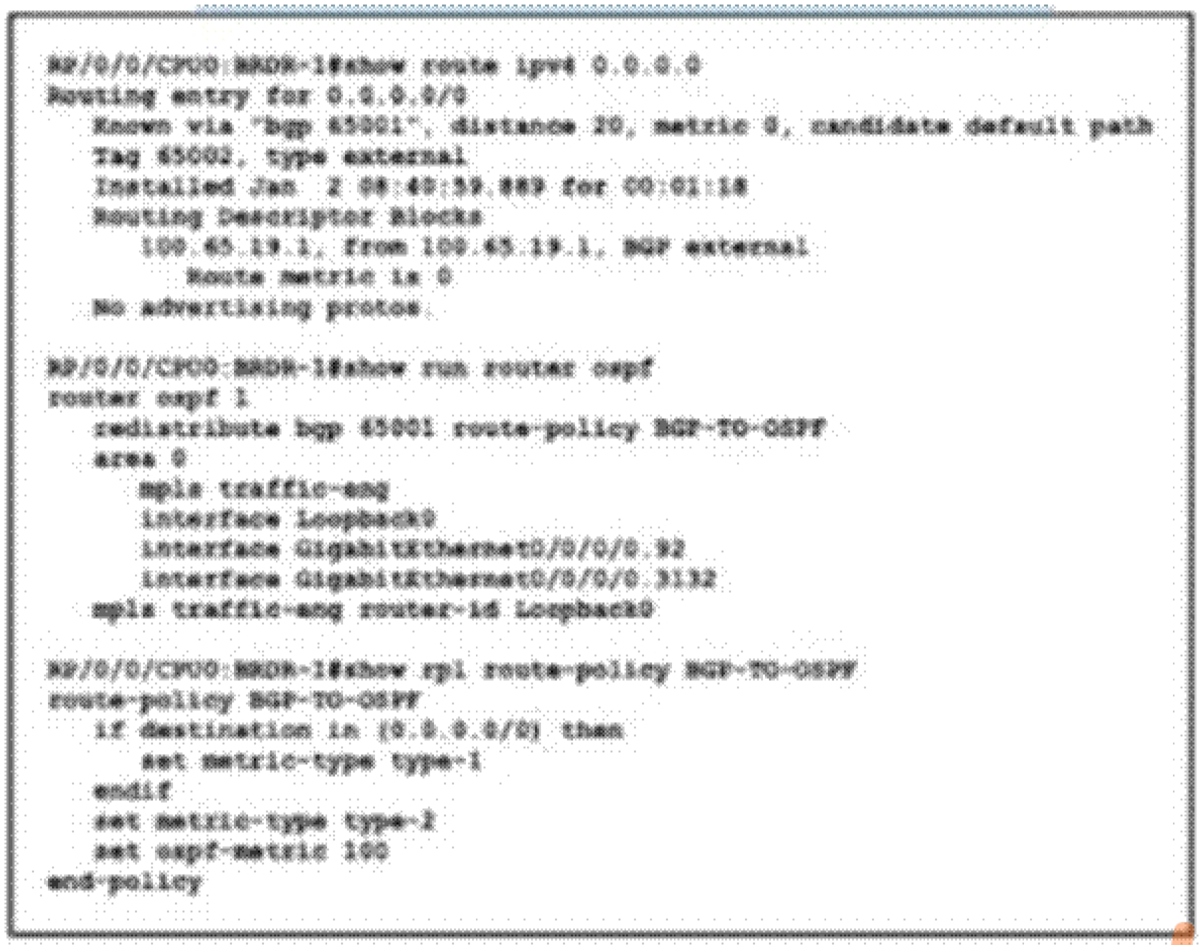


```
○ event manager applet ENABLE_OSPF_DEBUG
  event syslog pattern "%OSPF-5-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from LOADING to FULL"
  action 1.0 cli command "enable"
  action 2.0 cli command "debug ip ospf event"
  action 3.0 cli command "debug ip ospf adj"
  action 4.0 syslog priority informational msg "ENABLE_OSPF_DEBUG"

○ event manager applet ENABLE_OSPF_DEBUG
  event syslog pattern "%OSPF-5-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from LOADING to FULL"
  action 1.0 cli command "debug ip ospf event"
  action 2.0 cli command "debug ip ospf adj"
  action 3.0 syslog priority informational msg "ENABLE_OSPF_DEBUG"

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

○ event manager applet ENABLE_OSPF_DEBUG
  event syslog pattern "%OSPF-1-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from FULL to DOWN"
  action 1.0 cli command "debug ip ospf event"
  action 2.0 cli command "debug ip ospf adj"
  action 3.0 syslog priority informational msg "ENABLE_OSPF_DEBUG
```

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

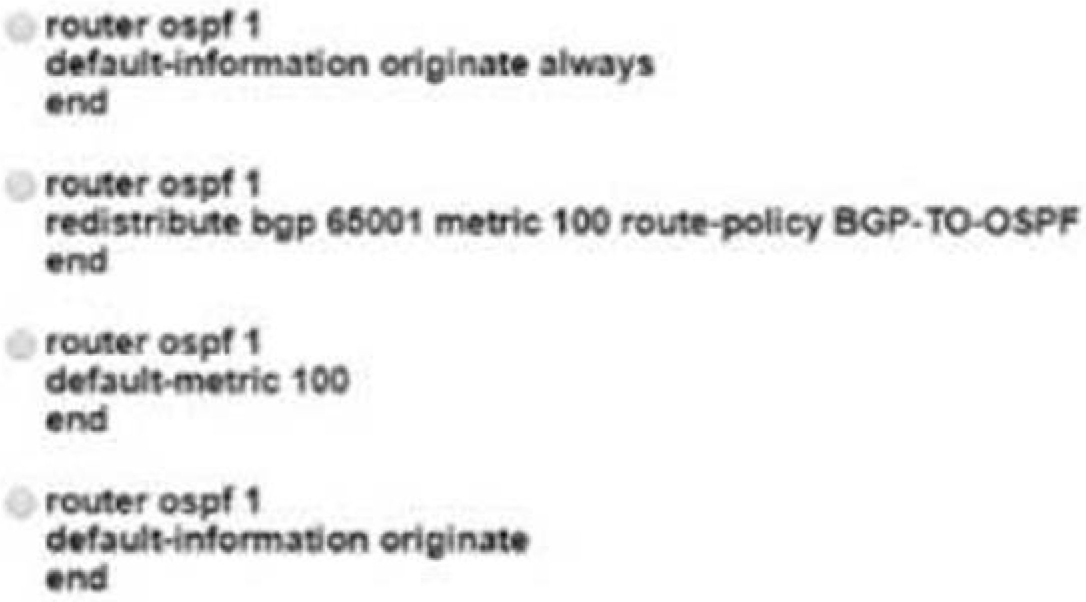
Correct Answer: C
Section:

QUESTION 167



```
RP/0/0/CPU0:BRDR-1#show route ipv4 0.0.0.0
Routing entry for 0.0.0.0/0
   Known via "bgp 65001", distance 20, metric 0, candidate default path
   Tag 65002, type external
   Installed Jan  2 08:40:59.889 for 00:01:18
   Routing Descriptor Blocks
      100.65.19.1, from 100.65.19.1, BGP external
         Route metric is 0
   No advertising protos.

RP/0/0/CPU0:BRDR-1#show run router ospf
router ospf 1
   redistribute bgp 65001 route-policy BGP-TO-OSPF
   area 0
      mpls traffic-eng
      interface Loopback0
      interface GigabitEthernet0/0/0/0.92
      interface GigabitEthernet0/0/0/0.3132
   mpls traffic-eng router-id Loopback0

RP/0/0/CPU0:BRDR-1#show rpl route-policy BGP-TO-OSPF
route-policy BGP-TO-OSPF
   if destination in (0.0.0.0/0) then
      set metric-type type-1
   endif
   set metric-type type-2
   set ospf-metric 100
end-policy
```

Refer to the exhibit. Router BRDR-1 is configured to receive the 0.0.0.0/0 and 172.17.1.0/24 network via BGP and advertise them into OSPF are 0. An engineer has noticed that the OSPF domain is receiving only the 172.17.1.0/24 route and default route 0.0.0.0/0 is still missing. Which configurating must engineer apply to resolve the problem?



```
○ router ospf 1
  default-information originate always
  end

○ router ospf 1
  redistribute bgp 65001 metric 100 route-policy BGP-TO-OSPF
  end

○ router ospf 1
  default-metric 100
  end

○ router ospf 1
  default-information originate
  end
```

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

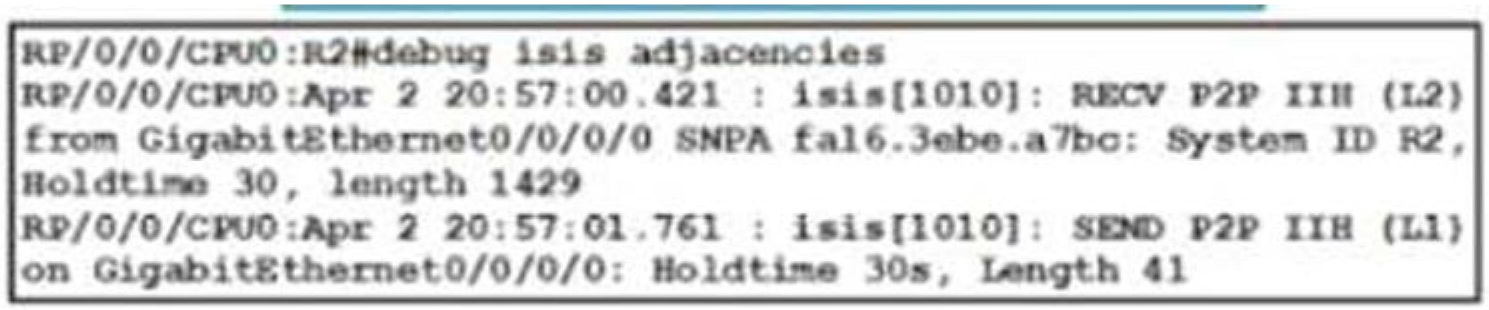
Correct Answer: D
Section:

QUESTION 168
AN engineer is implementing a route map to support redistribution within BGP. The route map must 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

Correct Answer: D
Section:

QUESTION 169



```
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.

Correct Answer: C
Section:

QUESTION 170
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.

Correct Answer: C
Section:

QUESTION 171
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.

Correct Answer: B
Section:

QUESTION 172
What occurs when a high bandwidth multicast stream is sent over an MVPN using Cisco hardware?

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

Correct Answer: D
Section:

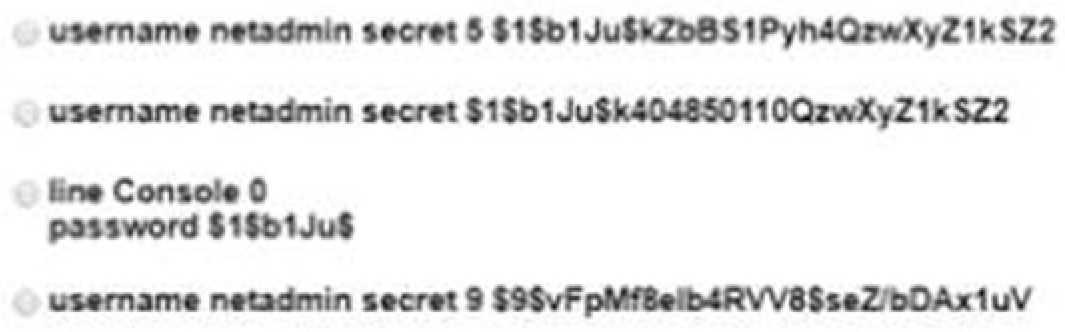
QUESTION 173
Which protocol is used to encrypt control plane traffic between SD-WAN controllers and SD-WAN endpoints?

A. DTLS
B. IPsec

C. PGP
D. HTTPS

Correct Answer: A
Section:
Explanation:
DTLS protocol is used to encrypt control plane traffic between vSmart (controllers) and other SDWAN endpoints.

QUESTION 174
An engineer must configure the strongest password authentication to locally authenticate on a router. Which configuration must be used?



○ username netadmin secret 5 $1$b1Ju$kZbBS1Pyh4QzwXyZ1kSZ2

○ username netadmin secret $1$b1Ju$k404850110QzwXyZ1kSZ2

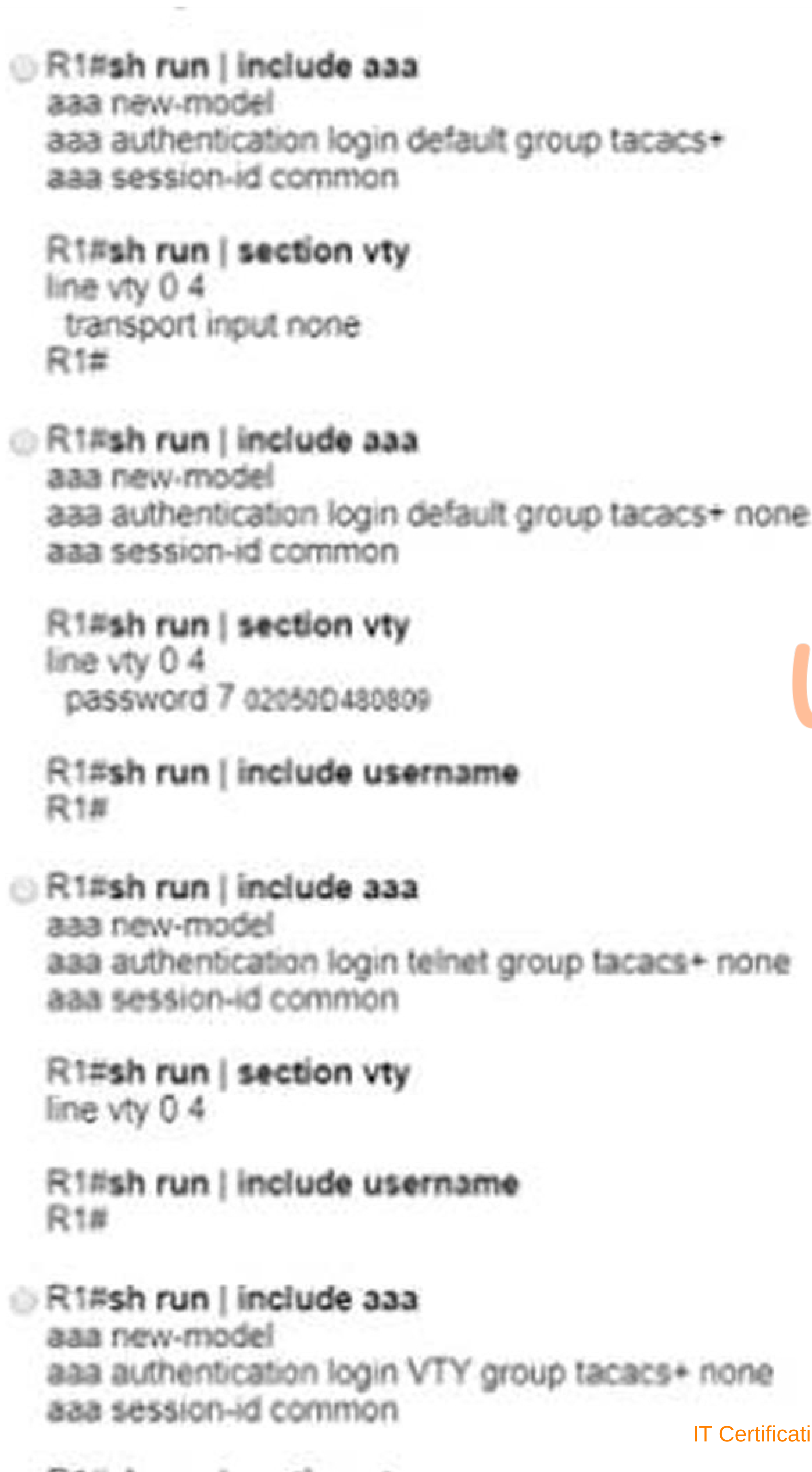
○ line Console 0
password $1$b1Ju$

○ username netadmin secret 9 $9$vFpMf8elb4RVV8$seZ/bDAx1uV

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

Correct Answer: D
Section:
Explanation:
Scrypt is safer than MD5, so answer A is wrong and answer D is correct R1(config)#username user secret ?
0 Specifies an UNENCRYPTED secret will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
<0-9> Encryption types not explicitly specified
LINE The UNENCRYPTED (cleartext) user secret
LINE The UNENCRYPTED (cleartext) user secret
+ The enable password command should no longer be used. Use enable secret instead. username joeblow password mypass command should no longer be used. Use username joeblow secret mypass instead.
+ Type 4 Passwords should never be used!
+ Use Type 6, Type 8 and Type 9 wherever possible.
+ Type 0, Type 5 and Type 7 should be migrated to other stronger methods.
Reference: https://community.cisco.com/t5/networking-documents/understanding-the-differencesbetween-the-cisco-password-secret/ta-p/3163238

QUESTION 175
The login method is configured on the VTY lines of a router with these parameters The first method for authentication it TACACS If TACACS is unavailable login is allowed without any provided credentials Which configuration accomplishes this task?



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

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

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

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

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

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

R1#sh run | section vty
line vty 0 4

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

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

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

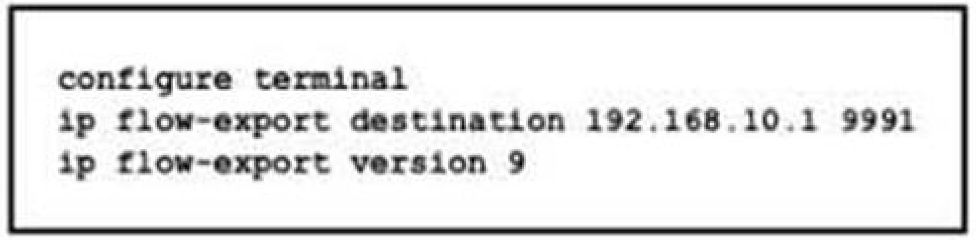
Correct Answer: B
Section:

QUESTION 176
Which network devices secure API platform?

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

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

QUESTION 177
Refer to the exhibit.



```
configure terminal
ip flow-export destination 192.168.10.1 9991
ip flow-export version 9
```

What is required to configure a second export destination for IP address 192.168.10.1?

A. Specify a VRF.
B. Specify a different UDP port.
C. Specify a different flow ID
D. Configure a version 5 flow-export to the same destination.
E. Specify a different TCP port.

Correct Answer: B
Section:
Explanation:
To configure multiple NetFlow export destinations to a router, use the following commands in global configuration mode:
Step 1: Router(config)# ip flow-export destination ip-address udp-port Step 2: Router(config)# ip flow-export destination ip-address udp-port The following example enables the exporting of information in NetFlow cache entries: ip flow-export destination 10.42.42.1 9991 ip flow-export destination 10.0.101.254 1999

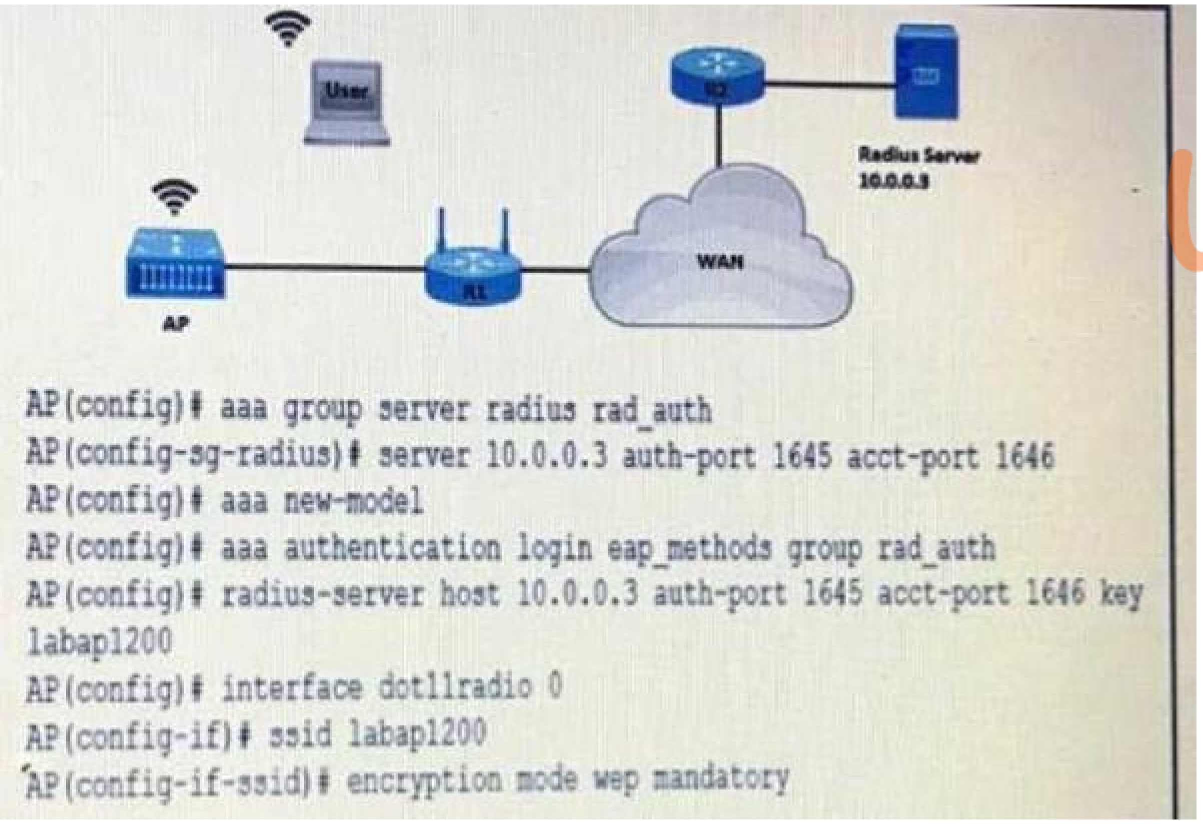
Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/12s_mdnf.html

QUESTION 178
Which threat defence mechanism, when deployed at the network perimeter, protects against zeroday attacks?

A. intrusion prevention
B. stateful inspection
C. sandbox
D. SSL decryption

Correct Answer: C
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheetc78-733182.html"File analysis and sandboxing: Secure Malware Analytics' highly secure environment helps youexecute, analyze, and test malware behavior to discover previously unknown ZERO-DAY threats. Theintegration of Secure Malware Analytics' sandboxing technology into Malware Defense results inmore dynamic analysis checked against a larger set of behavioral indicators. "

QUESTION 179
Refer to the exhibit.



```
AP(config)# aaa group server radius rad_auth
AP(config-sg-radius)# server 10.0.0.3 auth-port 1645 acct-port 1646
AP(config)# aaa new-model
AP(config)# aaa authentication login eap_methods group rad_auth
AP(config)# radius-server host 10.0.0.3 auth-port 1645 acct-port 1646 key
labap1200
AP(config)# interface dot11radio 0
AP(config-if)# ssid labap1200
AP(config-if-ssid)# encryption mode wep mandatory
```

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

A. AP(config-if-ssid)# authentication open wep wep_methods
B. AP(config-if-ssid)# authentication dynamic wep wep_methods
C. AP(config-if-ssid)# authentication dynamic open wep_dynamic
D. AP(config-if-ssid)# authentication open eap eap_methods

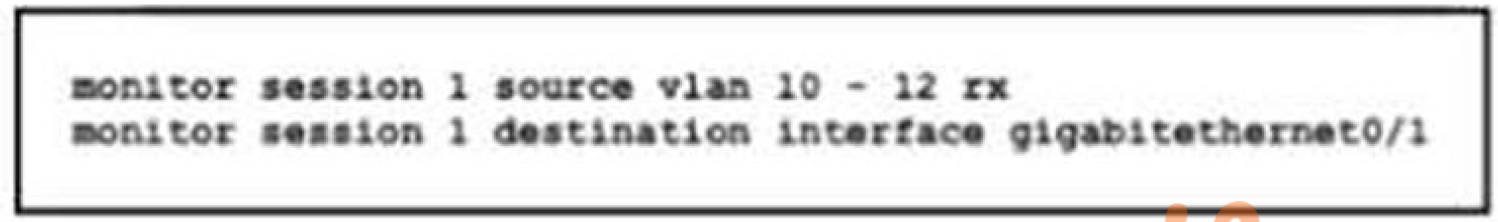
Correct Answer: D
Section:

QUESTION 180
Which OSPF networks types are compatible and allow communication through the two peering devices?

A. broadcast to nonbroadcast
B. point-to-multipoint to nonbroadcast
C. broadcast to point-to-point
D. point-to-multipoint to broadcast

Correct Answer: A
Section:
Explanation:
The following different OSPF types are compatible with each other:
+ Broadcast and Non-Broadcast (adjust hello/dead timers)
+ Point-to-Point and Point-to-Multipoint (adjust hello/dead timers)
Broadcast and Non-Broadcast networks elect DR/BDR so they are compatible. Point-topoint/ multipoint do not elect DR/BDR so they are compatible.

QUESTION 181
Refer to the exhibit.



```
monitor session 1 source vlan 10 - 12 rx
monitor session 1 destination interface gigabitethernet0/1
```

An engineer must configure a SPAN session. What is the effect of the configuration?

A. Traffic sent on VLANs 10, 11, and 12 is copied and sent to interface g0/1.
B. Traffic sent on VLANs 10 and 12 only is copied and sent to interface g0/1.
C. Traffic received on VLANs 10, 11, and 12 is copied and sent to Interface g0/1.
D. Traffic received on VLANs 10 and 12 only is copied and sent to interface g0/1.

Correct Answer: C
Section:

QUESTION 182
An engineer is configuring a GRE tunnel interface in the default mode. The engineer has assigned an IPv4 address on the tunnel and sourced the tunnel from an Ethernet interface. Which option also is required on the tunnel interface before it is operational?

A. (config-if)#tunnel destination <ip address>
B. (config-if)#keepalive <seconds retries>
C. (config-if)#ip mtu <value>
D. (config-if)#ip tcp adjust-mss <value>

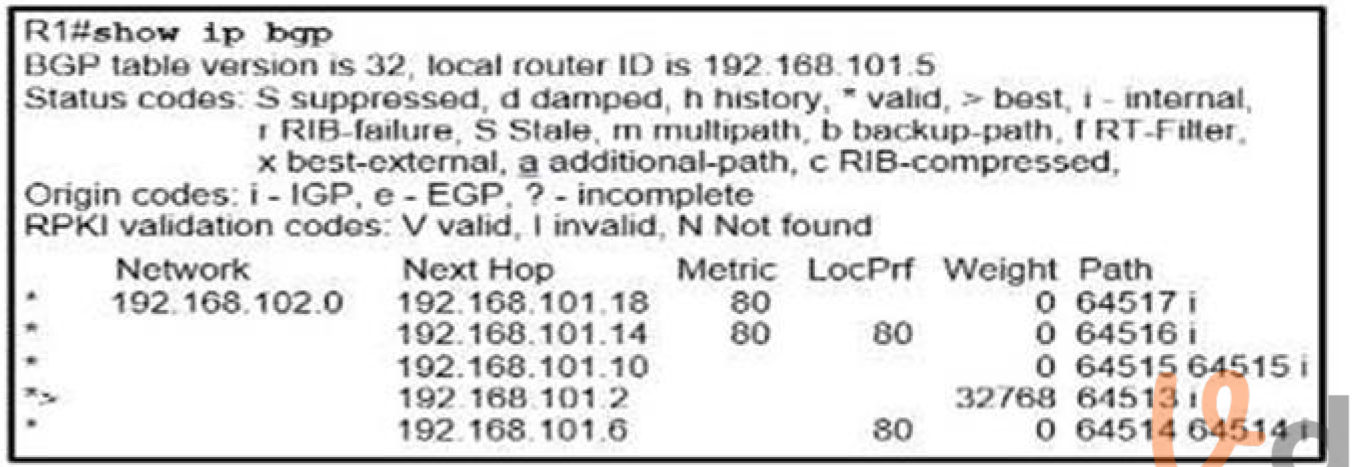
Correct Answer: A
Section:
Explanation:
A GRE interface definition includes: + An IPv4 address on the tunnel + A tunnel source + A tunnel destination Below is an example of how to configure a basic GRE tunnel: interface Tunnel 0 ip address 10.10.10.1 255.255.255.0 tunnel source fa0/0 tunnel destination 172.16.0.2 In this case the “IPv4 address on the tunnel” is 10.10.10.1/24 and “sourced the tunnel from an Ethernet interface” is the command “tunnel source fa0/0”. Therefore it only needs a tunnel destination, which is 172.16.0.2.Note: A multiple GRE (mGRE) interface does not require a tunnel destination address.

QUESTION 183
Which solution do laaS service providers use to extend a Layer 2 segment across a Layer 3 network?

A. VLAN
B. VTEP
C. VXLAN
D. VRF

Correct Answer: C
Section:

QUESTION 184
Refer to the exhibit.



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

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

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

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

Correct Answer: A
Section:
Explanation:
The '>' shown in the output above indicates that the path with a next hop of 192.168.101.2 is the current best path.
Path Selection Attributes: Weight > Local Preference > Originate > AS Path > Origin > MED > External > IGP Cost > eBGP Peering > Router ID BGP prefers the path with highest weight but the weights here are all 0 (which indicate all routes that are not originated by the local router) so we need to check the Local Preference. Answer '192.168.101.18' path without LOCAL_PREF (LocPrf column) means it has the default value of 100.
Therefore we can find the two next best paths with the next hop of 192.168.101.18 and 192.168.101.10.
We have to move to the next path selection attribute: Originate. BGP prefers the path that the local router originated (which is indicated with the "next hop 0.0.0.0"). But none of the two best paths is self-originated.
The AS Path of the next hop 192.168.101.18 is shorter than the AS Path of the next hop 192.168.101.10 then the next hop 192.168.101.18 will be chosen as the next best path.

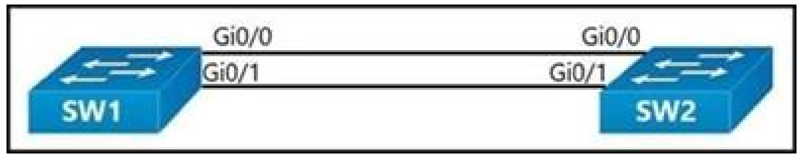
QUESTION 185
What Is a Type 2 hypervisor?

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

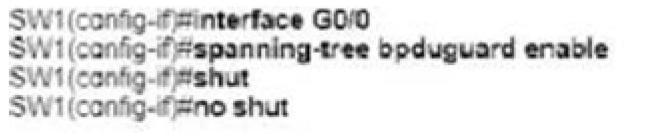
Correct Answer: A
Section:

QUESTION 186
Refer to the exhibit.



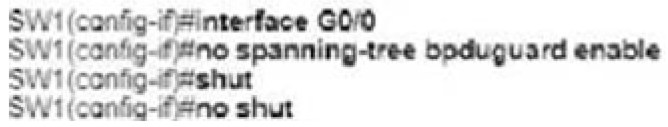
An engineer reconfigures the pot-channel between SW1 and SW2 from an access port to a trunk and immediately notices this error in SW1's log.
Which command set resolves this error?

A.



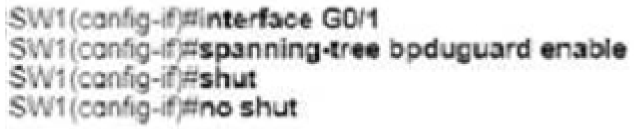
```
SW1(config-if)#interface G0/0
SW1(config-if)#spanning-tree bpduguard enable
SW1(config-if)#shut
SW1(config-if)#no shut
```

B.



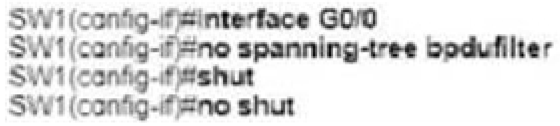
```
SW1(config-if)#interface G0/0
SW1(config-if)#no spanning-tree bpduguard enable
SW1(config-if)#shut
SW1(config-if)#no shut
```

C.



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

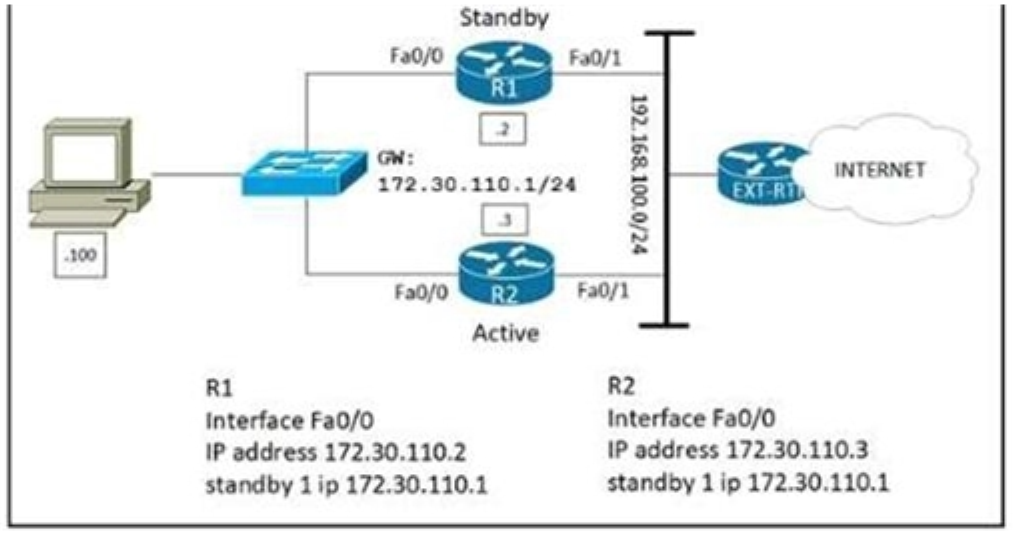
D.



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

Correct Answer: B
Section:

QUESTION 187
Refer to the exhibit.

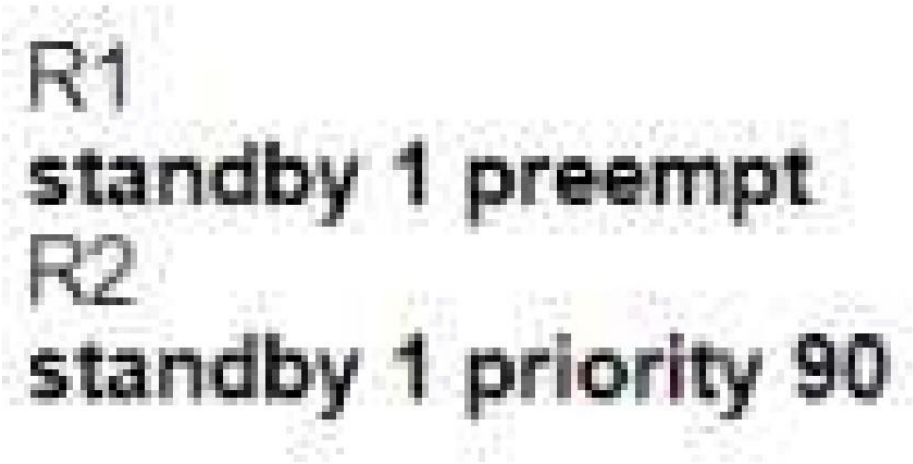


```
R1
Interface Fa0/0
IP address 172.30.110.2
standby 1 ip 172.30.110.1
```

```
R2
Interface Fa0/0
IP address 172.30.110.3
standby 1 ip 172.30.110.1
```

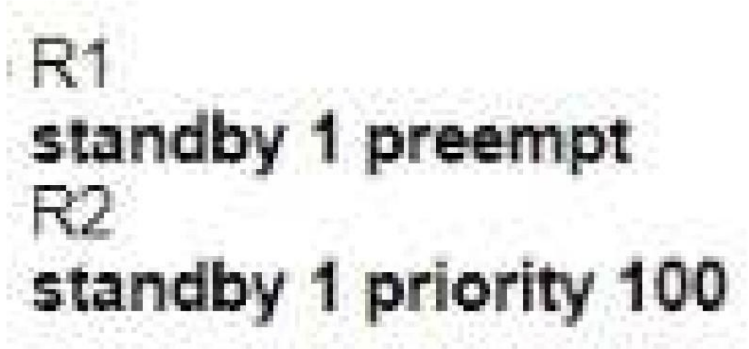
Which configuration change ensures that R1 is the active gateway whenever it is in a functional state for the 172.30.110.0724 network?

A.



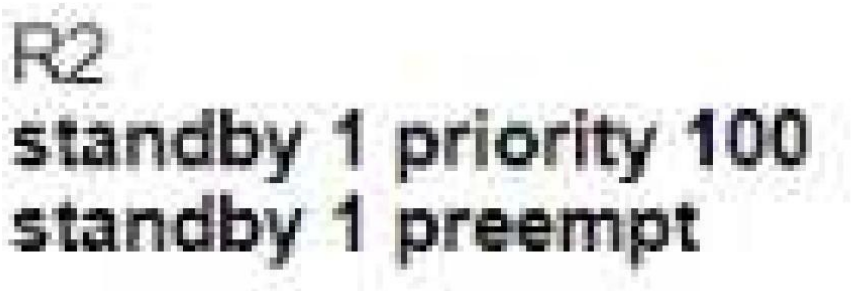
```
R1
standby 1 preempt
R2
standby 1 priority 90
```

B.



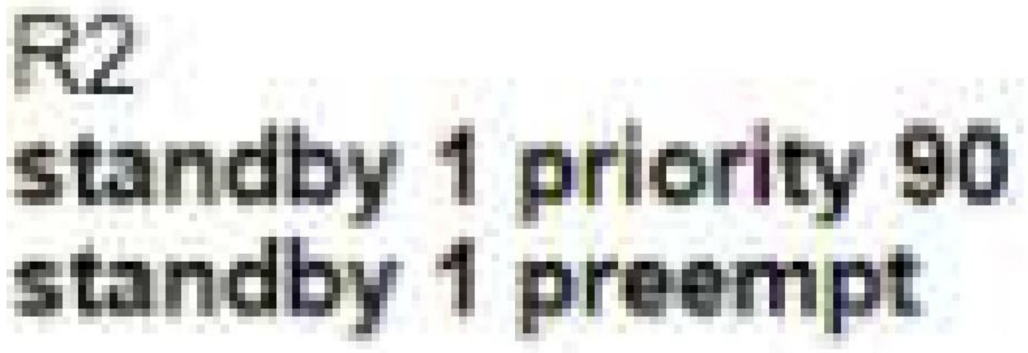
```
R1
standby 1 preempt
R2
standby 1 priority 100
```

C.



```
R2
standby 1 priority 100
standby 1 preempt
```

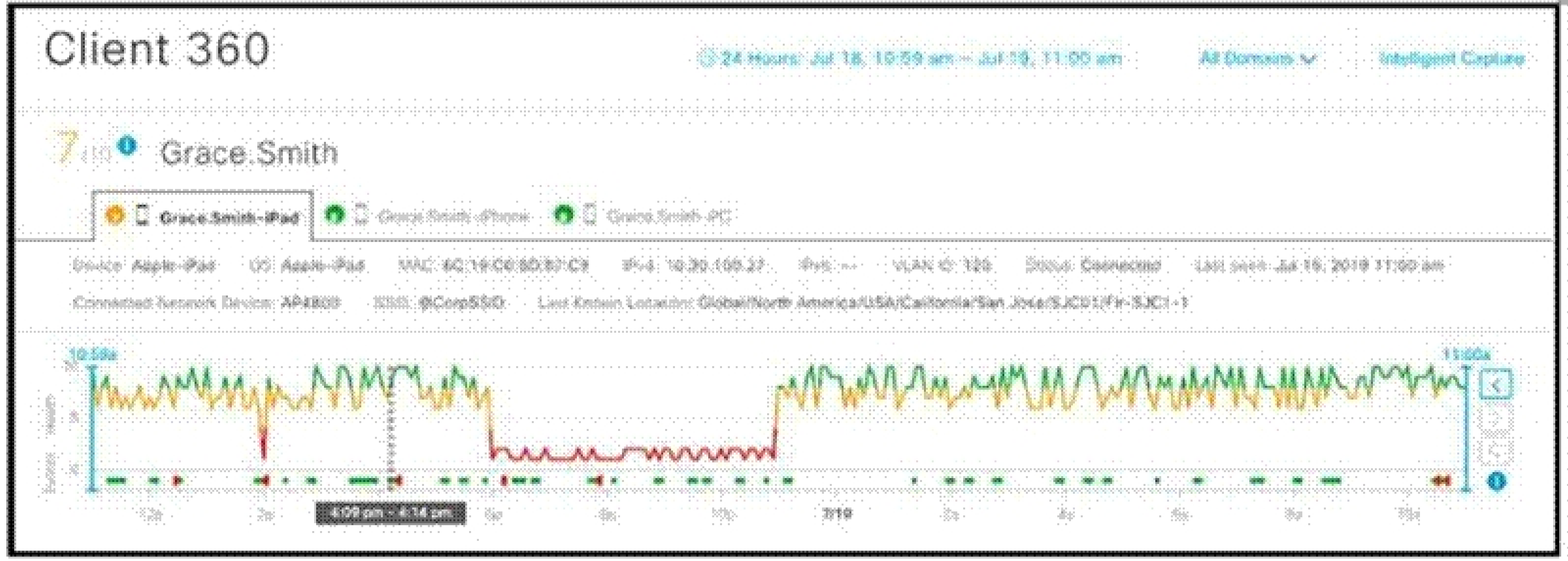
D.



```
R2
standby 1 priority 90
standby 1 preempt
```

Correct Answer: A
Section:

QUESTION 188
Refer to the exhibit.



Client 360

24 Hours: Jul 18, 10:59 am – Jul 19, 11:00 am   All Domains   Intelligent Capture

7 /10 Grace.Smith

Grace.Smith-iPad | Grace.Smith-iPhone | Grace.Smith-PC

Device: Apple-iPad   OS: Apple-iPad   MAC: 6C:19:C0:5D:87:C9   IPv4: 10.30.100.27   IPv6: --   VLAN ID: 120   Status: Connected   Last seen: Jul 19, 2019 11:00 am

Connected Network Device: AP4800   SSID: @CorpSSID   Last Known Location: Global/North America/USA/California/San Jose/SJC01/Flr-SJC1-1

Cisco DNA Center has obtained the username of the client and the multiple devices that the client is using on the network. How is Cisco DNA Center getting these context details?

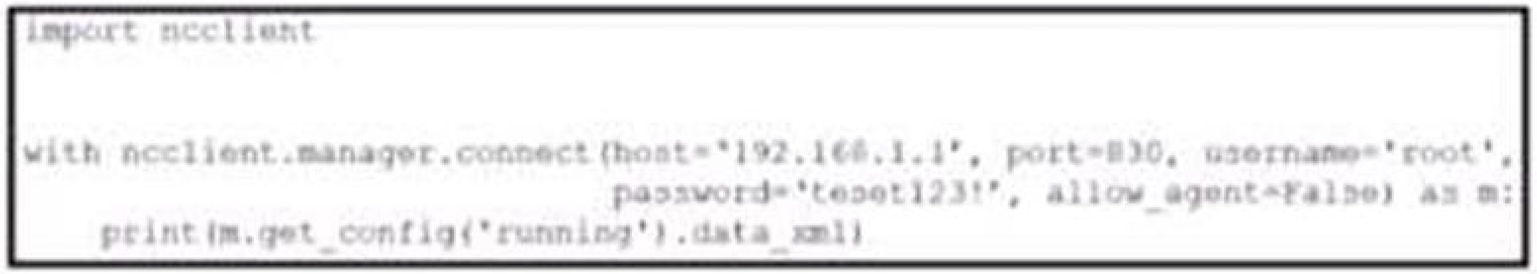
A. The administrator had to assign the username to the IP address manually in the user database tool on Cisco DNA Center.
B. Those details are provided to Cisco DNA Center by the Identity Services Engine
C. Cisco DNA Center pulled those details directly from the edge node where the user connected.
D. User entered those details in the Assurance app available on iOS and Android devices

Correct Answer: A

Section:

QUESTION 189

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

Correct Answer: D

Section:

QUESTION 190

What is the role of the RP in PIM sparse mode?

A. The RP responds to the PIM join messages with the source of requested multicast group

B. The RP maintains default aging timeouts for all multicast streams requested by the receivers.

C. The RP acts as a control-plane node and does not receive or forward multicast packets.

D. The RP is the multicast that is the root of the PIM-SM shared multicast distribution tree.

Correct Answer: D
Section:
Explanation:
Multicast Distribution Shared Tree - Unlike source trees that have their root at the source, shared trees use a single common root placed at some chosen point in the network. This shared root is called a rendezvous point (RP).
Source:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-5/configuration_guide/ip_mcast_rtng/b_165_ip_mcast_rtng_9300_cg/b_165_ip_mcast_rtng_9300_9500_cg_chapter_0100.html
https://netcraftsmen.com/pim-sparse-mode/

QUESTION 191
Which two actions, when applied in the LAN network segment, will facilitate Layer 3 CAPWAP discovery for lightweight AP? (Choose two.)

A. Utilize DHCP option 17.

B. Configure WLC IP address on LAN switch.

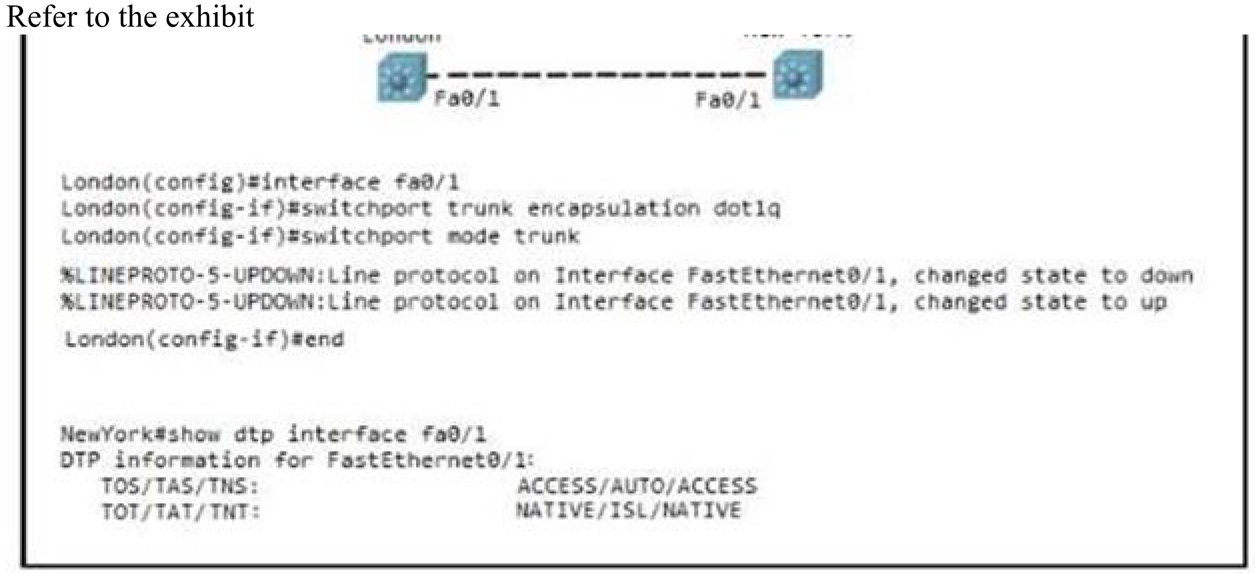
C. Utilize DHCP option 43.

D. Configure an ip helper-address on the router interface

E. Enable port security on the switch port

Correct Answer: C, E
Section:

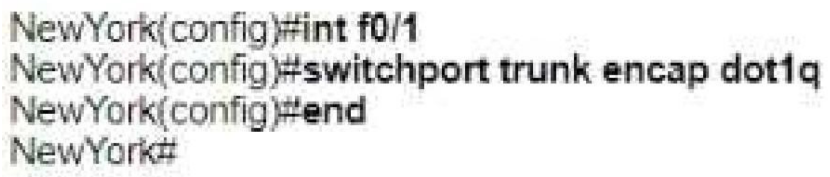
QUESTION 192
Refer to the exhibit



```
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
```

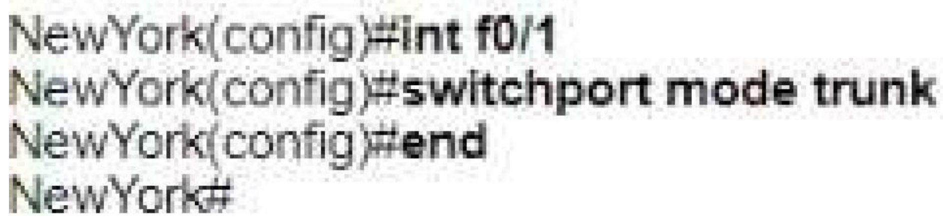
Communication between London and New York is down Which to resolve this issue?

A.



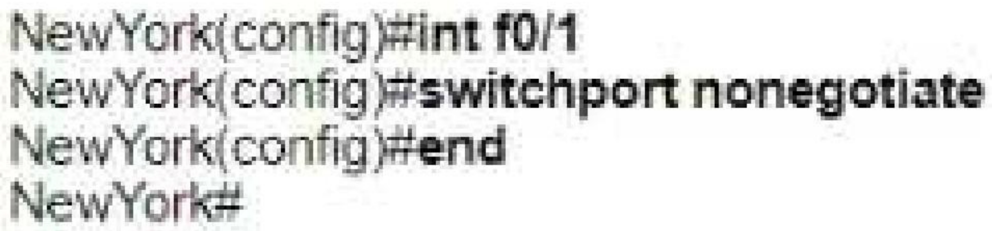
```
NewYork(config)#int f0/1
NewYork(config)#switchport trunk encap dot1q
NewYork(config)#end
NewYork#
```

B.



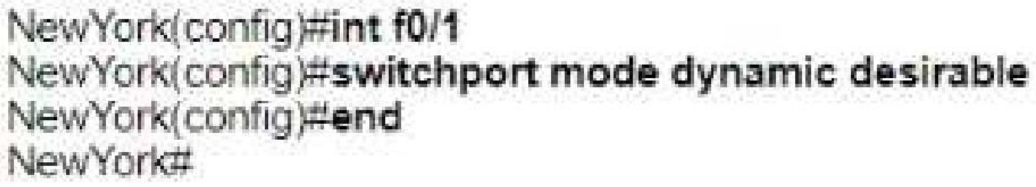
```
NewYork(config)#int f0/1
NewYork(config)#switchport mode trunk
NewYork(config)#end
NewYork#
```

C.



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

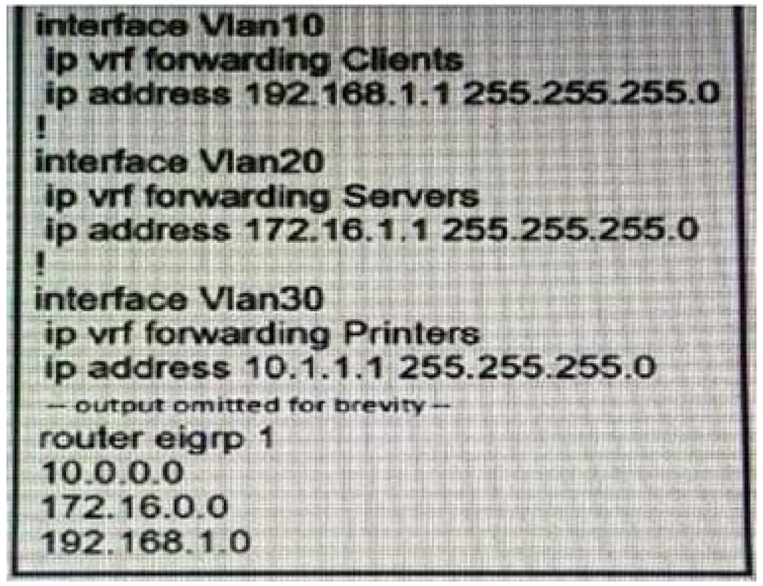
D.



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

Correct Answer: A
Section:
Explanation:
https://learningnetwork.cisco.com/s/question/0D53i00000Ksyty/tostastns-tottattnt

QUESTION 193

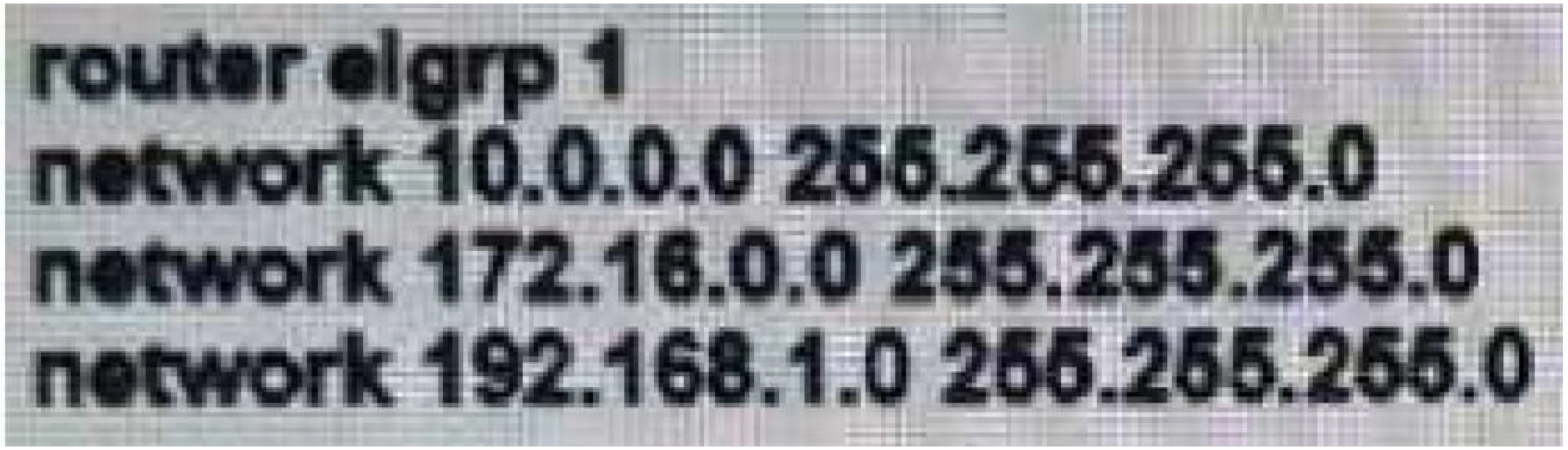


```
interface Vlan10
 ip vrf forwarding Clients
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan20
 ip vrf forwarding Servers
 ip address 172.16.1.1 255.255.255.0
!
interface Vlan30
 ip vrf forwarding Printers
 ip address 10.1.1.1 255.255.255.0
 -- output omitted for brevity --
router eigrp 1
10.0.0.0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

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

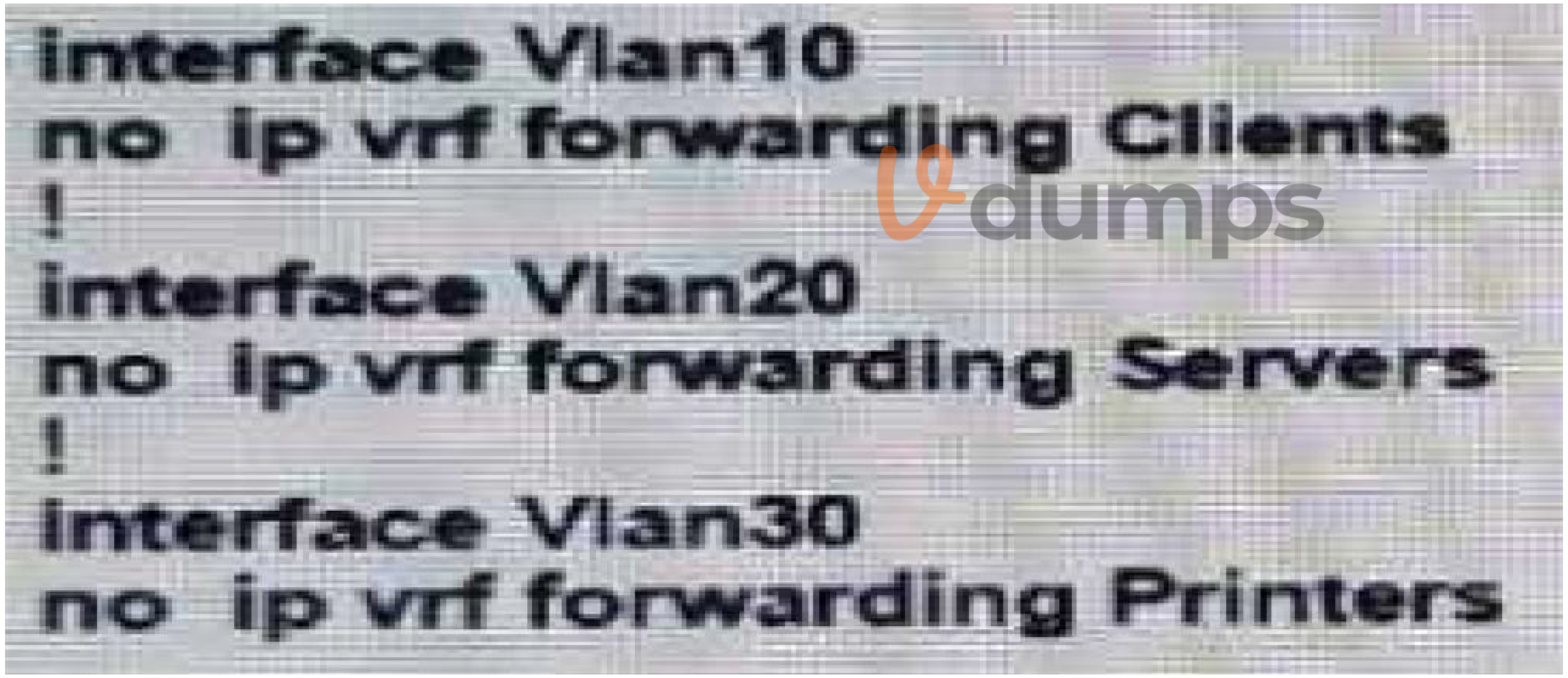
Which command set resolves this issue?

A.



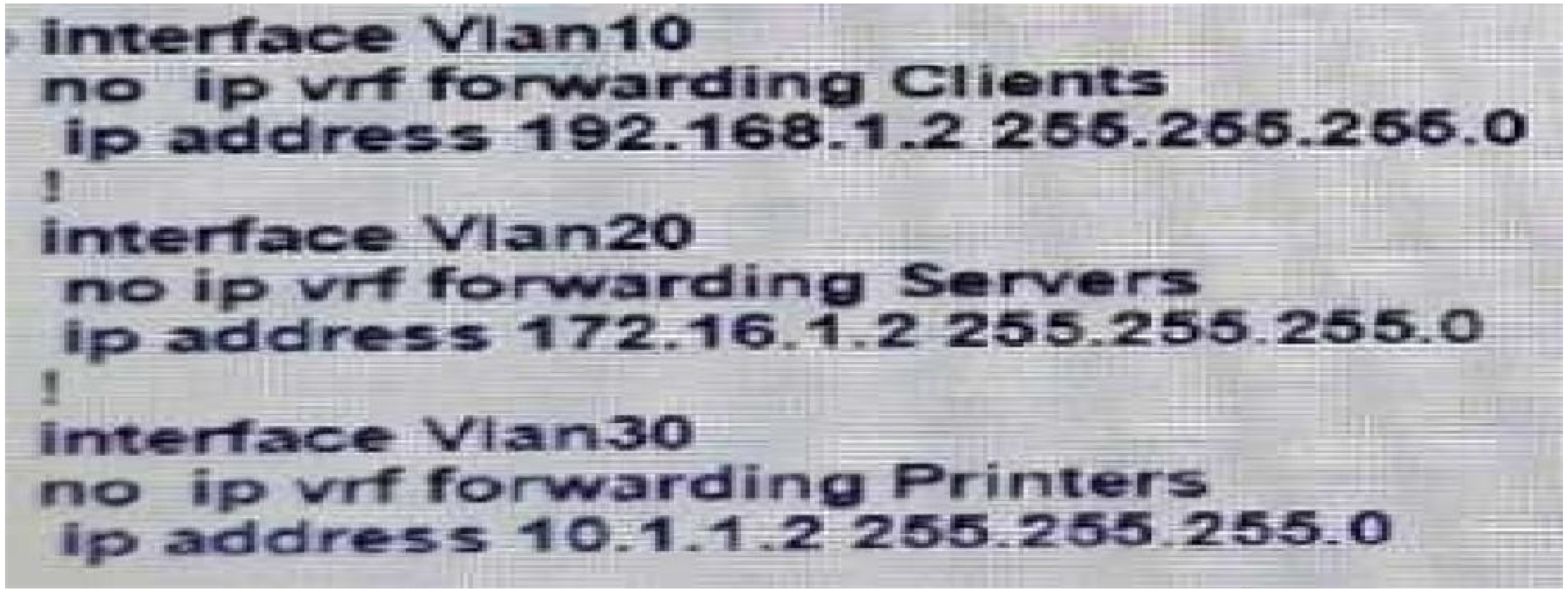
```
router eigrp 1
network 10.0.0.0 255.255.255.0
network 172.16.0.0 255.255.255.0
network 192.168.1.0 255.255.255.0
```

B.



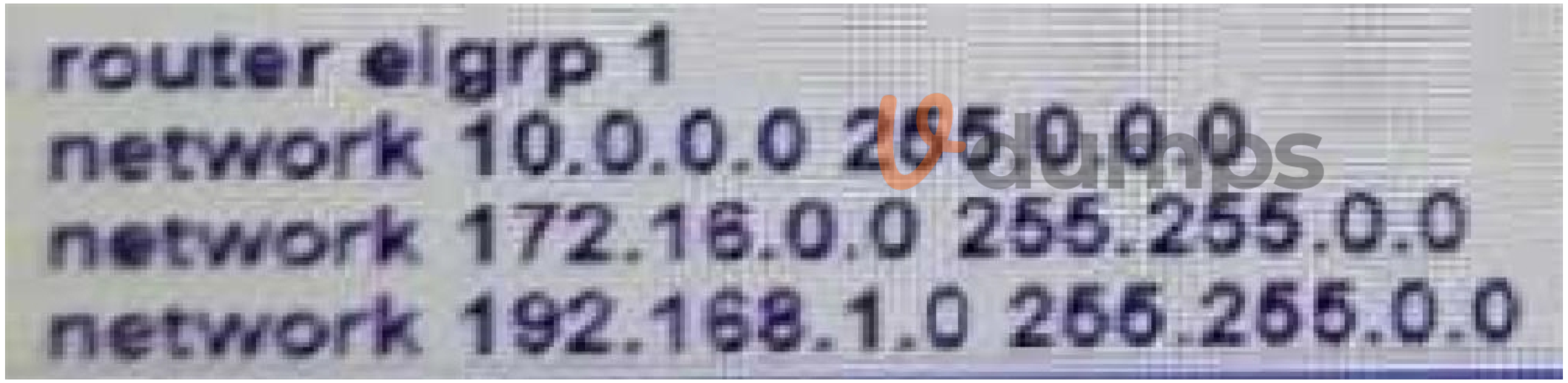
```
interface Vlan10
no  ip vrf forwarding Clients
!
interface Vlan20
no  ip vrf forwarding Servers
!
interface Vlan30
no  ip vrf forwarding Printers
```

C.



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

D.



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

Correct Answer: C
Section:
Explanation:
We must reconfigure the IP address after assigning or removing an interface to a VRF. Otherwise that interface does not have an IP address.

QUESTION 194
Why is an AP joining a different WLC than the one specified through option 43?

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

Correct Answer: B
Section:

QUESTION 195
What is a characteristic of Cisco DNA Northbound APIs?

A. They simplify the management of network infrastructure devices.
B. They enable automation of network infrastructure based on intent.
C. They utilize RESTCONF.
D. They utilize multivendor support APIs.

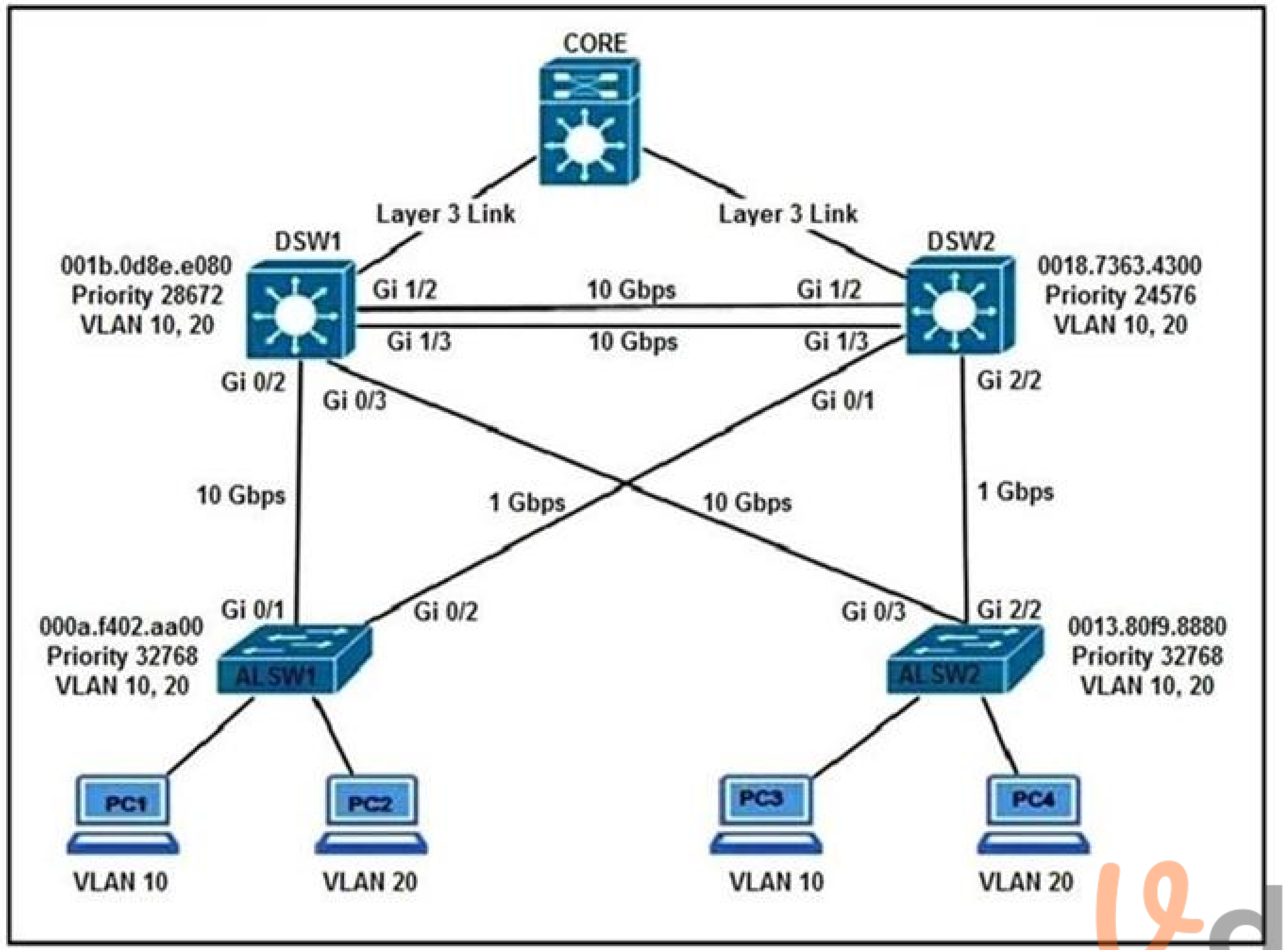
Correct Answer: C
Section:

QUESTION 196
An engineer configures a WLAN with fast transition enabled Some legacy clients fail to connect to this WLAN Which feature allows the legacy clients to connect while still allowing other clients to use fast transition based on then OLTIs?

A. over the DS
B. adaptive R
C. 802.11V
D. 802.11k

Correct Answer: B
Section:

QUESTION 197
Refer to the exhibit.



All switches are configured with the default port priority value. Which two commands ensure that traffic from PC1 is forwarded over Gi1/3 trunk port between DWS1 and DSW2? (Choose two)

A. DSW2(config-if)#spanning-tree port-priority 16
B. DSW2(config)#interface gi1/3
C. DSW1(config-if)#spanning-tree port-priority 0
D. DSW1(config) #interface gi1/3
E. DSW2(config-if)#spanning-tree port-priority 128

Correct Answer: A, B
Section:

QUESTION 198
Which two items are found in YANG data models? (Choose two.)

A. HTTP return codes
B. rpc statements
C. JSON schema
D. container statements
E. XML schema

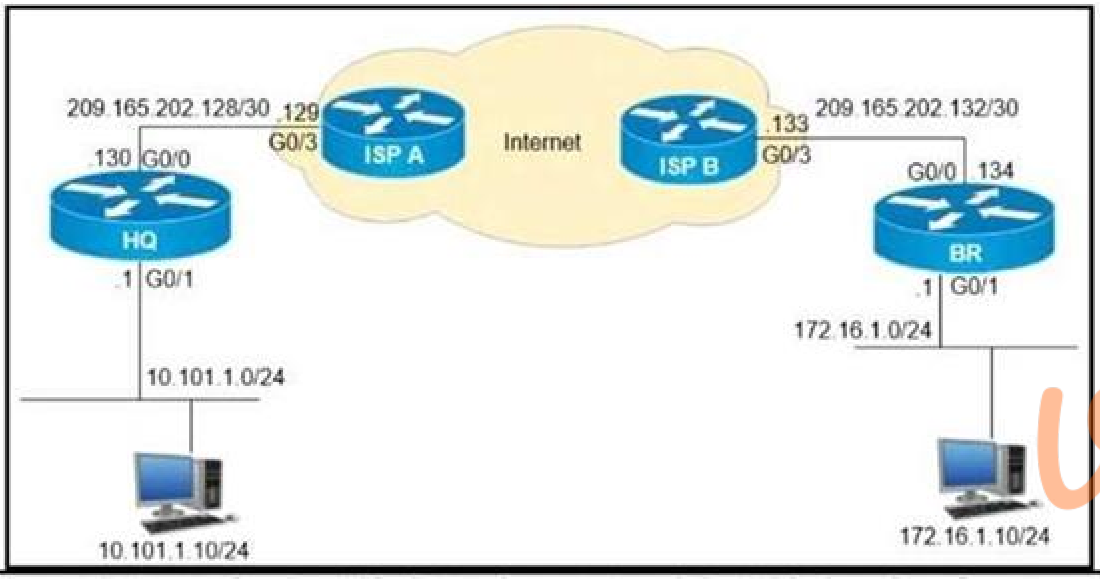
Correct Answer: C, E
Section:

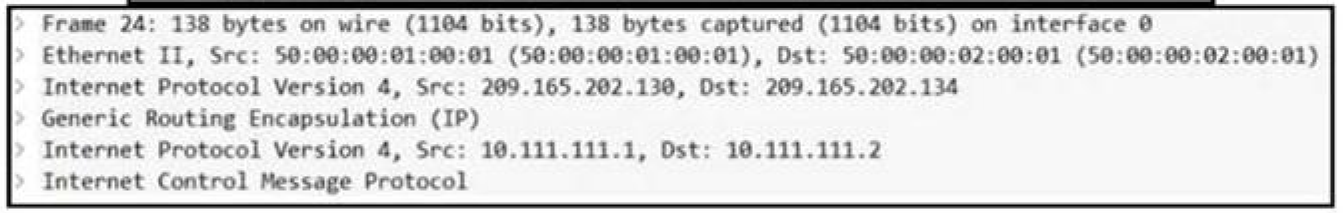
QUESTION 199
Which element enables communication between guest VMs within a virtualized environment?

A. hypervisor
B. vSwitch
C. virtual router
D. pNIC

Correct Answer: B
Section:

QUESTION 200
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 HO 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

Correct Answer: A
Section:

QUESTION 201
Which function does a fabric edge node perform in an SD-Access deployment?

A. Connects the SD-Access fabric to another fabric or external Layer 3 networks
B. Connects endpoints to the fabric and forwards their traffic

C. Provides reachability border nodes in the fabric underlay

D. Encapsulates end-user data traffic into LISP.

Correct Answer: B
Section:
Explanation:
There are five basic device roles in the fabric overlay:
+ Control plane node: This node contains the settings, protocols, and mapping tables to provide the endpoint-to-location (EID-to-RLOC) mapping system for the fabric overlay.
+ Fabric border node: This fabric device (for example, core layer device) connects external Layer 3 networks to the SDA fabric.
+ Fabric edge node: This fabric device (for example, access or distribution layer device) connects wired endpoints to the SDA fabric.
+ Fabric WLAN controller (WLC): This fabric device connects APs and wireless endpoints to the SDA fabric.
+ Intermediate nodes: These are intermediate routers or extended switches that do not provide any sort of SD-Access fabric role other than underlay services.

QUESTION 202
Which access point mode allows a supported AP to function like a WLAN client would, associating and identifying client connectivity issues?

A. client mode

B. SE-connect mode

C. sensor mode

D. sniffer mode

Correct Answer: C
Section:
Explanation:
As these wireless networks grow especially in remote facilities where IT professionals may not always be onsite, it becomes even more important to be able to quickly identify and resolve potential connectivity issuesideally before the users complain or notice connectivity degradation. To address these issues we have created Cisco's Wireless Service Assurance and a new AP mode called "sensor"mode. Cisco's Wireless Service Assurance platform has three components, namely, Wireless PerformanceAnalytics, Real-time Client Troubleshooting, and Proactive Health Assessment. Using a supported AP ordedicated sensor the device can actually function much like a WLAN client would associating andidentifying client connectivity issues within the network in real time without requiring an IT or technician to beon site.
Reference:
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/dam/en/us/td/docs/wireless/controller/technotes/8-5/b_Cisco_Aironet_Sensor_Deployment_Guide.html.xml

QUESTION 203
What is the structure of a JSON web token?

A. three parts separated by dots: header payload, and signature

B. header and payload

C. three parts separated by dots: version header and signature

D. payload and signature

Correct Answer: A
Section:
Explanation:
JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA or ECDSA.
JSON Web Tokens are composed of three parts, separated by a dot (.): Header, Payload, Signature. Therefore, a JWT typically looks like the following: xxxxx.yyyyy.zzzzz The header typically consists of two parts: the type of the token, which is JWT, and the signing algorithm being used, such as HMAC SHA256 or RSA.
The second part of the token is the payload, which contains the claims. Claims are statements about an entity (typically, the user) and additional data.
To create the signature part you have to take the encoded header, the encoded payload, a secret, the algorithm specified in the header, and sign that.
Reference: https://jwt.io/introduction/

QUESTION 204
Which technology does VXLAN use to provide segmentation for Layer 2 and Layer 3 traffic?

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

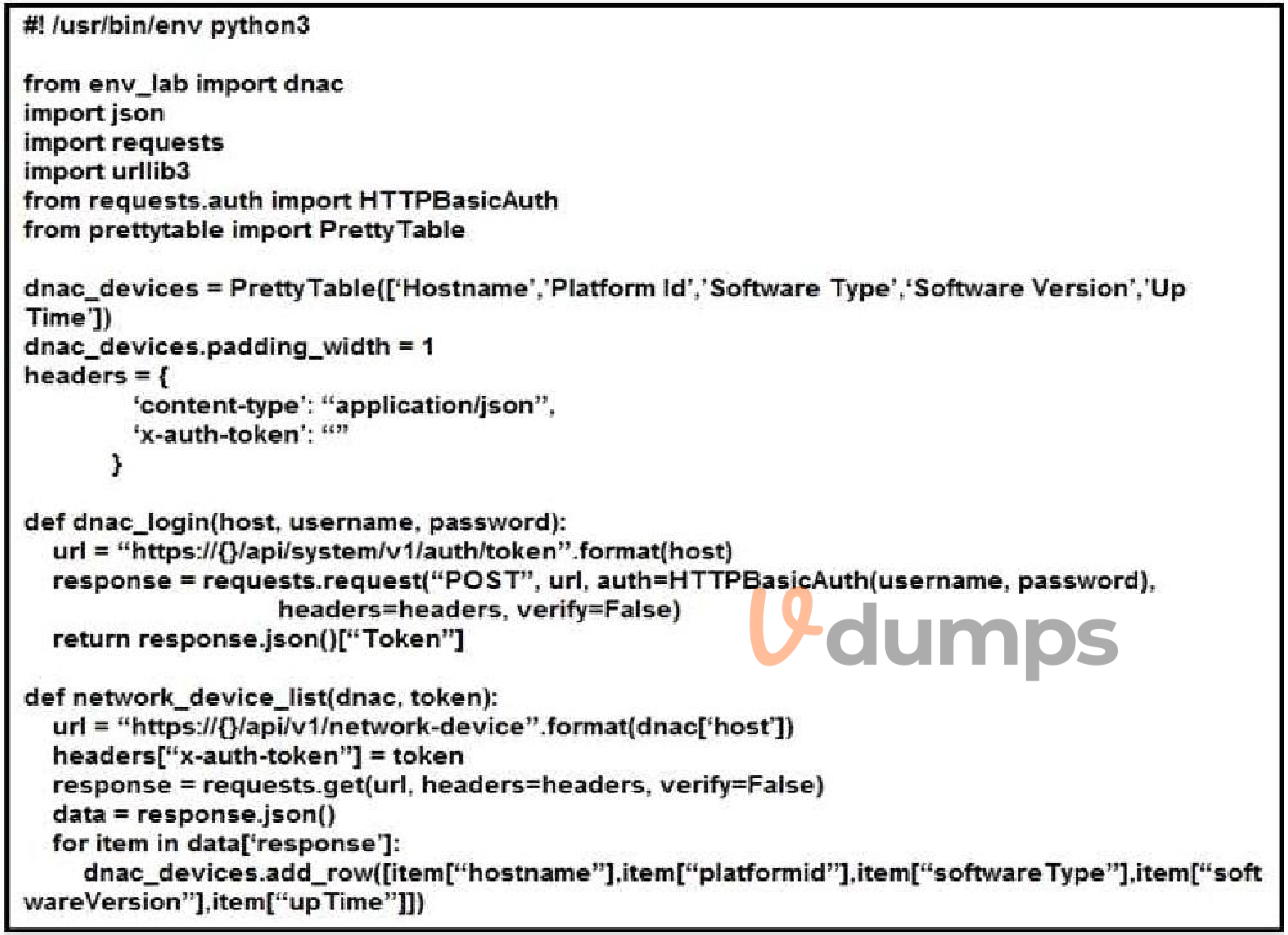
Correct Answer: D
Section:
Explanation:
VXLAN has a 24-bit VXLAN network identifier (VNI), which allows for up to 16 million (= 224) VXLAN segments to coexist within the same infrastructure. This surely solve the small number of traditional VLANs.

QUESTION 205
An engineer must protect their company against ransom ware attacks. Which solution allows the engineer to block the execution stage and prevent file encryption?

A. Use Cisco AMP deployment with the Malicious Activity Protection engineer enabled.
B. Use Cisco AMP deployment with the Exploit Prevention engine enabled.
C. Use Cisco Firepower and block traffic to TOR networks.
D. Use Cisco Firepower with Intrusion Policy and snort rules blocking SMB exploitation.

Correct Answer: B
Section:

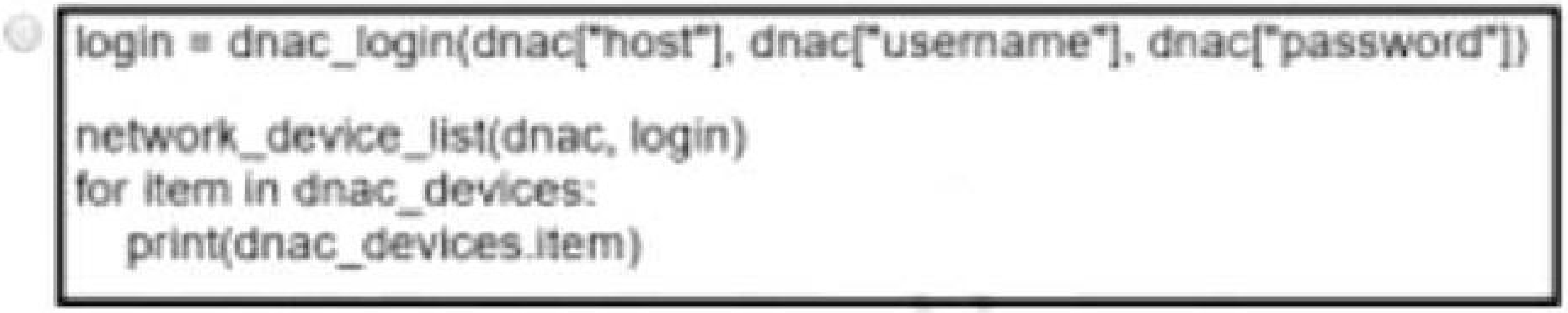
QUESTION 206
Refer to the exhibit.



```
#! /usr/bin/env python3

from env_lab import dnac
import json
import requests
import urllib3
from requests.auth import HTTPBasicAuth
from prettytable import PrettyTable

dnac_devices = PrettyTable([‘Hostname’,’Platform Id’,’Software Type’,‘Software Version’,’Up
Time’])
dnac_devices.padding_width = 1
headers = {
            ‘content-type’: “application/json”,
            ‘x-auth-token’: “”
         }

def dnac_login(host, username, password):
   url = “https://{}/api/system/v1/auth/token”.format(host)
   response = requests.request(“POST”, url, auth=HTTPBasicAuth(username, password),
                               headers=headers, verify=False)
   return response.json()[“Token”]

def network_device_list(dnac, token):
   url = “https://{}/api/v1/network-device”.format(dnac[‘host’])
   headers[“x-auth-token”] = token
   response = requests.get(url, headers=headers, verify=False)
   data = response.json()
   for item in data[‘response’]:
      dnac_devices.add_row([item[“hostname”],item[“platformid”],item[“softwareType”],item[“soft
wareVersion”],item[“upTime”]])
```

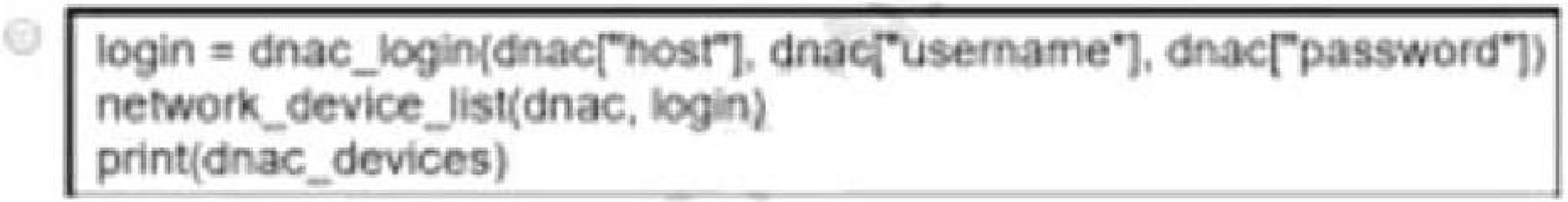
Which code results in the working Python script displaying a list of network devices from the Cisco DNA Center?

A.



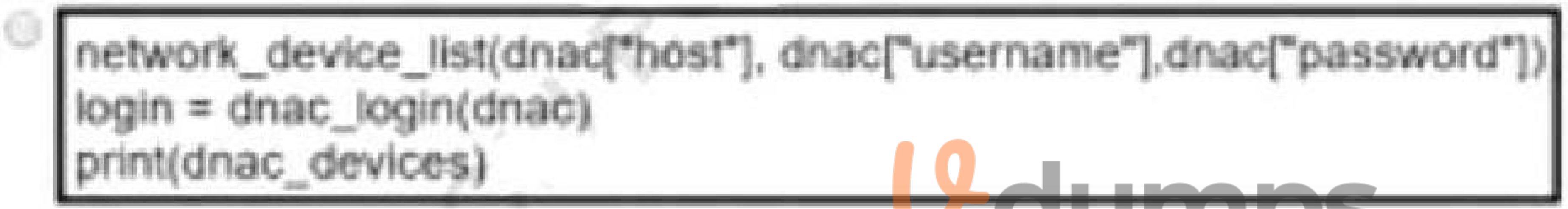
```
login = dnac_login(dnac["host"], dnac["username"], dnac["password"])

network_device_list(dnac, login)
for item in dnac_devices:
    print(dnac_devices.item)
```

B.



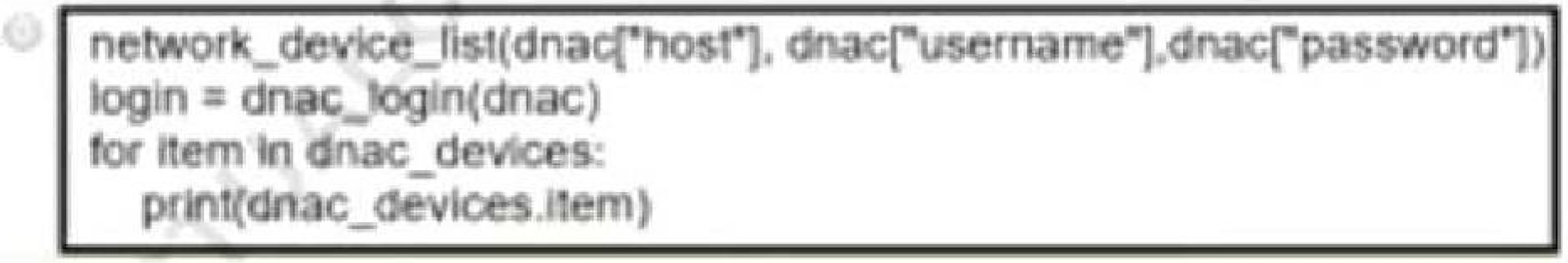
```
login = dnac_login(dnac["host"], dnac["username"], dnac["password"])
network_device_list(dnac, login)
print(dnac_devices)
```

C.



```
network_device_list(dnac["host"], dnac["username"],dnac["password"])
login = dnac_login(dnac)
print(dnac_devices)
```

D.

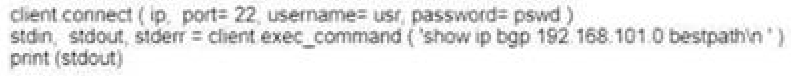


```
network_device_list(dnac["host"], dnac["username"],dnac["password"])
login = dnac_login(dnac)
for item in dnac_devices:
    print(dnac_devices.item)
```

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

Correct Answer: B
Section:

QUESTION 207
Which outcome is achieved with this Python code?



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

A. connects to a Cisco device using SSH and exports the routing table information

B. displays the output of the show command in a formatted way

C. connects to a Cisco device using SSH and exports the BGP table for the prefix

D. connects to a Cisco device using Telnet and exports the routing table information

Correct Answer: C
Section:

QUESTION 208

An engineer is configuring local web authentication on a WLAN. The engineer chooses the Authentication radio button under the Layer 3 Security options for Web Policy. Which device presents the web authentication for the WLAN?

A. ISE server

B. local WLC

C. RADIUS server

D. anchor WLC

Correct Answer: B
Section:
Explanation:

"The next step is to configure the WLC for the Internal web authentication. Internal web authentication is the defaultweb authentication type on WLCs." In step 4 of the link above, we will configure Security as described in this question.

Therefore we can deduce thisconfiguration is for Internal web authentication.

This paragraph was taken from the link https://www.cisco.com/c/en/us/support/docs/wirelessmobility/wlan-security/69340-web-auth-config.html#c5 :

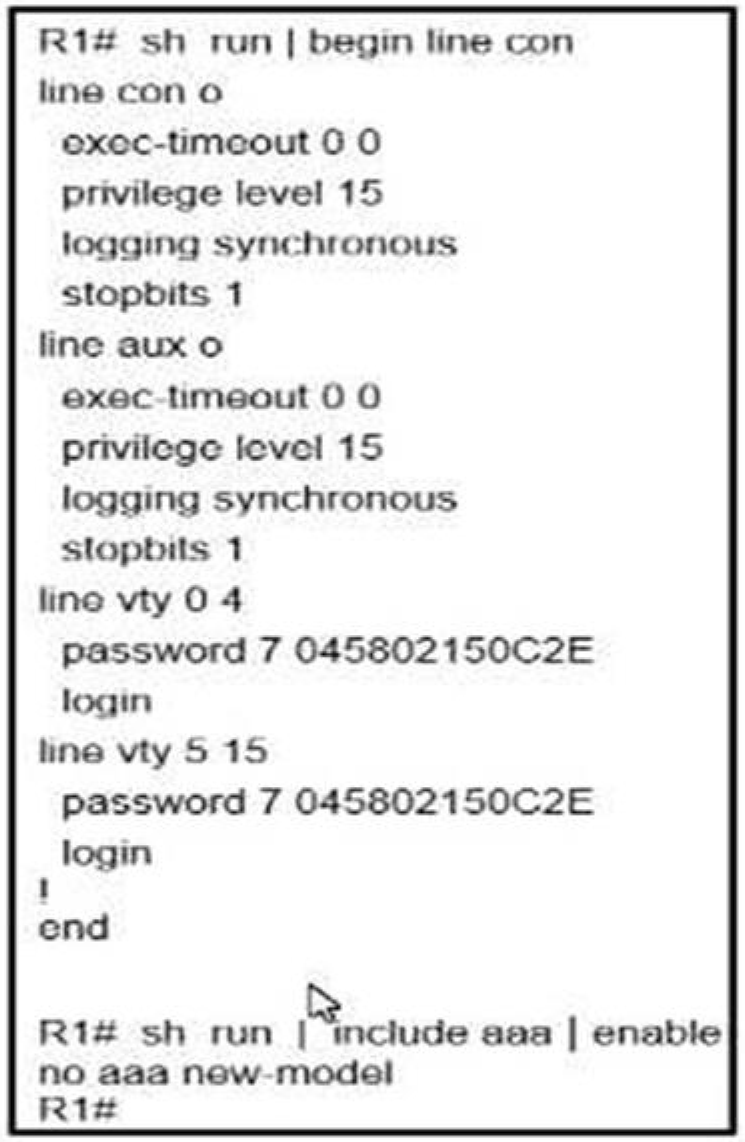
QUESTION 209

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

Correct Answer: C
Section:

QUESTION 210
Refer to the exhibit.



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

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

Which privilege level is assigned to VTY users?

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

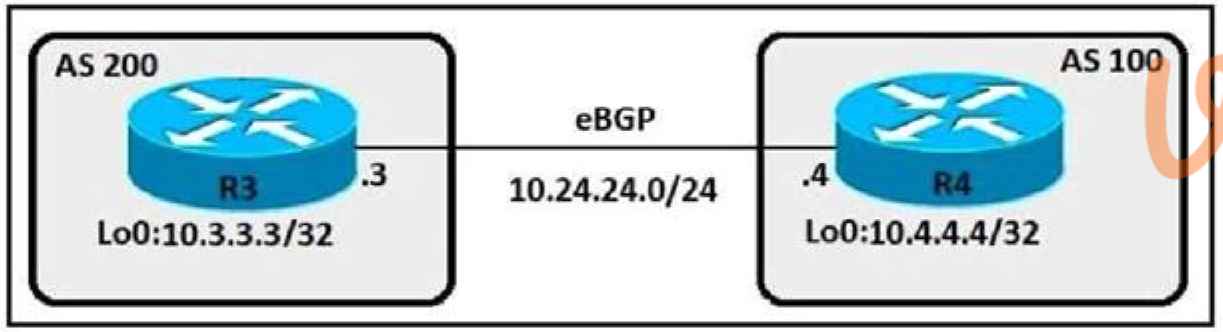
Correct Answer: A
Section:
Explanation:
Lines (CON, AUX, VTY) default to level 1 privileges.

QUESTION 211
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

Correct Answer: B
Section:
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 1https://media.zones.com/images/pdf/cisco-stealthwatch-solution-overview.pdf

QUESTION 212
Refer to the exhibit.



An engineer must establish eBGP peering between router R3 and router R4. Both routers should use their loopback interfaces as the BGP router ID. Which configuration set accomplishes this task?

A.
```
R3(config)#router bgp 200
R3(config-router)#neighbor 10.4.4.4 remote-as 100
R3(config-router)# neighbor 10.4.4.4 update-source Loopback0
R4(config)#router bgp 100
R4(config-router)#neighbor 10.3.3.3 remote-as 200
R4(config-router)#network 10.3.3.3 update-source Loopback0
```

B.
```
R3(config)#router bgp 200
R3(config-router)#neighbor 10.24.24.4 remote-as 100
R3(config-router)#neighbor 10.24.24.4 update-source Loopback0
R4(config)#router bgp 100
R4(config-router)#neighbor 10.24.24.3 remote-as 200
R4(config-router)#neighbor 10.24.24.3 update-source Loopback0
```

C.
```
R3(config)#router bgp 200
R3(config-router)#neighbor 10.4.4.4 remote-as 100
R3(config-router)#bgp router-id 10.3.3.3
R4(config)#router bgp 100
R4(config-router)#neighbor 10.3.3.3 remote-as 200
R4(config-router)#bgp router-id 10.4.4.4
```

D. R3(config)#router bgp 200
R3(config-router)#neighbor 10.24.24.4 remote-as 100
R3(config-router)#bgp router-id 10.3.3.3
R4(config)#router bgp 100
R4(config-router)#neighbor 10.24.24.3 remote-as 200
R4(config-router)#bgp router-id 10.4.4.4

Correct Answer: D
Section:

QUESTION 213
Which feature does Cisco TrustSec use to provide scalable, secure communication throughout a network?

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

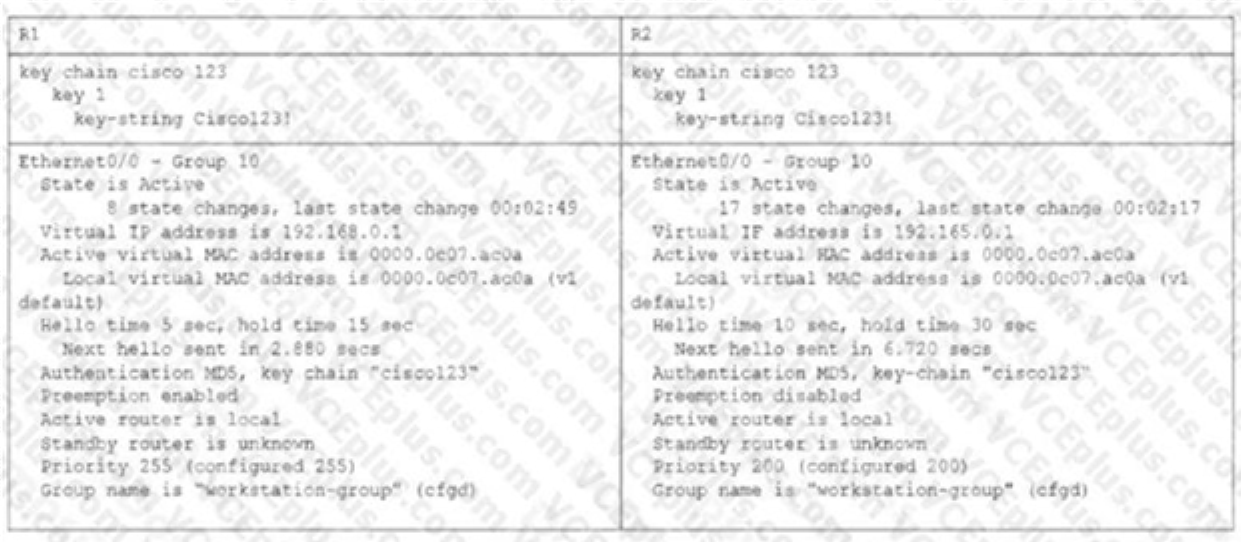
Correct Answer: B
Section:
Explanation:
Cisco TrustSec uses tags to represent logical group privilege. This tag, called a Security Group Tag
(SGT), is used in access policies. The SGT is understood and is used to enforce traffic by Cisco switches, routers and firewalls . Cisco TrustSec is defined in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

QUESTION 214
In a three-tier hierarchical campus network design, which action is a design best-practice for the core layer?

A. provide QoS prioritization services such as marking, queueing, and classification for critical network traffic
B. provide redundant Layer 3 point-to-point links between the core devices for more predictable and faster convergence
C. provide advanced network security features such as 802. IX, DHCP snooping, VACLs, and port security
D. provide redundant aggregation for access layer devices and first-hop redundancy protocols such as VRRP

Correct Answer: B
Section:

QUESTION 215
Refer to the Exhibit.



R1

```
key chain cisco 123
  key 1
    key-string Cisco123!
```

```
Ethernet0/0 - Group 10
  State is Active
        8 state changes, last state change 00:02:49
  Virtual IP address is 192.168.0.1
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1
default)
  Hello time 5 sec, hold time 15 sec
    Next hello sent in 2.880 secs
  Authentication MD5, key chain "cisco123"
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 255 (configured 255)
  Group name is "workstation-group" (cfgd)
```

R2

```
key chain cisco 123
  key 1
    key-string Cisco123!
```

```
Ethernet0/0 - Group 10
  State is Active
        17 state changes, last state change 00:02:17
  Virtual IP address is 192.165.0.1
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1
default)
  Hello time 10 sec, hold time 30 sec
    Next hello sent in 6.720 secs
  Authentication MD5, key-chain "cisco123"
  Preemption disabled
  Active router is local
  Standby router is unknown
  Priority 200 (configured 200)
  Group name is "workstation-group" (cfgd)
```

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

A. configure matching hold and delay timers

B. configure matching key-strings

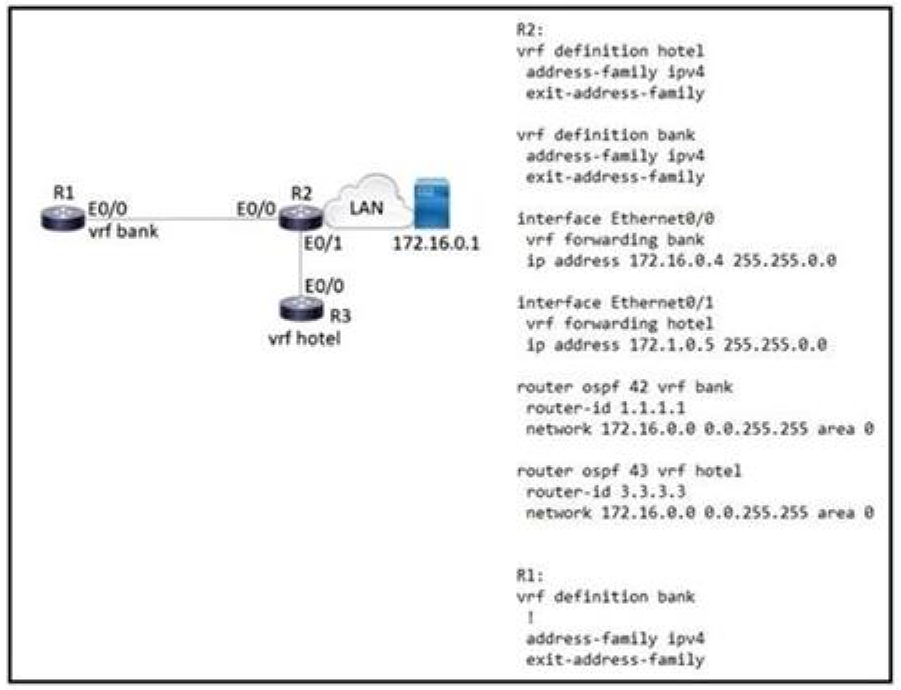
C. configure matching priority values

D. configure unique virtual IP addresses

Correct Answer: B
Section:
Explanation:

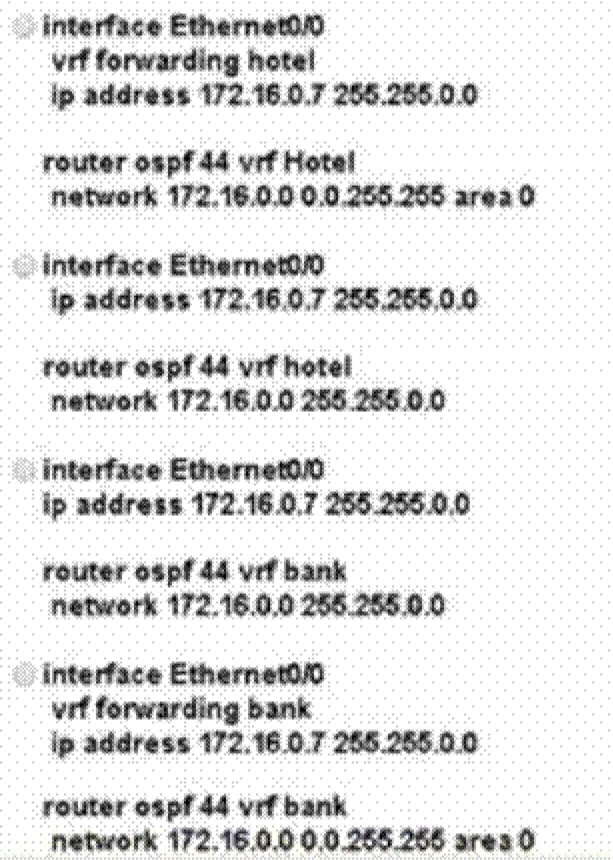
From the output exhibit, we notice that the key-string of R1 is ?Cisco123!? (letter ?C? is in capital) while that of R2 is ?cisco123!?. This causes a mismatch in the authentication so we have to fix their key-strings. key-string [encryption-type] text-string: Configures the text string for the key. The text-string argument is alphanumeric, case-sensitive, and supports special characters.
Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/security/configuration/guide/b_Cisco_Nexus_9000_Series_NXOS_Security_Configuration_Guide/b_Cisco_Nexus_9000_Series_NXOS_Security_Configuration_Guide_chapter_01111.pdf

QUESTION 216



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

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

interface Ethernet0/0
 vrf forwarding bank
 ip address 172.16.0.4 255.255.0.0

interface Ethernet0/1
 vrf forwarding hotel
 ip address 172.1.0.5 255.255.0.0

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

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


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

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

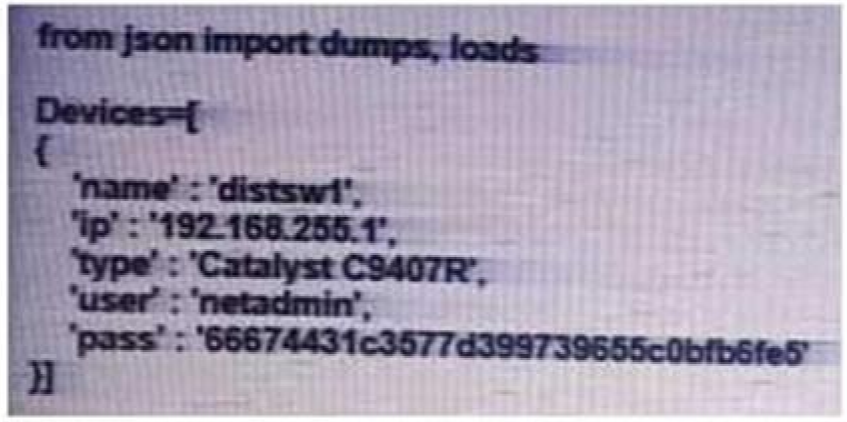


```
○ interface Ethernet0/0
   vrf forwarding hotel
   ip address 172.16.0.7 255.255.0.0

  router ospf 44 vrf Hotel
   network 172.16.0.0 0.0.255.255 area 0

○ interface Ethernet0/0
   ip address 172.16.0.7 255.255.0.0

  router ospf 44 vrf hotel
   network 172.16.0.0 255.255.0.0

○ interface Ethernet0/0
  ip address 172.16.0.7 255.255.0.0

  router ospf 44 vrf bank
   network 172.16.0.0 255.255.0.0

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

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

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

Correct Answer: D
Section:

QUESTION 217
An engineer must export the contents of the devices object in JSON format. Which statement must be used?



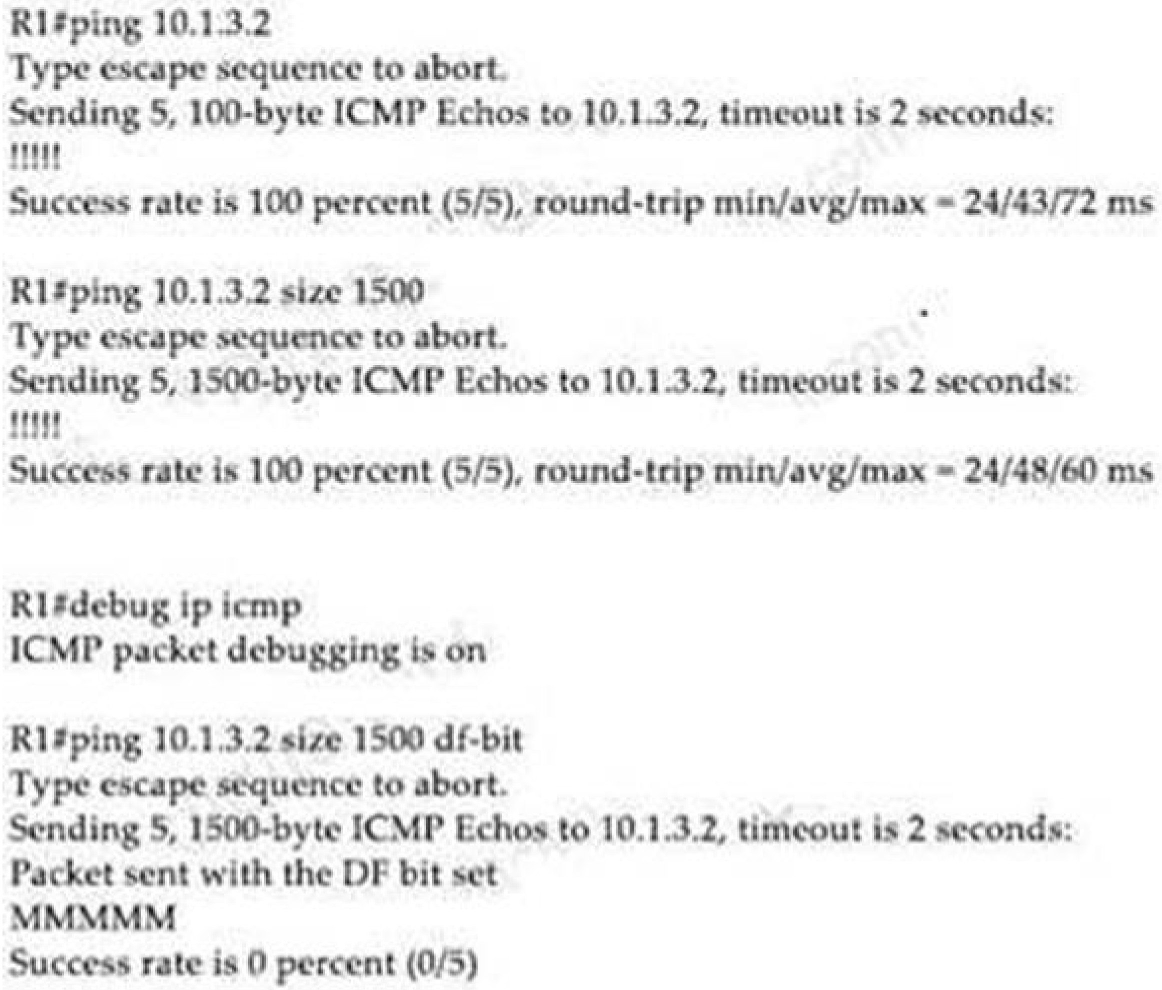
```
from json import dumps, loads

Devices=[
{
   'name' : 'distsw1',
   'ip' : '192.168.255.1',
   'type' : 'Catalyst C9407R',
   'user' : 'netadmin',
   'pass' : '66674431c3577d399739655c0bfb6fe5'
}]
```

A. json.repr(Devices)
B. json.dumps(Devices)
C. json.prints(Devices)

D. json.loads(Devices)

Correct Answer: B
Section:

QUESTION 218
Refer to the exhibit.



```
R1#ping 10.1.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/43/72 ms

R1#ping 10.1.3.2 size 1500
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 10.1.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/48/60 ms


R1#debug ip icmp
ICMP packet debugging is on

R1#ping 10.1.3.2 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 10.1.3.2, timeout is 2 seconds:
Packet sent with the DF bit set
MMMMM
Success rate is 0 percent (0/5)
```

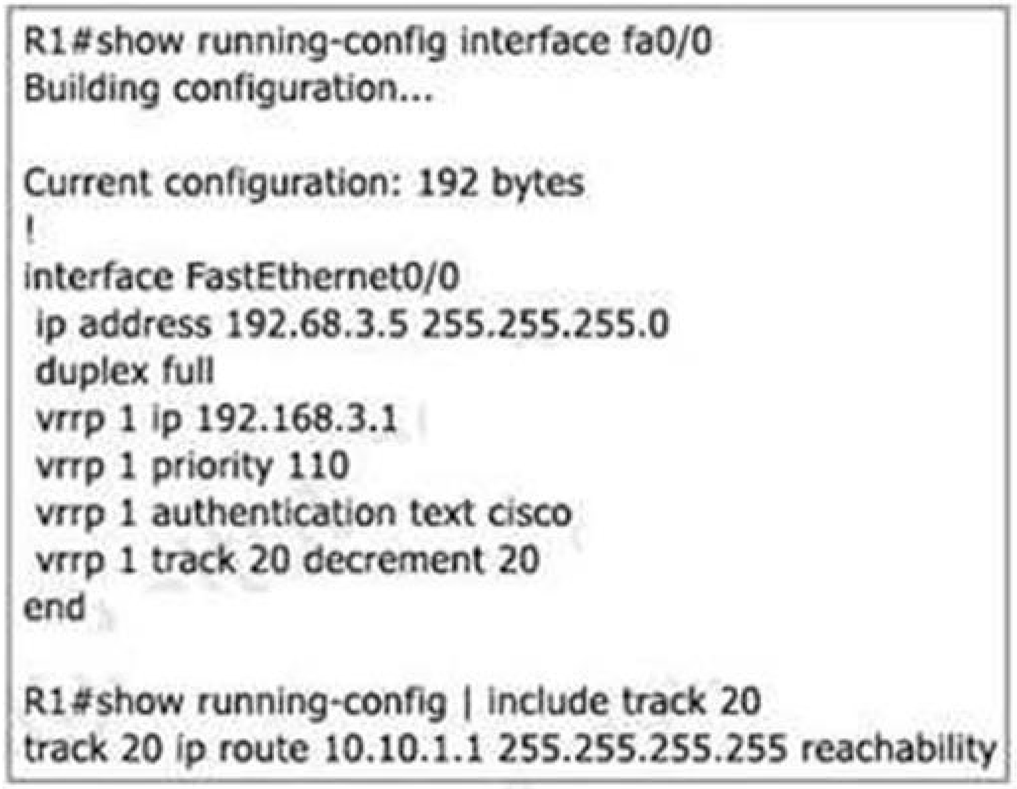
An engineer troubleshoots connectivity issues with an application. Testing is performed from the server gateway, and traffic with the DF bit set is dropped along the path after increasing packet size. Removing the DF bit setting at the gateway prevents the packets from being dropped. What is the cause of this issue?

A. PMTUD does not work due to ICMP Packet Too Big messages being dropped by an ACL
B. The remote router drops the traffic due to high CPU load
C. The server should not set the DF bit in any type of traffic that is sent toward the network
D. There is a CoPP policy in place protecting the WAN router CPU from this type of traffic

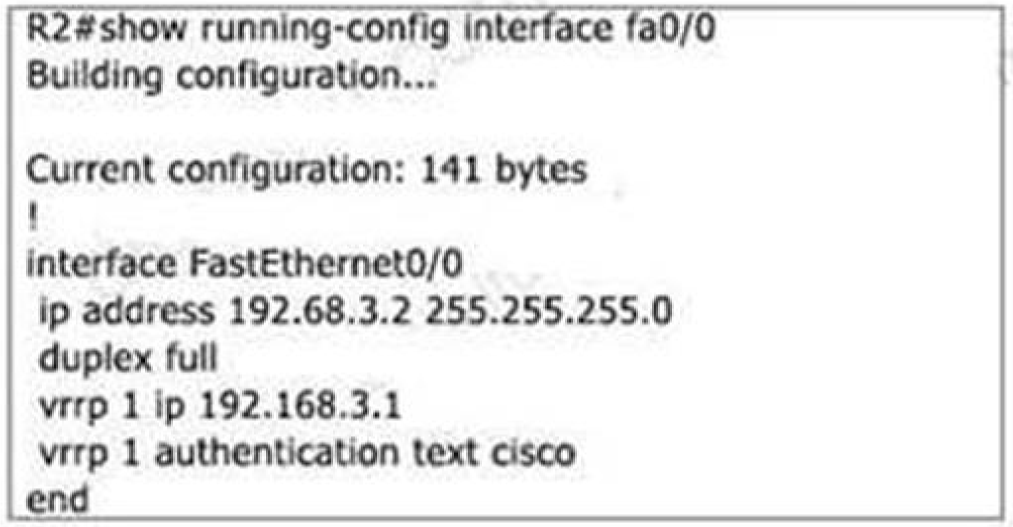
Correct Answer: C
Section:

QUESTION 219

Refer to the exhibit:



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

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

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



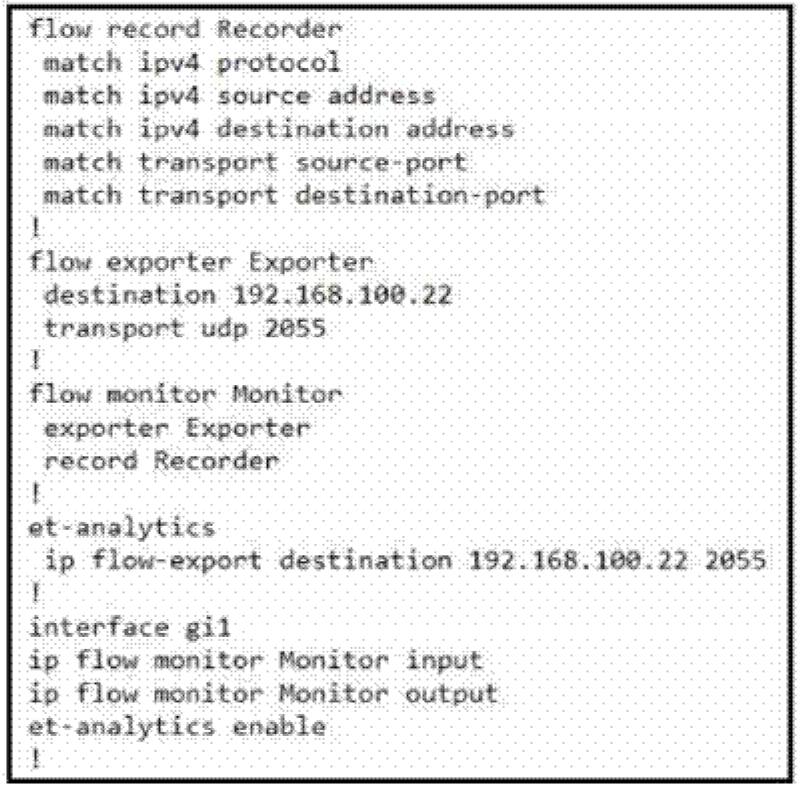
```
R2#show running-config interface fa0/0
Building configuration...

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

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

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

Correct Answer: D
Section:

QUESTION 220
Refer to the exhibit.



```
flow record Recorder
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
!
flow exporter Exporter
 destination 192.168.100.22
 transport udp 2055
!
flow monitor Monitor
 exporter Exporter
 record Recorder
!
et-analytics
 ip flow-export destination 192.168.100.22 2055
!
interface gi1
ip flow monitor Monitor input
ip flow monitor Monitor output
et-analytics enable
!
```

An engineer must add the SNMP interface table to the NetFlow protocol flow records. Where should the SNMP table option be added?

A. under the interface
B. under the flow record
C. under the flow monitor
D. under the flow exporter

Correct Answer: D
Section:
Explanation:
option interface-table This command causes the periodic sending of an options table, which will allow the collector to map the interface SNMP indexes provided in the flow records to interface names. The optional timeout can alter the frequency at which the reports are sent.
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# option interface-table
https://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_02.html

QUESTION 221

Which NGFW mode block flows crossing the firewall?

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

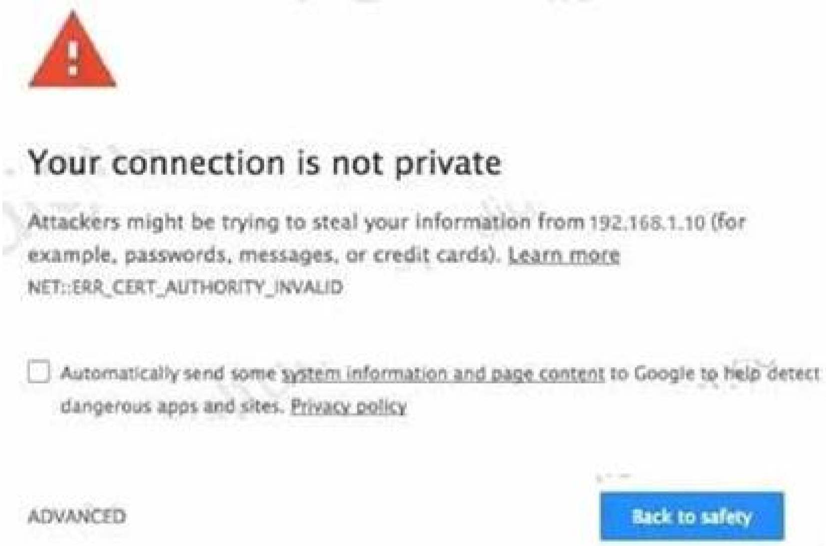
Correct Answer: D
Section:
Explanation:
Firepower Threat Defense (FTD) provides six interface modes which are: Routed, Switched, Inline Pair, Inline Pair with Tap, Passive, Passive (ERSPAN).
When Inline Pair Mode is in use, packets can be blocked since they are processed inline When you use Inline Pair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

QUESTION 222
Which deployment option of Cisco NGFW provides scalability?

A. tap
B. clustering
C. inline tap
D. high availability

Correct Answer: B
Section:
Explanation:
Clustering lets you group multiple Firepower Threat Defense (FTD) units together as a single logical device. Clustering is only supported for the FTD device on the Firepower 9300 and the Firepower 4100 series. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices.}

QUESTION 223
Refer to the exhibit.



Your connection is not private

Attackers might be trying to steal your information from 192.168.1.10 (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

An engineer is designing a guest portal on Cisco ISE using the default configuration. During the testing phase, the engineer receives a warning when displaying the guest portal. Which issue is occurring?

A. The server that is providing the portal has an expired certificate

B. The server that is providing the portal has a self-signed certificate

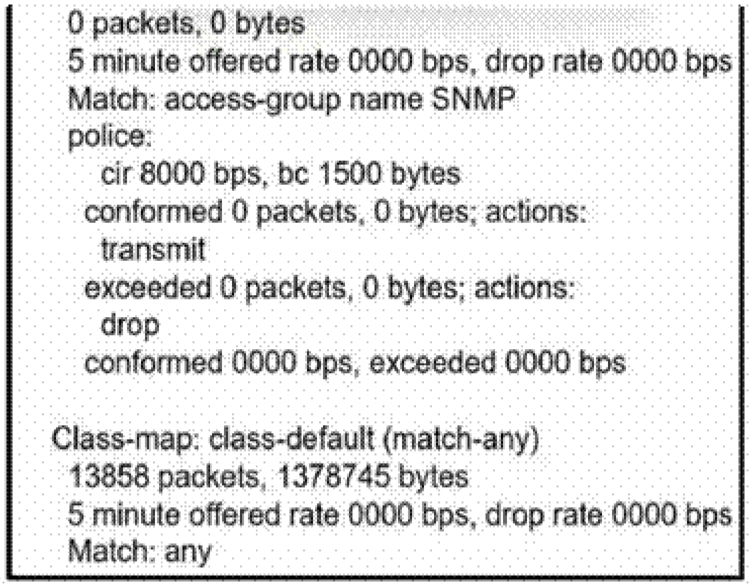
C. The connection is using an unsupported protocol

D. The connection is using an unsupported browser

Correct Answer: B
Section:

QUESTION 224

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.

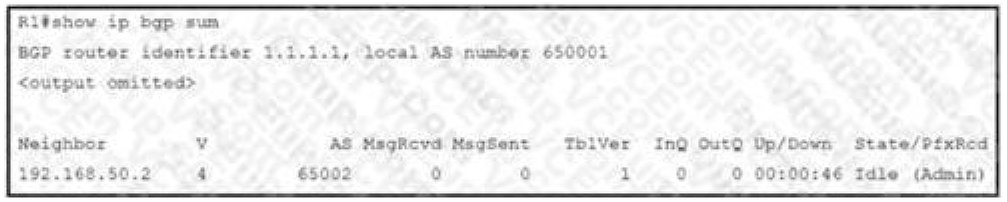
C. Traffic passing through R1 that matches access list SNMP is policed.

D. Traffic generated by R1 that matches access list SNMP is policed.

Correct Answer: C
Section:

QUESTION 225

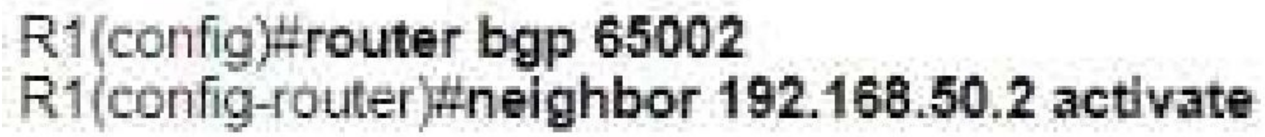
Refer to the exhibit.



```
R1#show ip bgp sum
BGP router identifier 1.1.1.1, local AS number 650001
<output omitted>

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

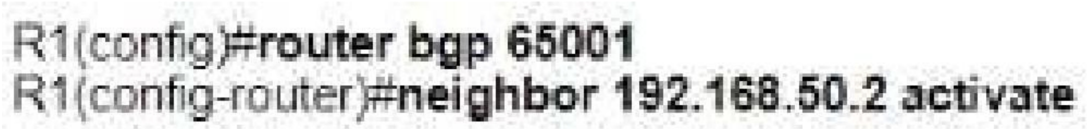
Which command set changes the neighbor state from Idle (Admin) to Active?

A.



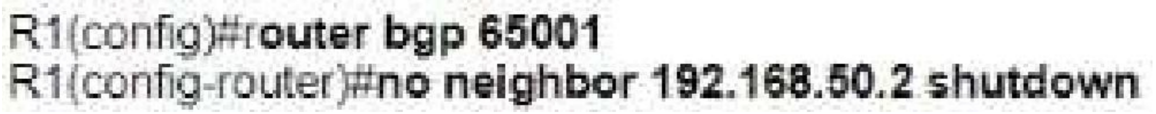
```
R1(config)#router bgp 65002
R1(config-router)#neighbor 192.168.50.2 activate
```

B.



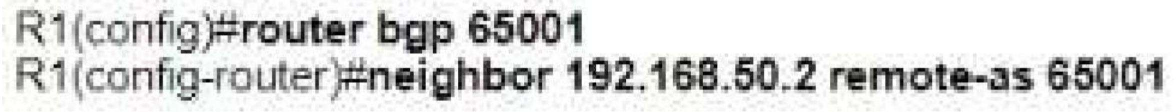
```
R1(config)#router bgp 65001
R1(config-router)#neighbor 192.168.50.2 activate
```

C.



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

D.



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

Correct Answer: C
Section:

QUESTION 226
A network engineer configures a WLAN controller with increased security for web access. There is IP connectivity with the WLAN controller, but the engineer cannot start a management session from a web browser. Which action resolves the issued

A. Disable JavaScript on the web browser
B. Disable Adobe Flash Player
C. Use a browser that supports 128-bit or larger ciphers.
D. Use a private or incognito session.

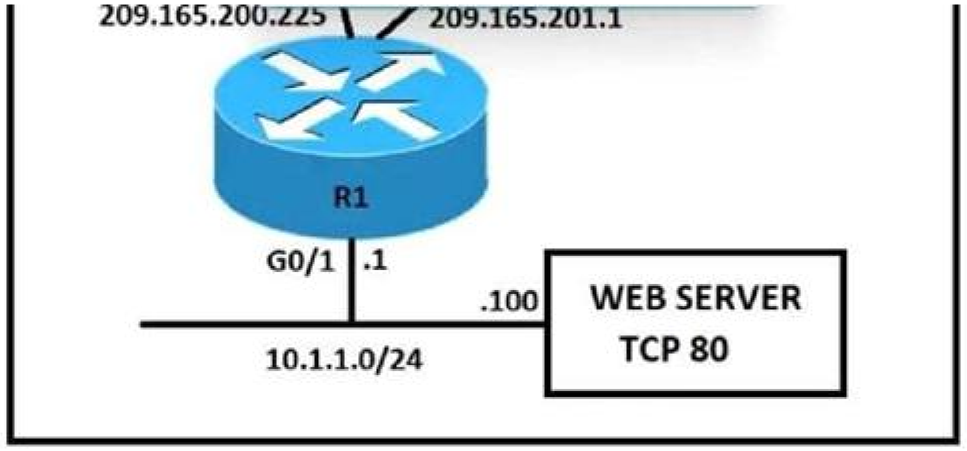
Correct Answer: C
Section:

QUESTION 227
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

Correct Answer: C
Section:

QUESTION 228
Refer to the exhibit.



An engineer must configure static NAT on R1 lo allow users HTTP access to the web server on TCPport 80. The web server must be reachable through ISP 1 and ISP 2. Which command set should beapplied 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 8080 209.165.201.1 8080
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

Correct Answer: B
Section:

QUESTION 229
By default, which virtual MAC address does HSRP group 16 use?

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

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

QUESTION 230
A customer requests a design that includes GLBP as the FHRP The network architect discovers that the members of the GLBP group have different throughput capabilities Which GLBP load balancing method supports this environment?

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

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

used by an extended

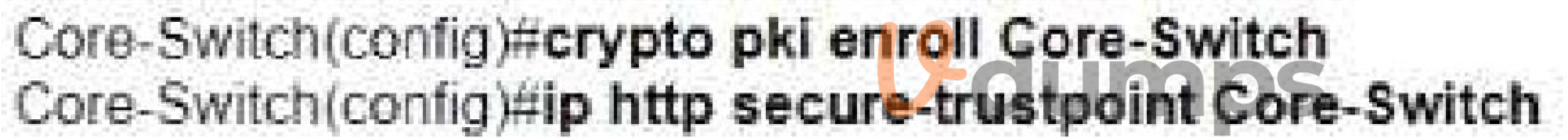
QUESTION 231
In a Cisco SD-WAN solution, which two functions are performed by OMP? (Choose two.)

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

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

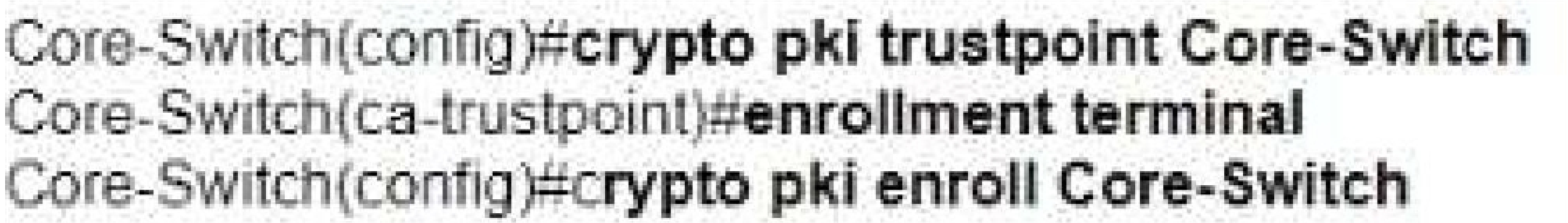
QUESTION 232
A network engineer is enabling HTTPS access to the core switch, which requires a certificate to beinstalled on the switch signed by the corporate certificate authority Which configuration commandsare required to issue a certificate signing request from the core switch?

A.



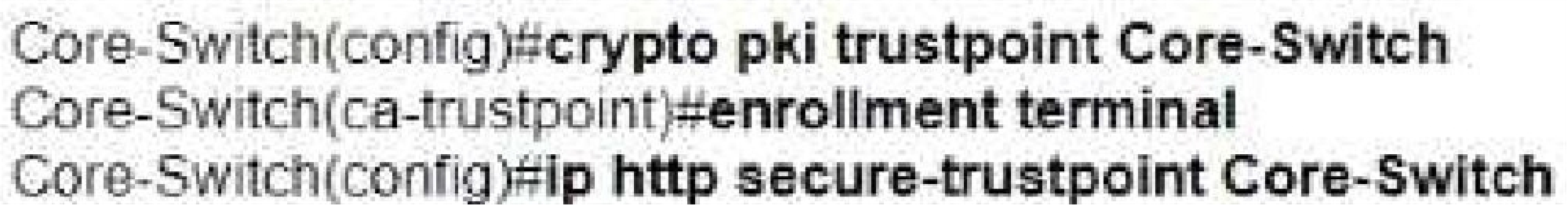
```
Core-Switch(config)#crypto pki enroll Core-Switch
Core-Switch(config)#ip http secure-trustpoint Core-Switch
```

B.



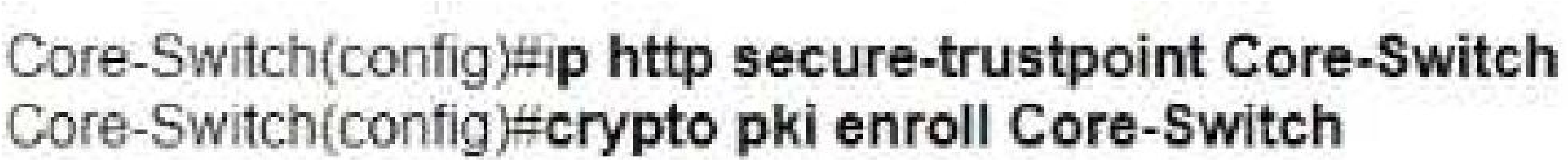
```
Core-Switch(config)#crypto pki trustpoint Core-Switch
Core-Switch(ca-trustpoint)#enrollment terminal
Core-Switch(config)#crypto pki enroll Core-Switch
```

C.



```
Core-Switch(config)#crypto pki trustpoint Core-Switch
Core-Switch(ca-trustpoint)#enrollment terminal
Core-Switch(config)#ip http secure-trustpoint Core-Switch
```

D.



```
Core-Switch(config)#ip http secure-trustpoint Core-Switch
Core-Switch(config)#crypto pki enroll Core-Switch
```

Correct Answer: B
Section:
Explanation:
Certificate authorities (CAs) are responsible for managing certificate requests and issuing certificates to participating IPSec network devices. These services provide centralized security key and certificate management for the participating devices. Specific CA servers are referred to as "trustpoints." The command "crypto pki trustpoint name" declares the trustpoint and a given name and enters catrustpoint configuration mode.
The command "enrollment terminal" specifies manual cut-and-paste certificate enrollment method.
The certificate request will be displayed on the console terminal so that you may manually copied (or cut).
The command "crypto pki enroll name" generates certificate request and displays the request for copying and pasting into the certificate server.
The full configuration is shown in the reference below.
Reference: https://www.cisco.com/c/en/us/td/docs/ios/ios_xe/sec_secure_connectivity/configuration/guide/convert/sec_pki_xe_3s_book/sec_cert_enroll_pki_xe.html

QUESTION 233
What is the process for moving a virtual machine from one host machine to another with no downtime?

A. high availability
B. disaster recovery
C. live migration
D. multisite replication

Correct Answer: C
Section:

QUESTION 234
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.

Correct Answer: D
Section:

QUESTION 235
An engineer must create a new SSID on a Cisco 9800 wireless LAN controller. The client has asked to use a pre-shared key for authentication Which profile must the engineer edit to achieve this requirement?

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

Correct Answer: B

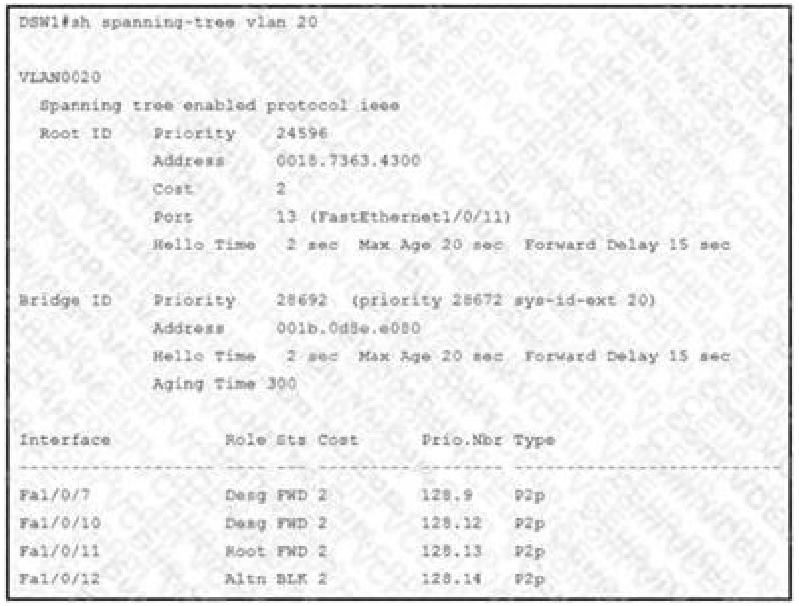
Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116880-configwpa2-psk-00.html

QUESTION 236
A vulnerability assessment highlighted that remote access to the switches is permitted using unsecure and unencrypted protocols Which configuration must be applied to allow only secure and reliable remote access for device administration?

A. line vty 0 15 login local transport input none
B. line vty 0 15 login local transport input telnet ssh
C. line vty 0 15 login local transport input ssh
D. line vty 0 15 login local transport input all

Correct Answer: C
Section:

QUESTION 237
Refer to the exhibit.



```
DSW1#sh spanning-tree vlan 20

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

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

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

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

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

Correct Answer: C
Section:

QUESTION 238
How does a fabric AP fit in the network?

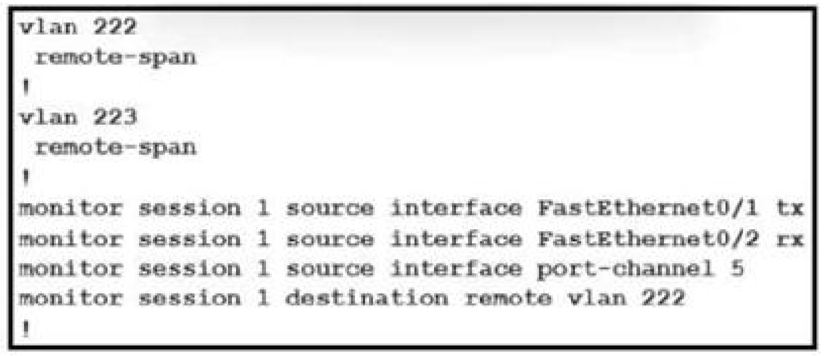
A. It is in local mode and must be connected directly to the fabric border node
B. It is in FlexConnect mode and must be connected directly to the fabric edge switch.

C. It is in FlexConnect mode and must be connected directly to the fabric border node

D. It is in local mode and must be connected directly to the fabric edge switch.

Correct Answer: D
Section:

QUESTION 239
Refer to the exhibit.



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

What is the result when a technician adds the monitor session 1 destination remote vlan 223 command1?

A. The RSPAN VLAN is replaced by VLAN 223.

B. RSPAN traffic is sent to VLANs 222 and 223

C. An error is flagged for configuring two destinations.

D. RSPAN traffic is split between VLANs 222 and 223.

Correct Answer: A
Section:

QUESTION 240
How are map-register messages sent in a LISP deployment?

A. egress tunnel routers to map resolvers to determine the appropriate egress tunnel router

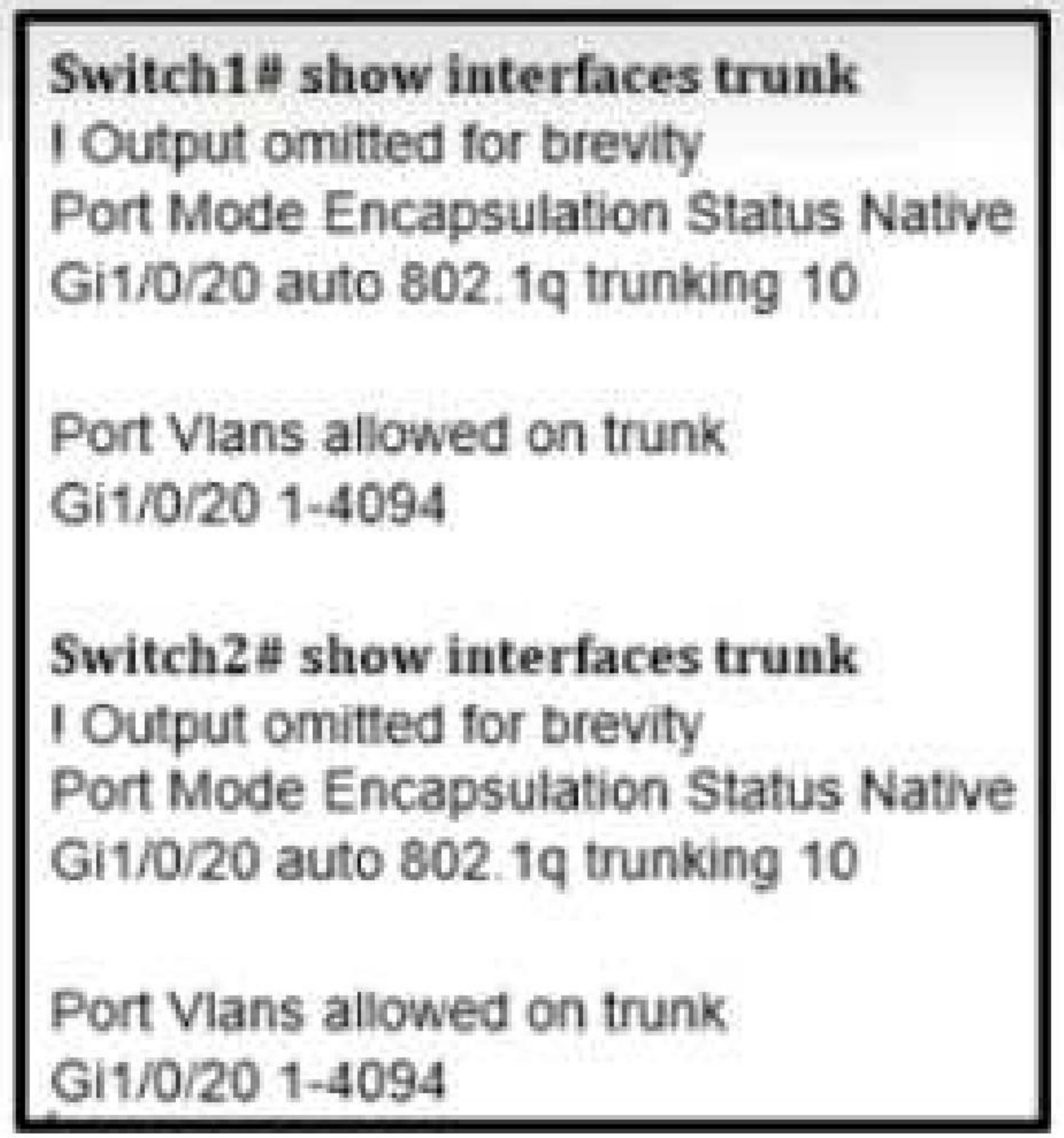
B. ingress tunnel routers to map servers to determine the appropriate egress tunnel router

C. egress tunnel routers to map servers to determine the appropriate egress tunnel router

D. ingress tunnel routers to map resolvers to determine the appropnate egress tunnel router

Correct Answer: C
Section:
Explanation:
During operation, an Egress Tunnel Router (ETR) sends periodic Map-Register messages to all its configured map servers.

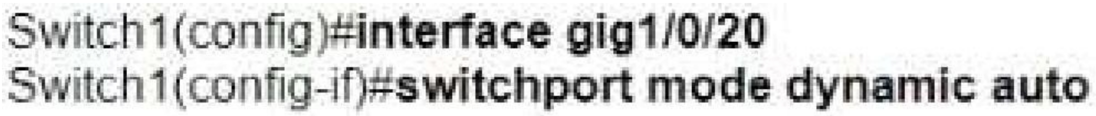
QUESTION 241
Refer to the exhibit.



```
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
```

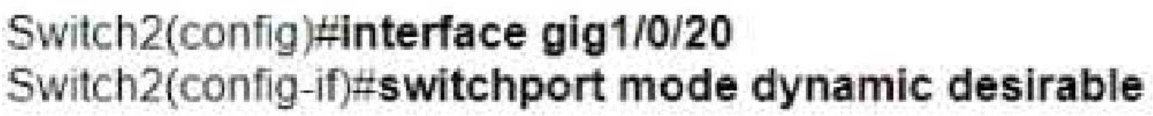
The trunk does not work over the back-to-back link between Switch1 interface Giq1/0/20 and Switch2 interface Gig1/0/20. Which configuration fixes the problem?

A.



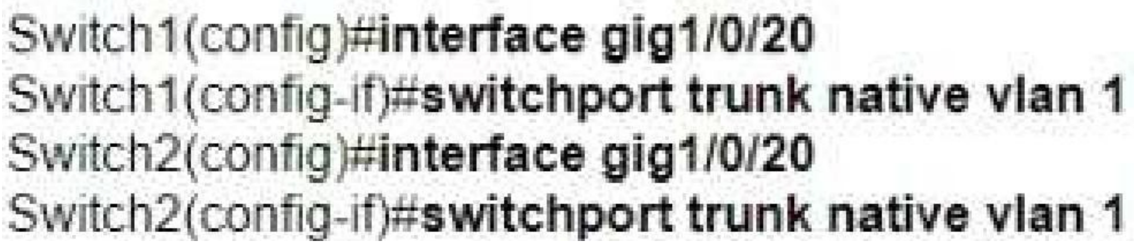
```
Switch1(config)#interface gig1/0/20
Switch1(config-if)#switchport mode dynamic auto
```

B.



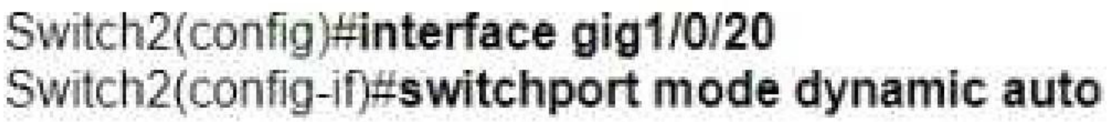
```
Switch2(config)#interface gig1/0/20
Switch2(config-if)#switchport mode dynamic desirable
```

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
```

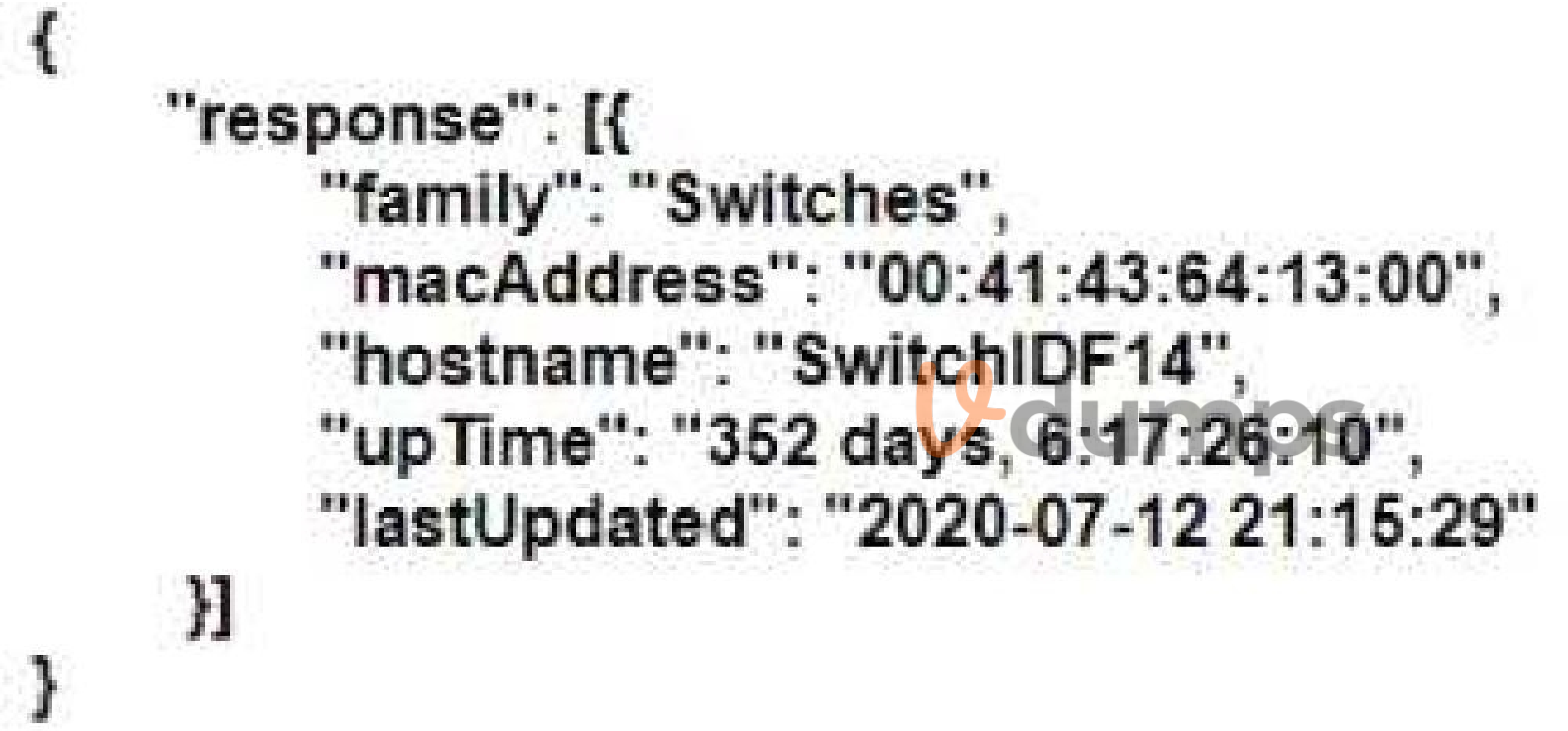
D.



```
Switch2(config)#interface gig1/0/20
Switch2(config-if)#switchport mode dynamic auto
```

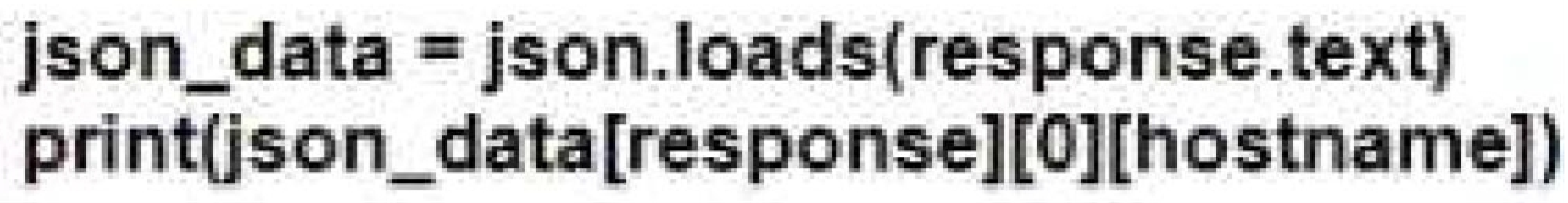
Correct Answer: B
Section:

QUESTION 242
Based on the router's API output in JSON format below, which Python code will display the value of the "hostname" key?



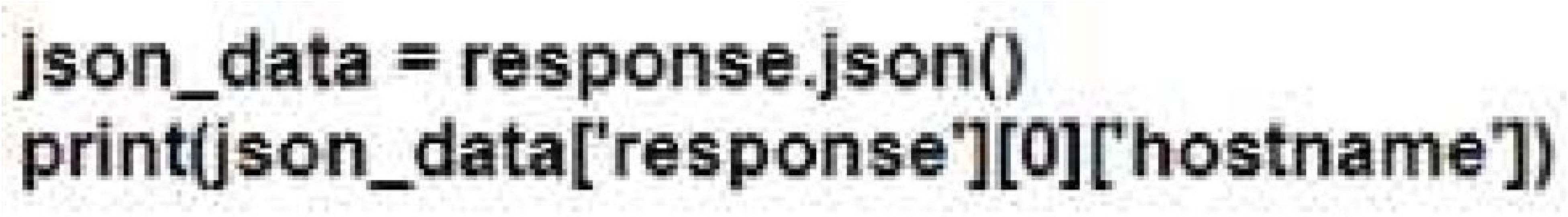
```
{
    "response": [{
        "family": "Switches",
        "macAddress": "00:41:43:64:13:00",
        "hostname": "SwitchIDF14",
        "upTime": "352 days, 6:17:26:10",
        "lastUpdated": "2020-07-12 21:15:29"
    }]
}
```

A.



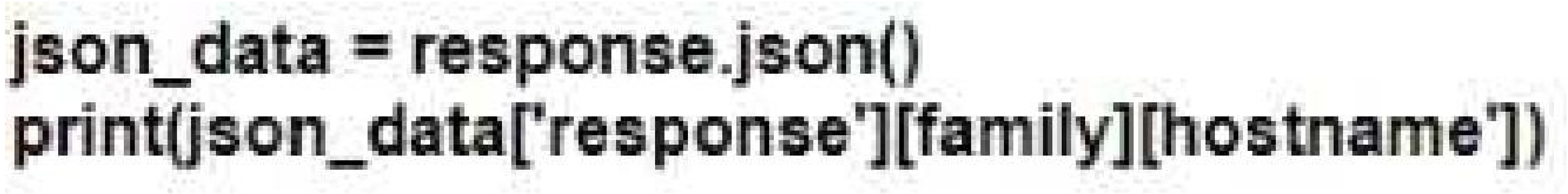
```
json_data = json.loads(response.text)
print(json_data[response][0][hostname])
```

B.



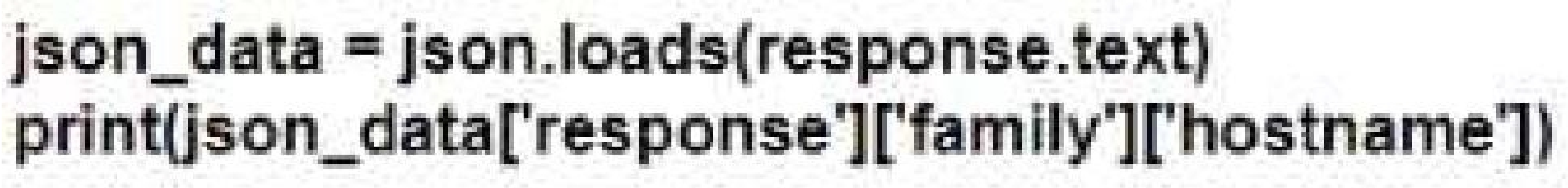
```
json_data = response.json()
print(json_data['response'][0]['hostname'])
```

C.



```
json_data = response.json()
print(json_data['response'][family][hostname'])
```

D.

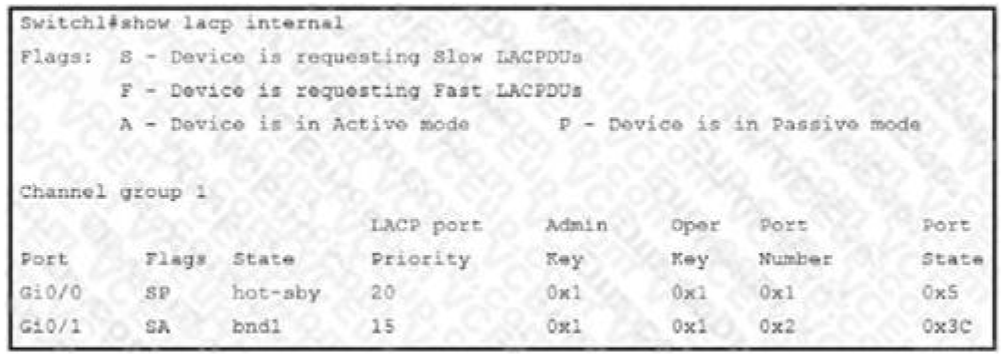


```
json_data = json.loads(response.text)
print(json_data['response']['family']['hostname'])
```

Correct Answer: D
Section:

QUESTION 243

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

An engineer attempts to bundle interface GiO/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

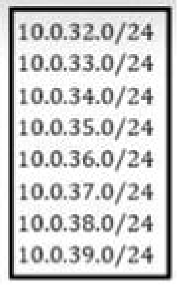
C. Enable fast LACP PDUs on interface Gi0/0.

D. Set LACP max-bundle to 2 on interface Port-channeM

Correct Answer: D
Section:

QUESTION 244

Refer to the exhibit.



10.0.32.0/24
10.0.33.0/24
10.0.34.0/24
10.0.35.0/24
10.0.36.0/24
10.0.37.0/24
10.0.38.0/24
10.0.39.0/24

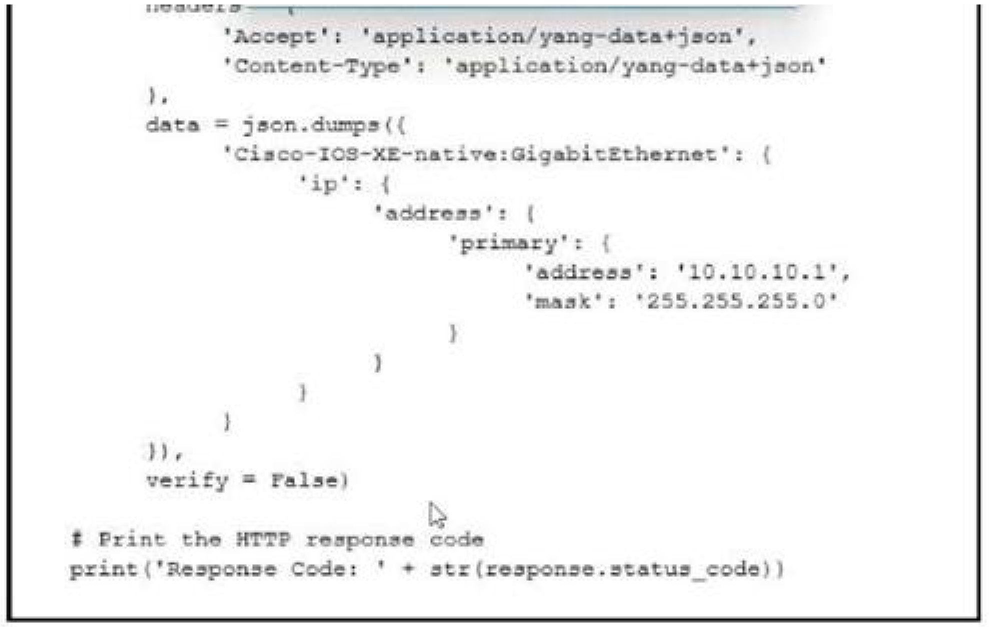
An engineer must permit traffic from these networks and block all other traffic An informational log message should be triggered when traffic enters from these prefixes Which access list must be used?

A. access-list acl_subnets permit ip 10.0.32.0 0 0.0.255 log
B. access-list acl_subnets permit ip 10.0.32.0 0.0.7.255 log
C. access-list acl_subnets permit ip 10.0.32.0 0.0.7.255 access-list acl_subnets deny ip any log
D. access-list acl_subnets permit ip 10.0.32.0 255.255.248.0 log

Correct Answer: B
Section:

QUESTION 245

Refer to the exhibit.



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

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

After the code is run on a Cisco IOS-XE router, the response code is 204.

What is the result of the script?

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

Correct Answer: D
Section:

QUESTION 246
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

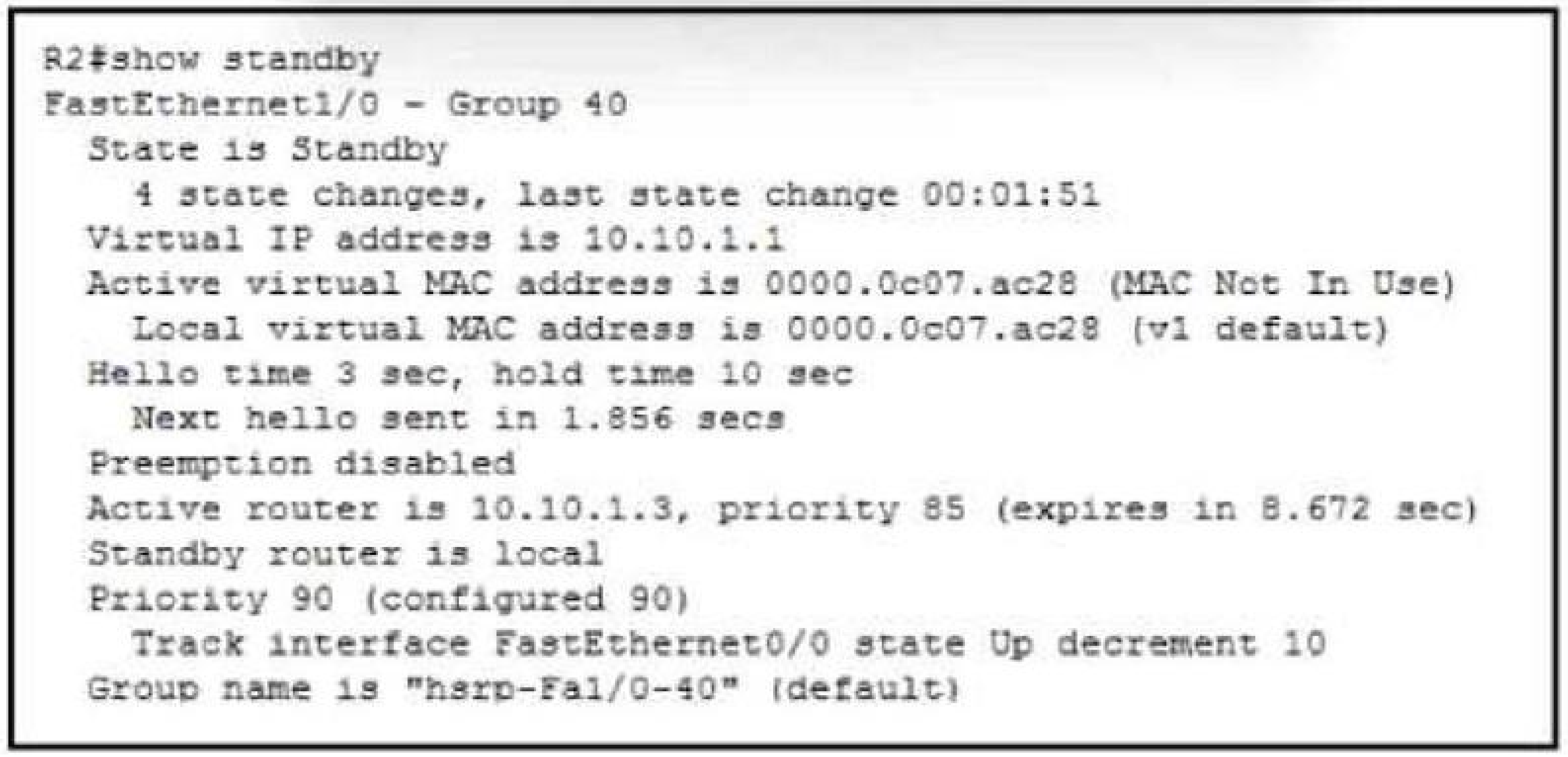
Correct Answer: A, C
Section:

QUESTION 247
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

Correct Answer: A, E
Section:

QUESTION 248
Refer to the exhibit.



```
R2#show standby
FastEthernet1/0 - Group 40
  State is Standby
    4 state changes, last state change 00:01:51
  Virtual IP address is 10.10.1.1
  Active virtual MAC address is 0000.0c07.ac28 (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac28 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.856 secs
  Preemption disabled
  Active router is 10.10.1.3, priority 85 (expires in 8.672 sec)
  Standby router is local
  Priority 90 (configured 90)
    Track interface FastEthernet0/0 state Up decrement 10
  Group name is "hsrp-Fa1/0-40" (default)
```

After configuring HSRP an engineer enters the show standby command. Which two facts are derived from the output? (Choose two.)

A. The router with IP 10.10 1.3 is active because it has a higher IP address

B. If Fa0/0 is shut down, the HSRP priority on R2 becomes 80

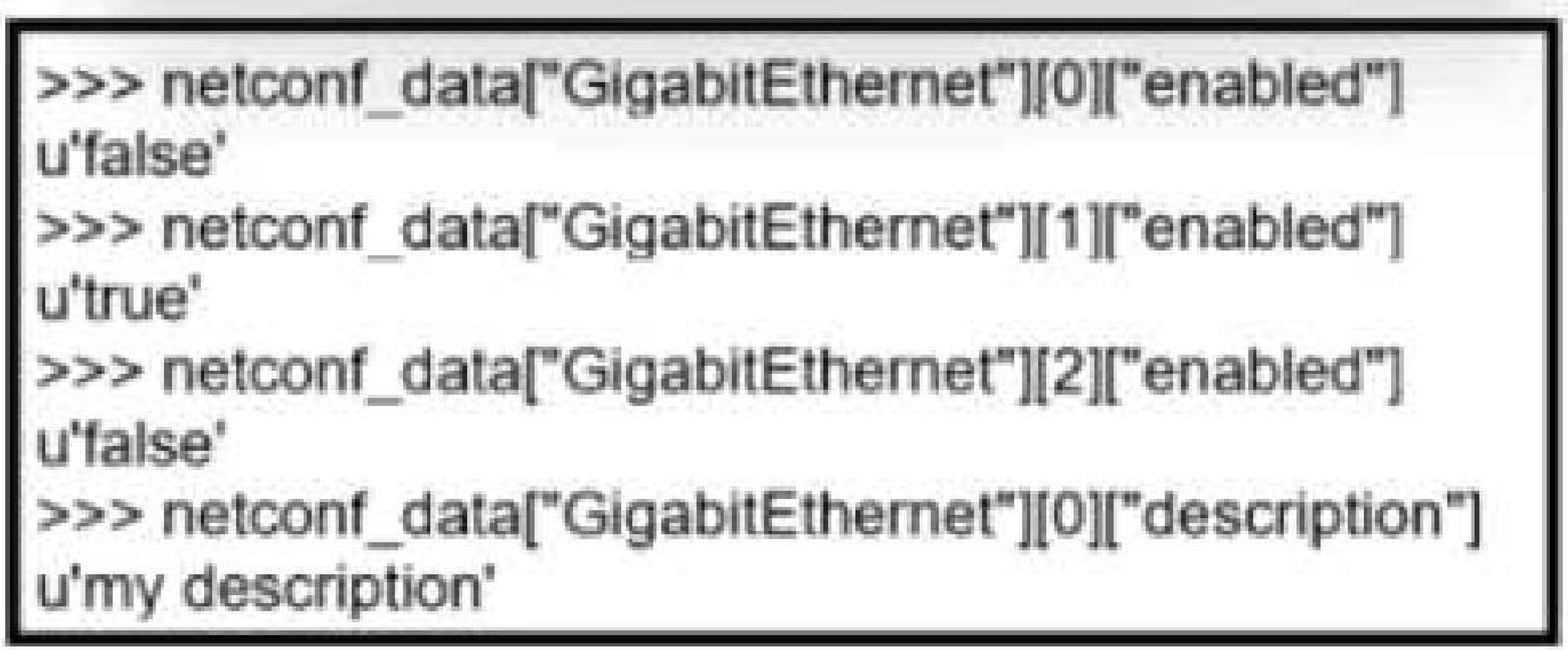
C. R2 Fa1/0 regains the primary role when the link comes back up

D. R2 becomes the active router after the hold time expires.

E. R2 is using the default HSRP hello and hold timers.

Correct Answer: D, E
Section:

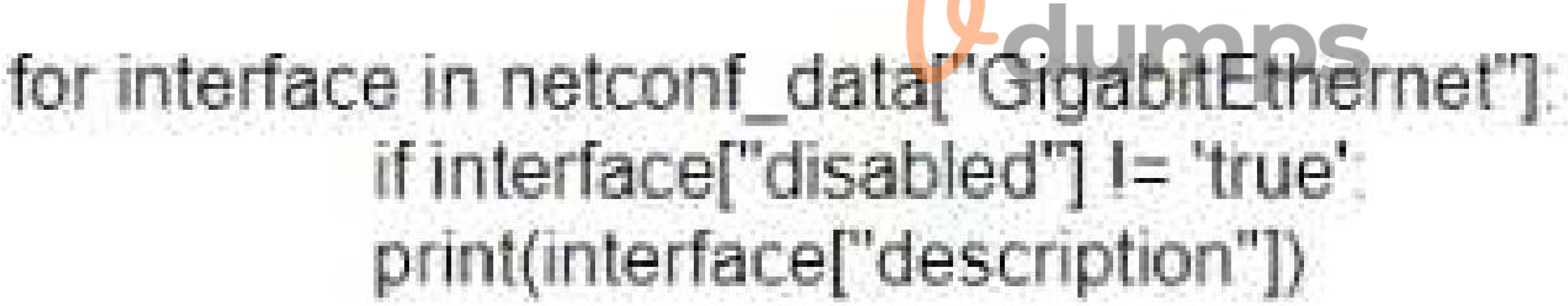
QUESTION 249
Refer to the exhibit.



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

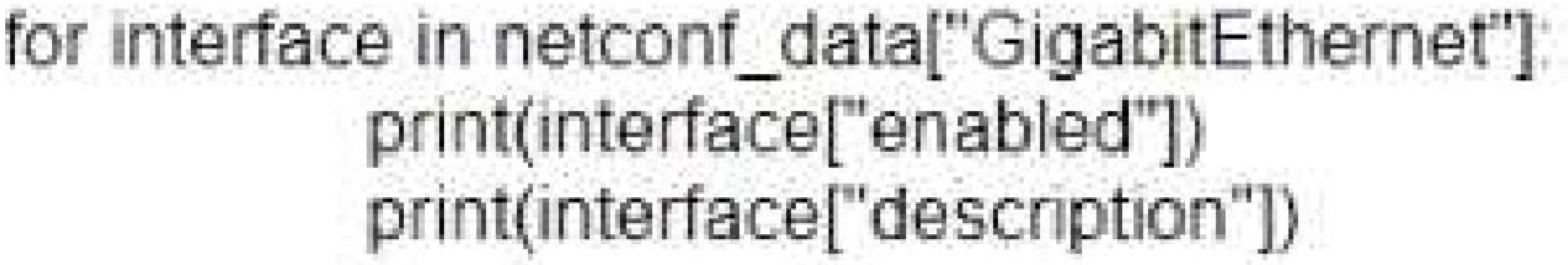
Which Python code snippet prints the descriptions of disabled interfaces only?

A.



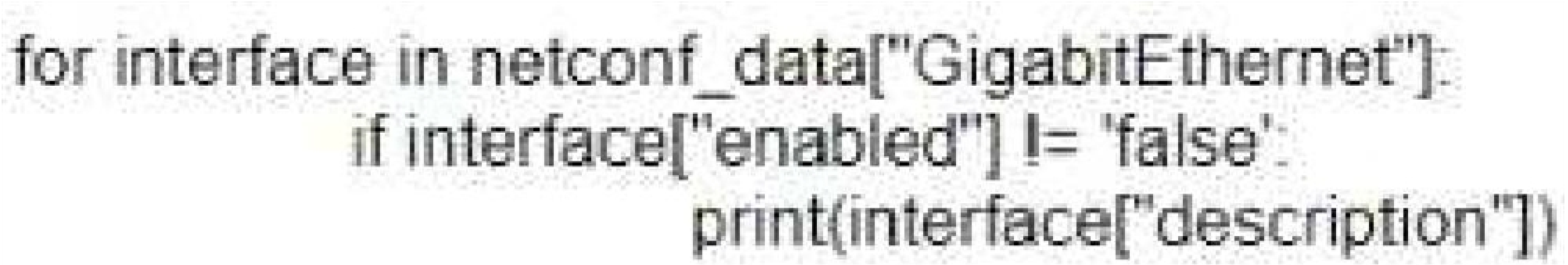
```
for interface in netconf_data["GigabitEthernet"]:
          if interface["disabled"] != 'true':
          print(interface["description"])
```

B.



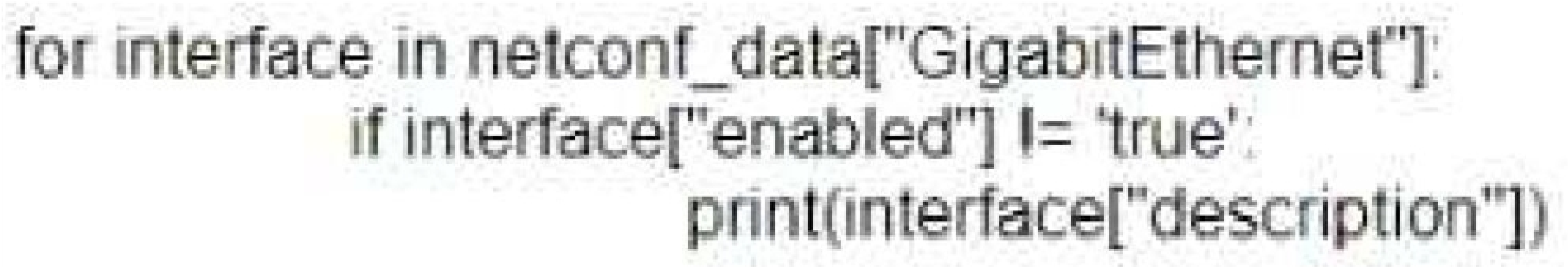
```
for interface in netconf_data["GigabitEthernet"]:
          print(interface["enabled"])
          print(interface["description"])
```

C.



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

D.



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

Correct Answer: D
Section:

QUESTION 250
When firewall capabilities are considered, which feature is found only in Cisco next-generation firewalls?

A. malware protection
B. stateful inspection
C. traffic filtering
D. active/standby high availability

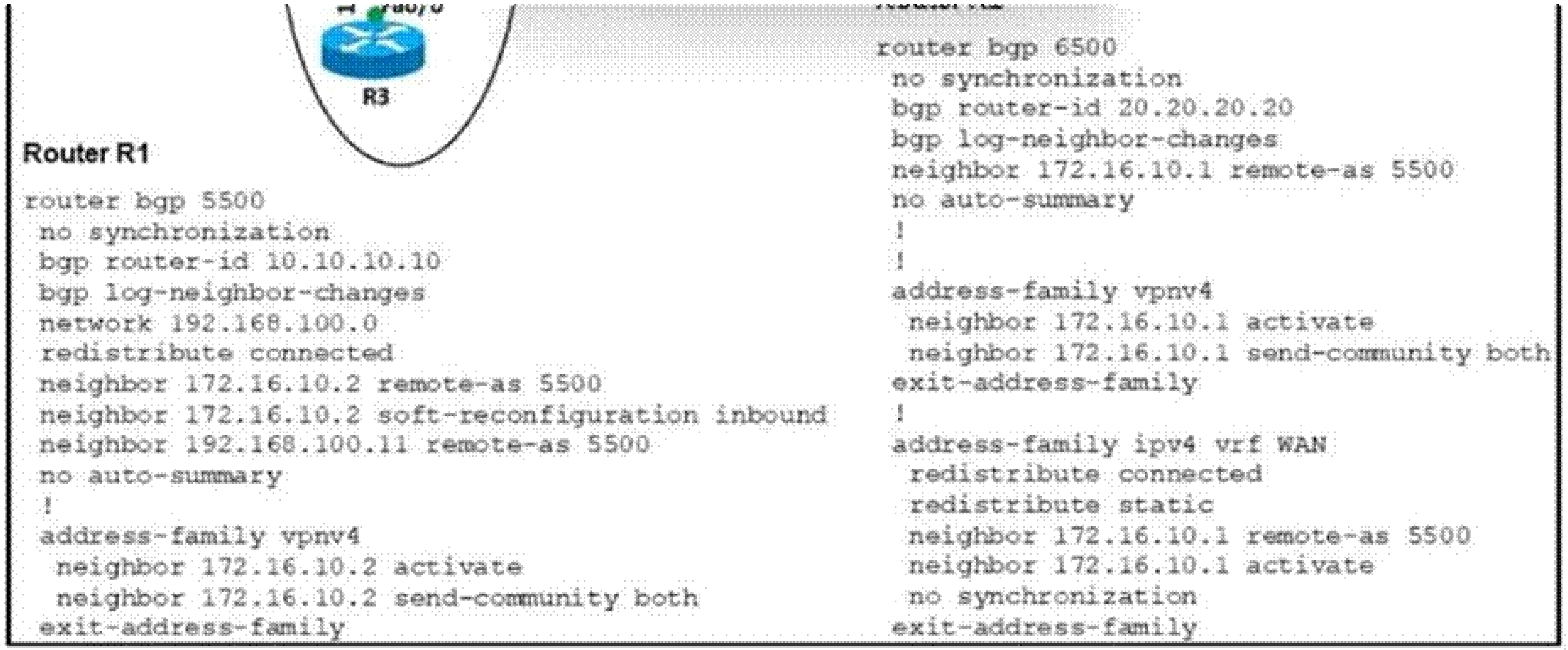
Correct Answer: A
Section:

QUESTION 251
What does a northbound API accomplish?

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

Correct Answer: A
Section:

QUESTION 252
Refer to the exhibit.



Router R1

```
router bgp 5500
 no synchronization
 bgp router-id 10.10.10.10
 bgp log-neighbor-changes
 network 192.168.100.0
 redistribute connected
 neighbor 172.16.10.2 remote-as 5500
 neighbor 172.16.10.2 soft-reconfiguration inbound
 neighbor 192.168.100.11 remote-as 5500
 no auto-summary
 !
 address-family vpnv4
  neighbor 172.16.10.2 activate
  neighbor 172.16.10.2 send-community both
 exit-address-family
```

```
router bgp 6500
 no synchronization
 bgp router-id 20.20.20.20
 bgp log-neighbor-changes
 neighbor 172.16.10.1 remote-as 5500
 no auto-summary
 !
 !
 address-family vpnv4
  neighbor 172.16.10.1 activate
  neighbor 172.16.10.1 send-community both
 exit-address-family
 !
 address-family ipv4 vrf WAN
  redistribute connected
  redistribute static
  neighbor 172.16.10.1 remote-as 5500
  neighbor 172.16.10.1 activate
  no synchronization
 exit-address-family
```

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

A. Change the network statement on R1 to 172.16 10.0

B. Change the remote-as number for 192 168.100.11.

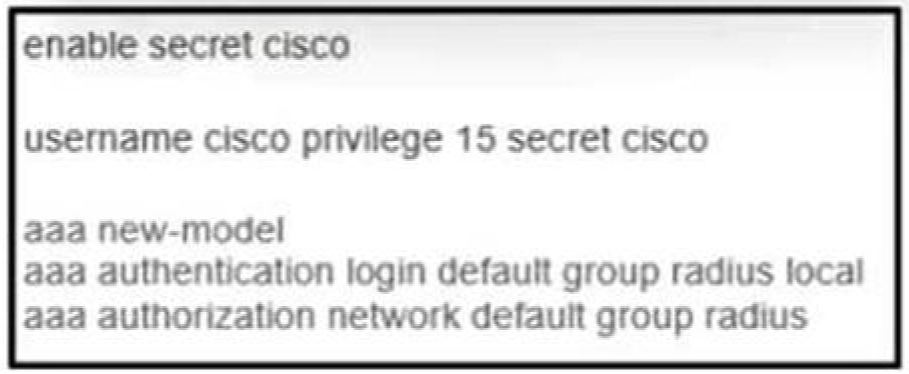
C. Enable synchronization on R1 and R2

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

Correct Answer: D
Section:

QUESTION 253

Refer to the exhibit.



```
enable secret cisco

username cisco privilege 15 secret cisco

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

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

A. aaa authorization exec default group radius none

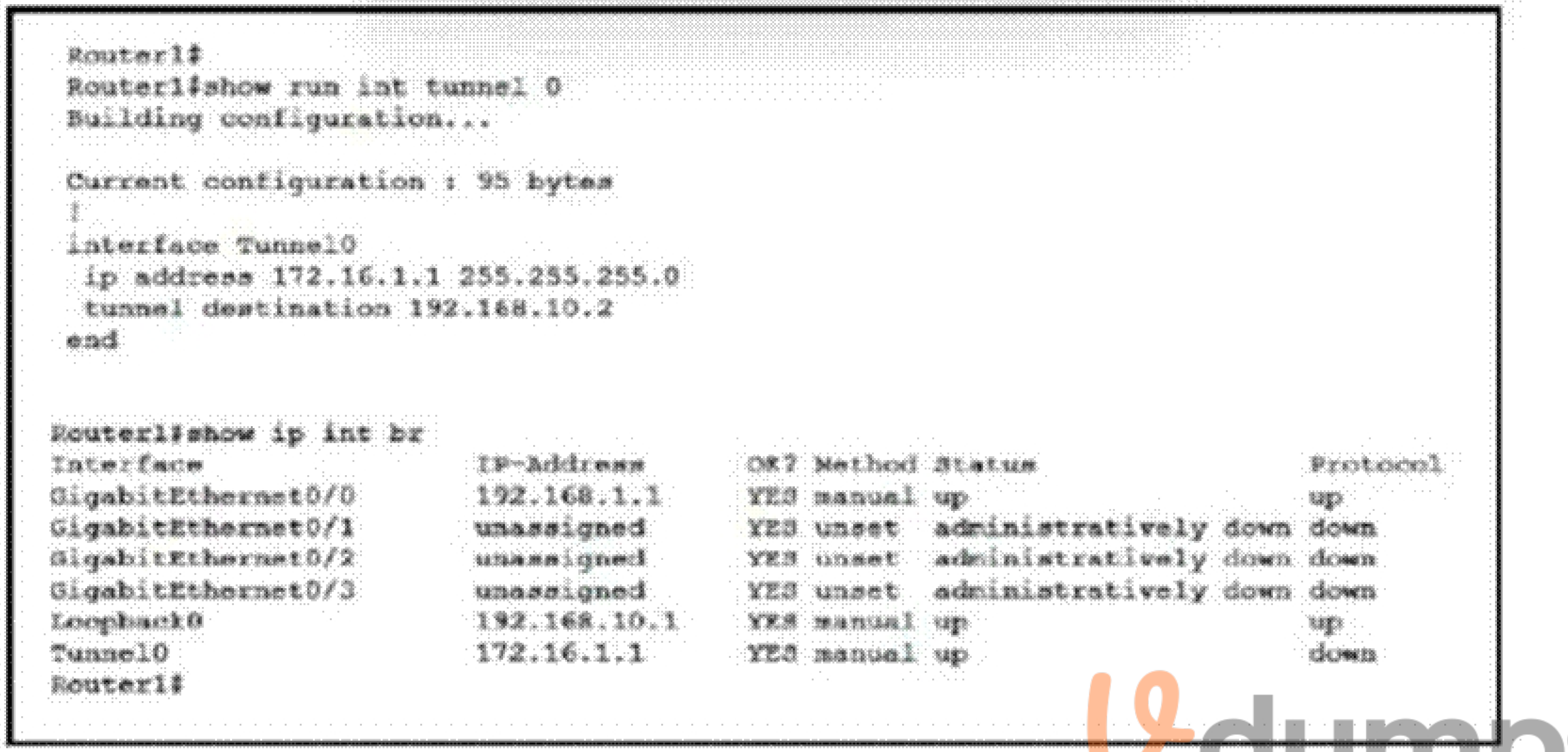
B. aaa authentication login default group radius local none

C. aaa authorization exec default group radius if-authenticated

D. aaa authorization exec default group radius

Correct Answer: C
Section:

QUESTION 254
Refer to the exhibit.



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

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


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

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

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

Correct Answer: B
Section:

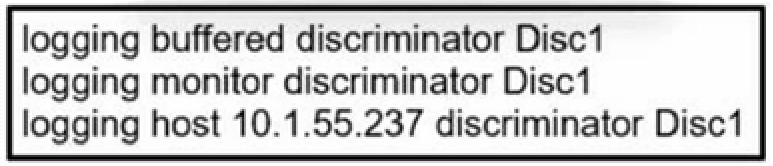
QUESTION 255
Which method is used by an AP to join HA controllers and is configured in NVRAM?

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

Correct Answer: A
Section:
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.

QUESTION 256

Refer to the exhibit.



```
logging buffered discriminator Disc1
logging monitor discriminator Disc1
logging host 10.1.55.237 discriminator Disc1
```

A network engineer is enabling logging to a local buffer, to the terminal and to a syslog server for all debugging level logs filtered by facility code 7. Which command is needed to complete this configuration snippet?

A. logging buffered debugging

B. logging discriminator Disc1 severity includes 7

C. logging buffered discriminator Disc1 debugging

D. logging discriminator Disc1 severity includes 7 facility includes fac7

Correct Answer: D

Section:

QUESTION 257

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

Correct Answer: B

Section:

QUESTION 258

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

Correct Answer: A

Section:

Explanation:

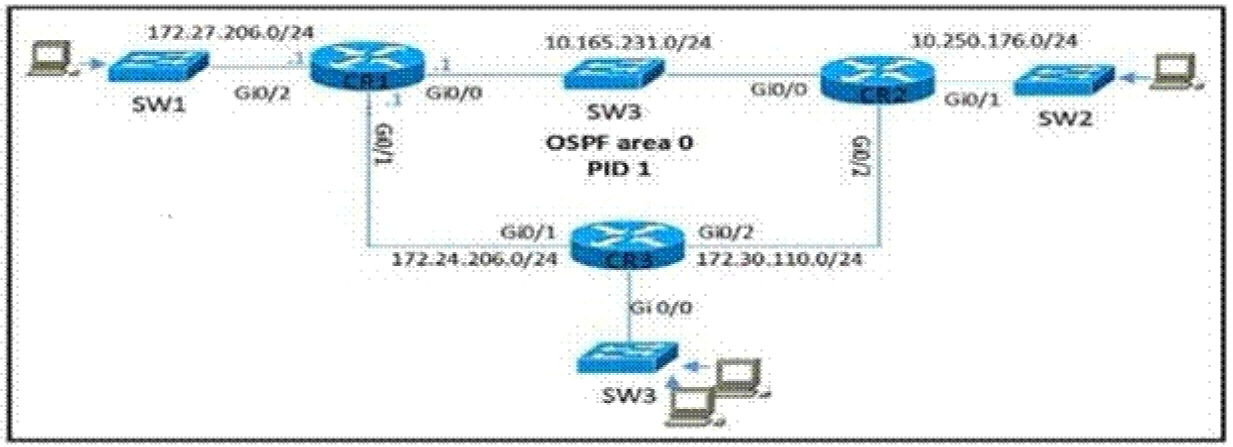
The Design area is where you create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network. Use the Design workflow if you do not already have an existing infrastructure. If you have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

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-andmanagement/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 requiresdevelopment from a clean slate – no legacy code around. It is an approach used when you're startingfresh and with no restrictions or dependencies."

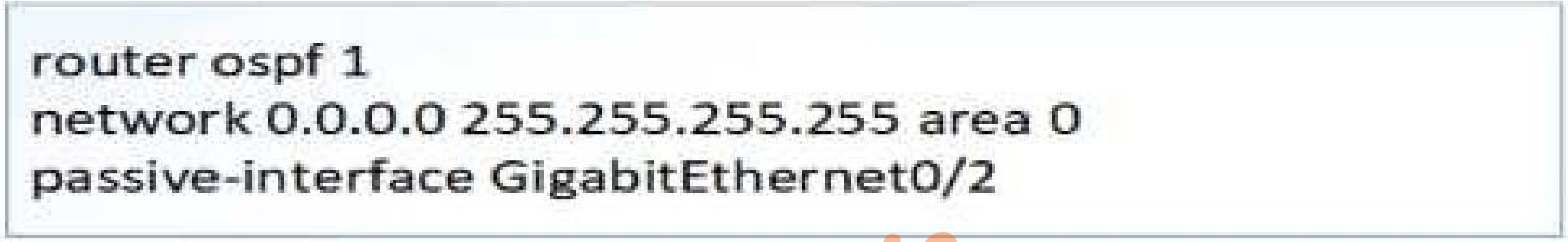
QUESTION 259

Refer to the exhibit.



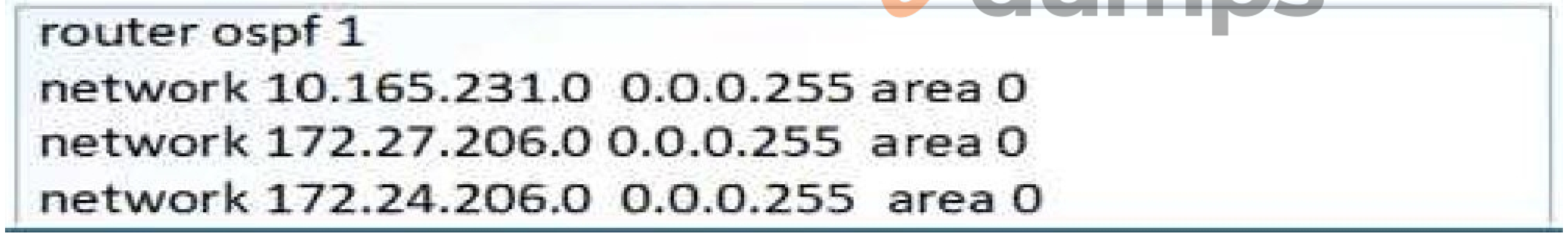
CR2 and CR3 ate configured with OSPF. Which configuration, when applied to CR1. allows CR1 to exchange OSPF Information with CR2 and CR3 but not with other network devices or on new Interfaces that are added to CR1?

A.



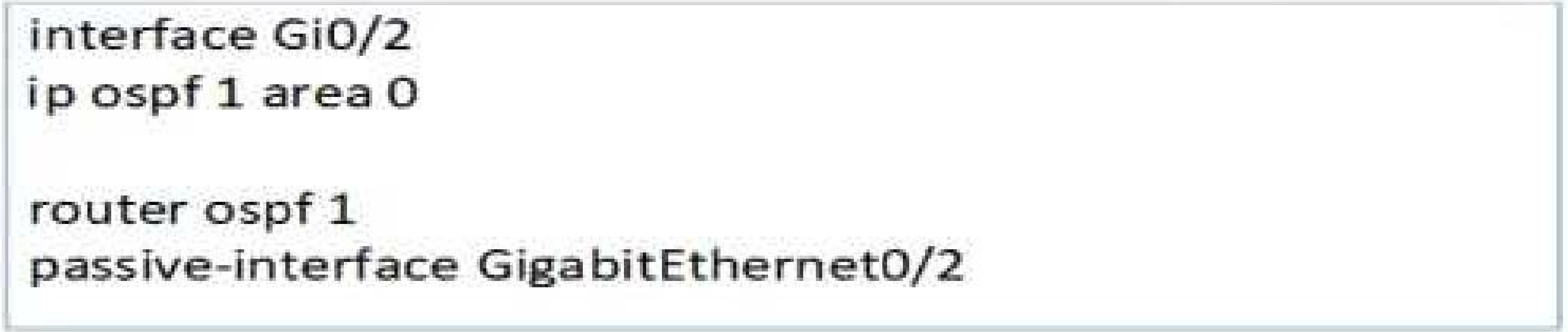
```
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
passive-interface GigabitEthernet0/2
```

B.



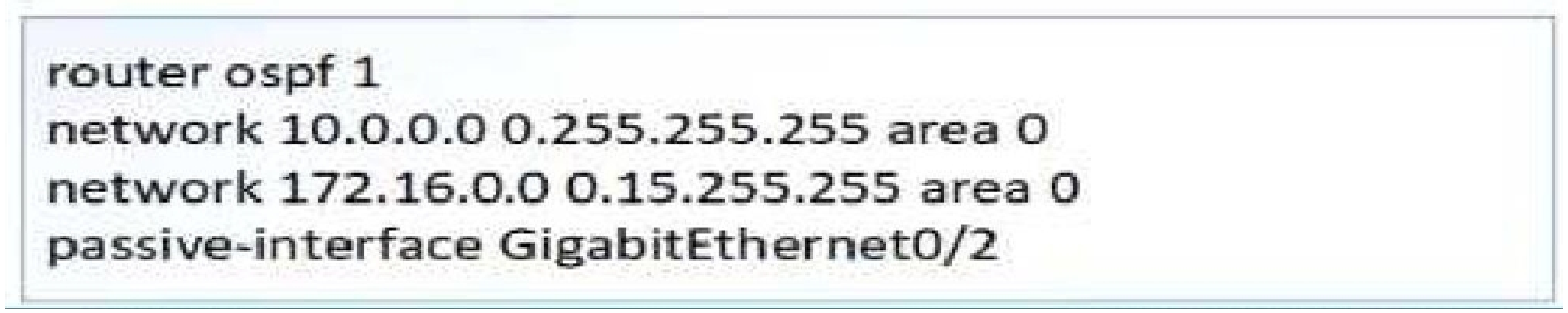
```
router ospf 1
network 10.165.231.0  0.0.0.255 area 0
network 172.27.206.0 0.0.0.255  area 0
network 172.24.206.0  0.0.0.255   area 0
```

C.



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

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

D.

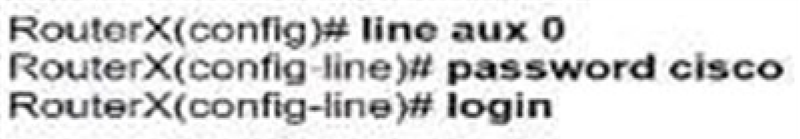


```
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
network 172.16.0.0 0.15.255.255 area 0
passive-interface GigabitEthernet0/2
```

Correct Answer: D
Section:

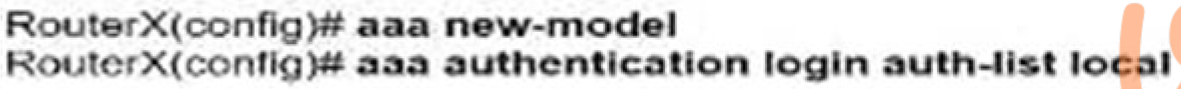
QUESTION 260
An administrator must enable Telnet access to Router X using the router username and password database for authentication. Which configuration should be applied?

A.



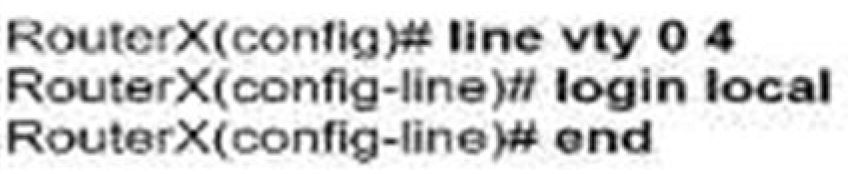
```
RouterX(config)# line aux 0
RouterX(config-line)# password cisco
RouterX(config-line)# login
```

B.



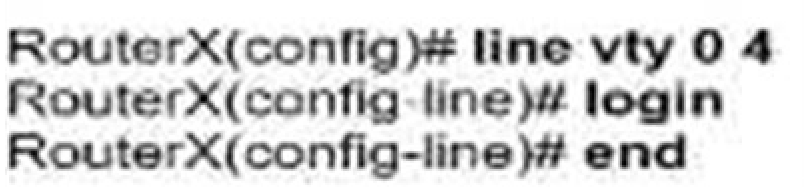
```
RouterX(config)# aaa new-model
RouterX(config)# aaa authentication login auth-list local
```

C.



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

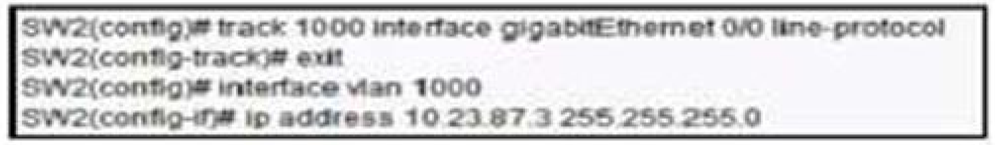
D.



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

Correct Answer: D
Section:

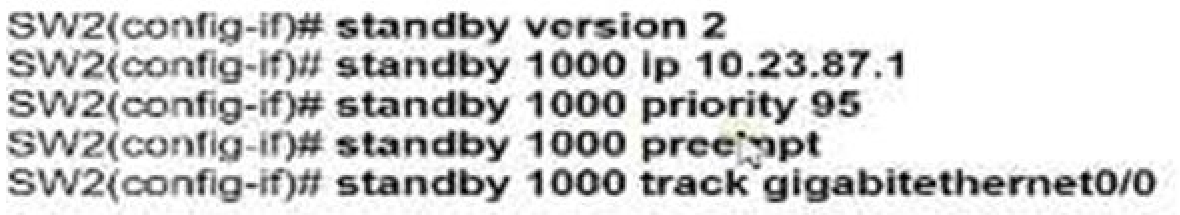
QUESTION 261
Refer to the exhibit.



```
SW2(config)# track 1000 interface gigabitEthernet 0/0 line-protocol
SW2(config-track)# exit
SW2(config)# interface vlan 1000
SW2(config-if)# ip address 10.23.87.3 255.255.255.0
```

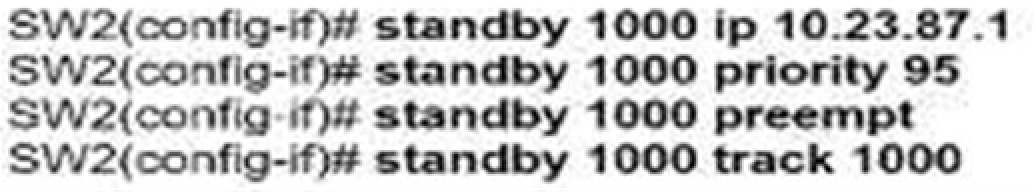
An engineer must configure HSRP for VLAN 1000 on SW2. The secondary switch must immediately take over the role of active router If the interlink with the primary switch fails. Which command set completes this task?

A.



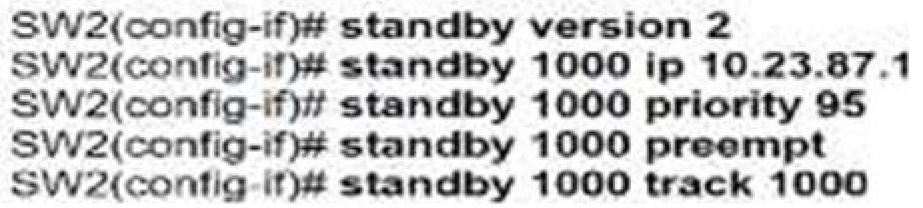
```
SW2(config-if)# standby version 2
SW2(config-if)# standby 1000 ip 10.23.87.1
SW2(config-if)# standby 1000 priority 95
SW2(config-if)# standby 1000 preempt
SW2(config-if)# standby 1000 track gigabitethernet0/0
```

B.



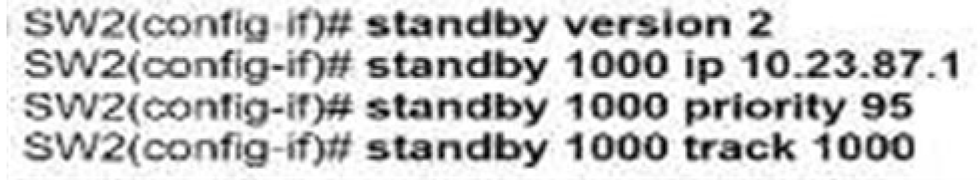
```
SW2(config-if)# standby 1000 ip 10.23.87.1
SW2(config-if)# standby 1000 priority 95
SW2(config-if)# standby 1000 preempt
SW2(config-if)# standby 1000 track 1000
```

C.



```
SW2(config-if)# standby version 2
SW2(config-if)# standby 1000 ip 10.23.87.1
SW2(config-if)# standby 1000 priority 95
SW2(config-if)# standby 1000 preempt
SW2(config-if)# standby 1000 track 1000
```

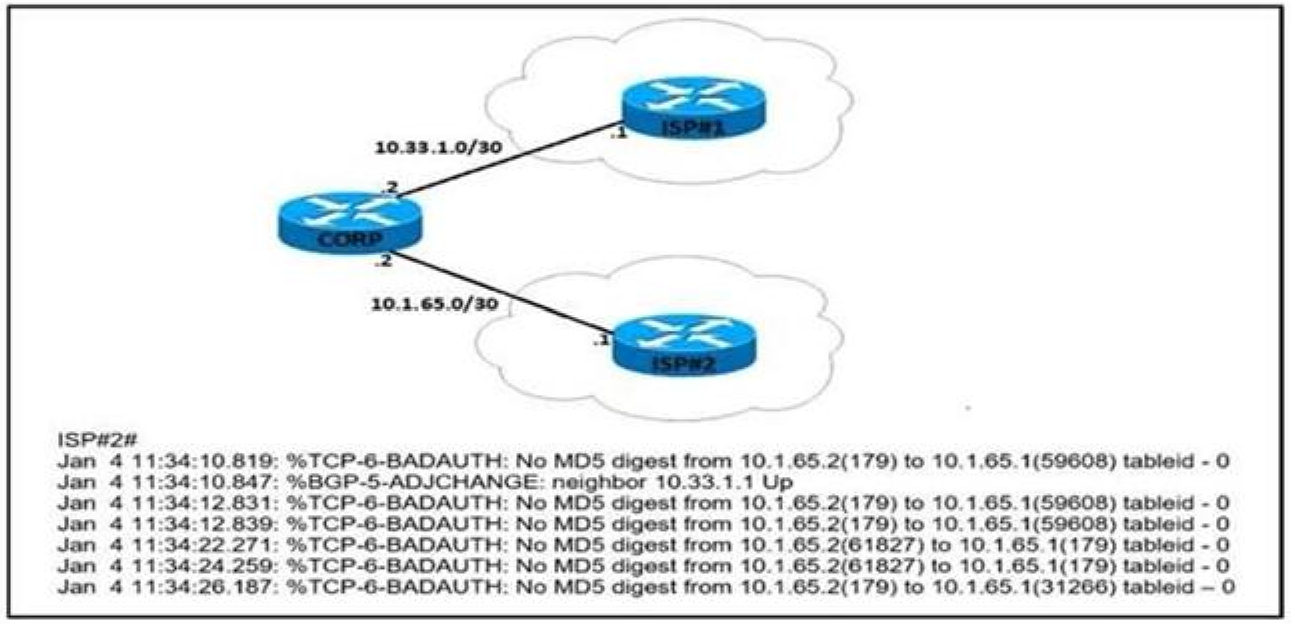
D.



```
SW2(config-if)# standby version 2
SW2(config-if)# standby 1000 ip 10.23.87.1
SW2(config-if)# standby 1000 priority 95
SW2(config-if)# standby 1000 track 1000
```

Correct Answer: C
Section:

QUESTION 262
Refer to the exhibit.



```
ISP#2#
Jan  4 11:34:10.819: %TCP-6-BADAUTH: No MD5 digest from 10.1.65.2(179) to 10.1.65.1(59608) tableid - 0
Jan  4 11:34:10.847: %BGP-5-ADJCHANGE: neighbor 10.33.1.1 Up
Jan  4 11:34:12.831: %TCP-6-BADAUTH: No MD5 digest from 10.1.65.2(179) to 10.1.65.1(59608) tableid - 0
Jan  4 11:34:12.839: %TCP-6-BADAUTH: No MD5 digest from 10.1.65.2(179) to 10.1.65.1(59608) tableid - 0
Jan  4 11:34:22.271: %TCP-6-BADAUTH: No MD5 digest from 10.1.65.2(61827) to 10.1.65.1(179) tableid - 0
Jan  4 11:34:24.259: %TCP-6-BADAUTH: No MD5 digest from 10.1.65.2(61827) to 10.1.65.1(179) tableid - 0
Jan  4 11:34:26.187: %TCP-6-BADAUTH: No MD5 digest from 10.1.65.2(179) to 10.1.65.1(31266) tableid – 0
```

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

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

Correct Answer: B
Section:

QUESTION 263
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.

Correct Answer: C, E
Section:

QUESTION 264
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. scalable. hub-and-spoke topology.

Correct Answer: C, D
Section:
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 serviceside 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-sdwanapplication-awarerouting-deploy-guide.html

QUESTION 265

How does CEF switching differ from process switching on Cisco devices?

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

Correct Answer: B
Section:
Explanation:
Cisco Express Forwarding (CEF) switching is a proprietary form of scalable switching intended to tackle the problems associated with demand caching. With CEF switching, the information which is conventionally stored in a route cache is split up over several data structures. The CEF code is able to maintain these data structures in the Gigabit Route Processor (GRP), and also in slave processors such as the line cards in the 12000 routers. The data structures that provide optimized lookup for efficient packet forwarding include:
The Forwarding Information Base (FIB) table - CEF uses a FIB to make IP destination prefix-based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and these changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table.
Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for route cache maintenance that is associated with switching paths such as fast switching and optimum switching.
Adjacency table - Nodes in the network are said to be adjacent if they can reach each other with a single hop across a link layer. In addition to the FIB, CEF uses adjacency tables to prepend Layer 2 addressing information. The adjacency table maintains Layer 2 next-hop addresses for all FIB entries.
CEF can be enabled in one of two modes:
Central CEF mode - When CEF mode is enabled, the CEF FIB and adjacency tables reside on the route processor, and the route processor performs the express forwarding. You can use CEF mode when line cards are not available for
CEF switching, or when you need to use features not compatible with distributed CEF switching.
Distributed CEF (dCEF) mode - When dCEF is enabled, line cards maintain identical copies of the FIB and adjacency tables. The line cards can perform the express forwarding by themselves, relieving the main processor - Gigabit Route
Processor (GRP) - of involvement in the switching operation. This is the only switching method available on the Cisco 12000 Series Router. dCEF uses an Inter-Process Communication (IPC) mechanism to ensure synchronization of FIBs and adjacency tables on the route processor and line cards.
For more information about CEF switching, see Cisco Express Forwarding (CEF) White Paper.

QUESTION 266
A customer wants to provide wireless access to contractors using a guest portal on Cisco ISE. The portal Is also used by employees A solution is implemented, but contractors receive a certificate error when they attempt to access the portal
Employees can access the portal without any errors.
Which change must be implemented to allow the contractors and employees to access the portal?

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

Correct Answer: C
Section:

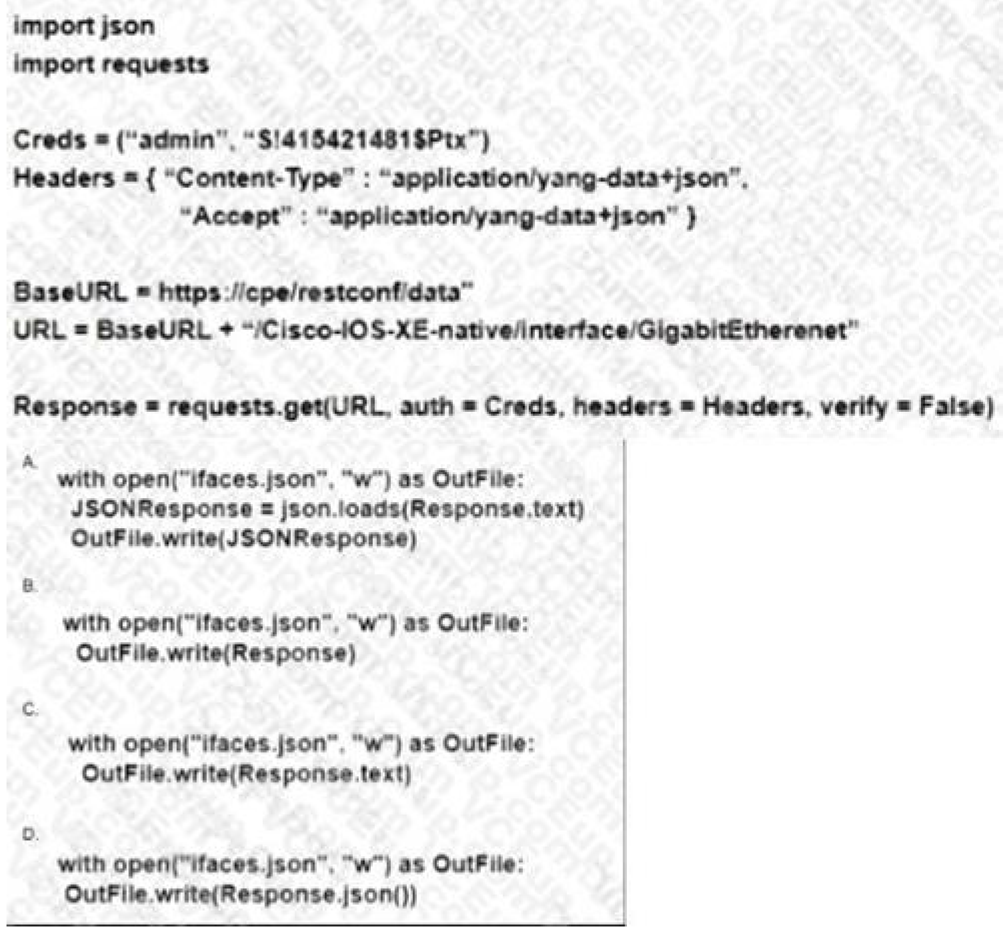
QUESTION 267
A client device roams between access points located on different floors in an atrium. The access points are Joined to the same controller and configured in local mode. The access points are in different AP groups and have different IP addresses, but the client VLAN in the groups is the same.
Which type of roam occurs?

A. inter-controller

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

Correct Answer: D
Section:
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_CONSOLIDA TED_chapter_01100.htmlIn three types of client roaming above, only with Inter- Subnet Roaming thecontrollers are in different subnets.

QUESTION 268
Which Python code snippet must be added to the script to save the returned configuration as a JSONformatted file?



```
import json
import requests

Creds = ("admin", "S!415421481$Ptx")
Headers = { "Content-Type" : "application/yang-data+json",
            "Accept" : "application/yang-data+json" }

BaseURL = https://cpe/restconf/data"
URL = BaseURL + "/Cisco-IOS-XE-native/interface/GigabitEtherenet"

Response = requests.get(URL, auth = Creds, headers = Headers, verify = False)
```

A.
```
with open("ifaces.json", "w") as OutFile:
  JSONResponse = json.loads(Response.text)
  OutFile.write(JSONResponse)
```

B.
```
with open("ifaces.json", "w") as OutFile:
  OutFile.write(Response)
```

C.
```
with open("ifaces.json", "w") as OutFile:
  OutFile.write(Response.text)
```

D.
```
with open("ifaces.json", "w") as OutFile:
  OutFile.write(Response.json())
```

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

Correct Answer: C
Section:

QUESTION 269
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

Correct Answer: A
Section:
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

QUESTION 270
What is one difference between EIGRP and OSPF?

A. OSPF is a Cisco proprietary protocol, and EIGRP is an IETF open standard protocol.
B. OSPF uses the DUAL distance vector algorithm, and EIGRP uses the Dijkstra link-state algorithm
C. EIGRP uses the variance command lot unequal cost load balancing, and OSPF supports unequal cost balancing by default.
D. EIGRP uses the DUAL distance vector algorithm, and OSPF uses the Dijkstra link-state algorithm

Correct Answer: D
Section:
Explanation:
EIGRP is based on DUAL (Diffusing Update Algorithm) while OSPF uses Dijkstra's Shortest Path Algorithm with the major difference in how they calculate the shortest routing path.
OSPF has capability to calculate the best shortest path to each reachable subnet/network using an algorithm called SFP (Shortest Path First) also known as Dijkstra algorithm. "Neighbor Table" that contain all discovered OSPF neighbour with whom routing information will be interchanged.

QUESTION 271
Why would a log file contain a * next to the date?

A. The network device was receiving NTP time when the log messages were recorded.
B. The network device was unable to reach The NTP server when the log messages were recorded
C. The network device is not configured to use NTP.

D. The network device is nor configured to use NTP time stamps for logging

Correct Answer: B
Section:

QUESTION 272
Which action is performed by Link Management Protocol in a Cisco StackWise Virtual domain?

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

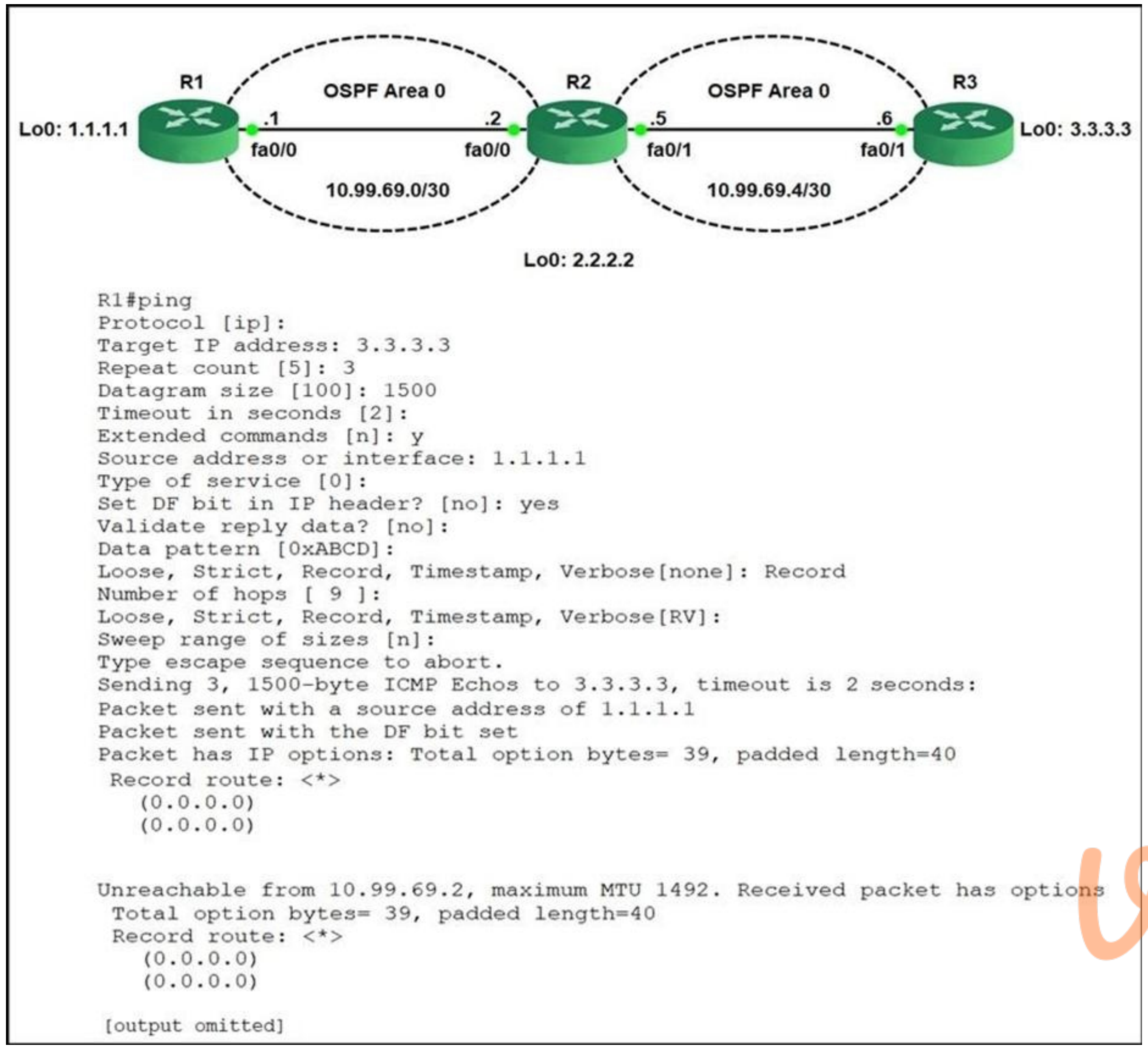
Correct Answer: A
Section:
Explanation:
The Link Management Protocol (LMP) performs the following functions: + Verifies link integrity by establishing bidirectional traffic forwarding, and rejects any unidirectional links + Exchanges periodic hellos to monitor and maintain the health of the links + Negotiates the version of StackWise Virtual header between the switches StackWise Virtual link role resolution
Reference: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-stack-wp-cte-en.html

QUESTION 273
A customer transitions a wired environment to a Cisco SD-Access solution. The customer does not want to integrate the wireless network with the fabric. Which wireless deployment approach enables the two systems to coexist and meets the customer requirement?

A. Deploy the APs in autonomous mode
B. Deploy the wireless network over the top of the fabric
C. Deploy a separate network for the wireless environment
D. Implement a Cisco DNA Center to manage the two networks

Correct Answer: B
Section:

QUESTION 274
Refer to the exhibit.



```
R1#ping
Protocol [ip]:
Target IP address: 3.3.3.3
Repeat count [5]: 3
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 1.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]: yes
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: Record
Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
Packet sent with the DF bit set
Packet has IP options: Total option bytes= 39, padded length=40
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)


Unreachable from 10.99.69.2, maximum MTU 1492. Received packet has options
 Total option bytes= 39, padded length=40
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)

 [output omitted]
```

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

A. The DF bit has been set

B. The maximum packet size accepted by the command is 147G bytes

C. R2 and R3 do not have an OSPF adjacency

D. R3 is missing a return route to 10.99.69.0/30

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

QUESTION 275
A network engineer is configuring OSPF on a router. The engineer wants to prevent having a route to 177.16.0.0/16 learned via OSPF. In the routing table and configures a prefix list using the command ip prefix-list OFFICE seq S deny
172.16.0.0/16. Winch two identical configuration commands must be applied to accomplish the goal? (Choose two.)

A. distribute-list prefix OFFICE in under the OSPF process

B. Ip prefix-list OFFICE seq 10 permit 0.0.0.0/0 Ie 32
C. ip prefix-list OFFICE seq 10 permit 0.0.0.0/0 ge 32
D. distribute-list OFFICE out under the OSPF process
E. distribute-list OFFICE in under the OSPF process

Correct Answer: A, B
Section:

QUESTION 276
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

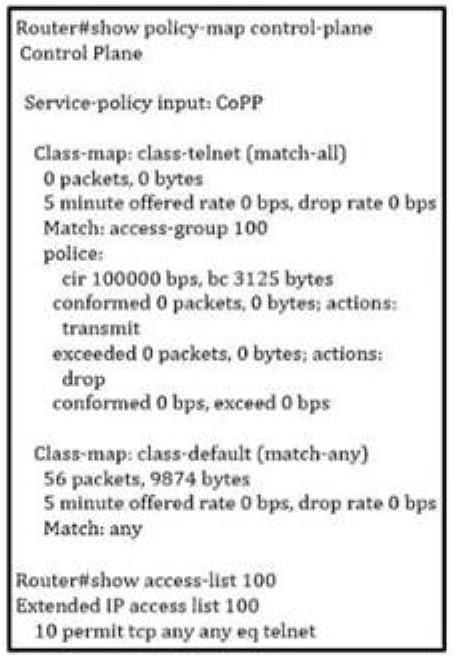
Correct Answer: A
Section:
Explanation:
Fabric Enabled WLC:
Fabric enabled WLC is integrated with LISP control plane. This WLC is responsible for AP image /Config, Radio Resource Management, Client Session management and roaming and all other wireless control plane functions.
For WLC Fabric Integration:
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

QUESTION 277
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

Correct Answer: D
Section:
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.

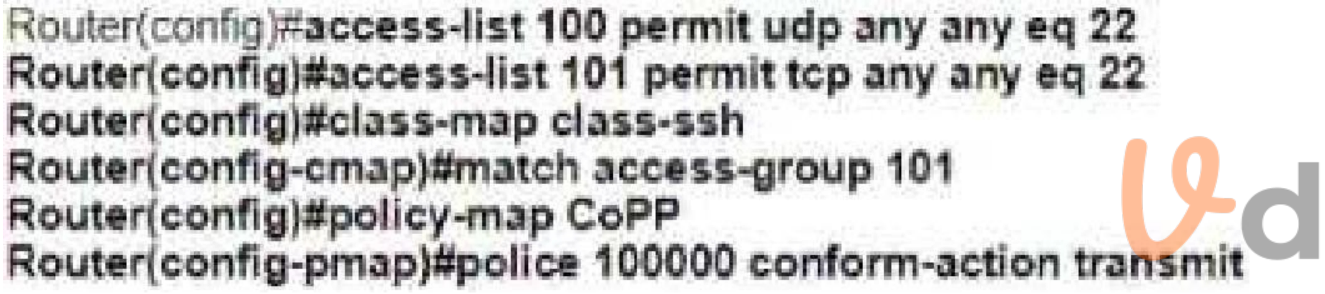
QUESTION 278
Refer to the exhibit.



```
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
```

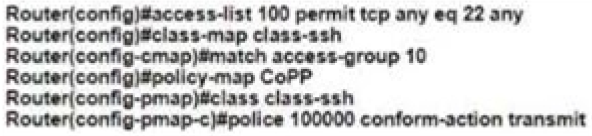
Which commands are required to allow SSH connection to the router?

A.



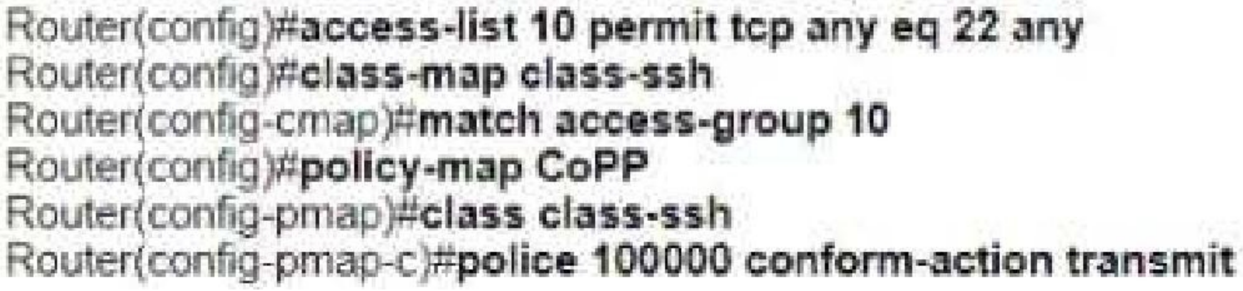
```
Router(config)#access-list 100 permit udp any any eq 22
Router(config)#access-list 101 permit tcp any any eq 22
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 101
Router(config)#policy-map CoPP
Router(config-pmap)#police 100000 conform-action transmit
```

B.



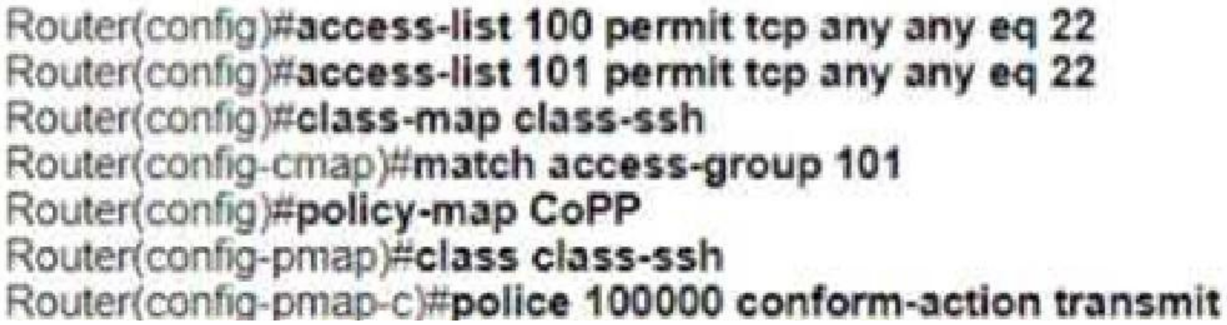
```
Router(config)#access-list 100 permit tcp any eq 22 any
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 10
Router(config)#policy-map CoPP
Router(config-pmap)#class class-ssh
Router(config-pmap-c)#police 100000 conform-action transmit
```

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
```

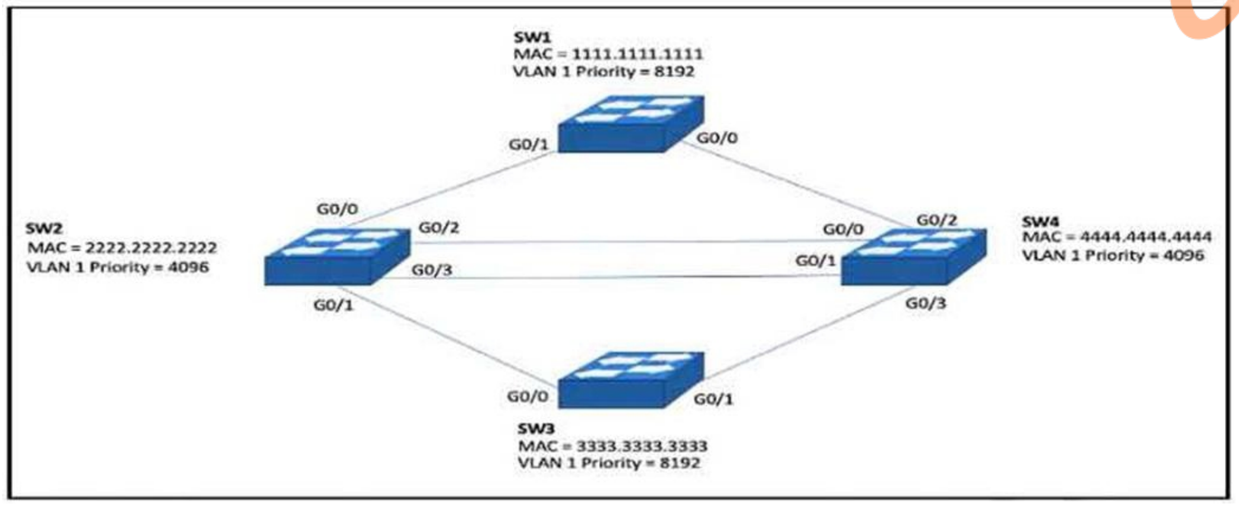
Correct Answer: D
Section:

QUESTION 279
Which two solutions are used for backing up a Cisco DNA Center Assurance database? (Choose two)

A. NFS share
B. non-linux server
C. local server
D. remote server
E. bare metal server

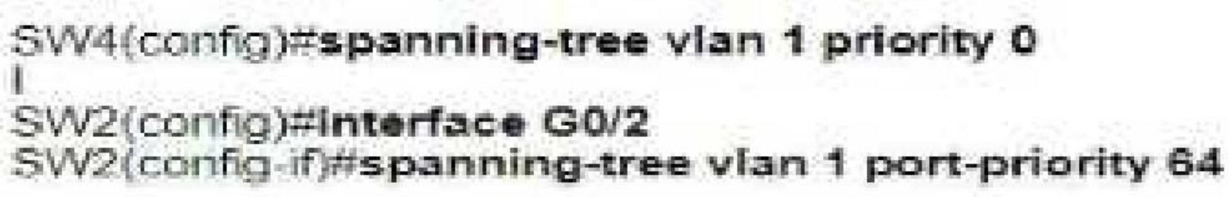
Correct Answer: A, E
Section:
Explanation:
Cisco DNA Center creates the backup files and posts them to a remote server. Each backup is uniquely stored using the UUID as the directory name.To support Assurance data backups, the server must be a Linux-based NFS server that meets the following requirements:
– Support NFS v4 and NFS v3.
– Cisco DNA Center stores backup copies of Assurance data on an external NFS device and automation data on an external remote sync (rsync) target location.
– The remote share for backing up an Assurance database (NDP) must be an NFS share.
Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/networkautomation-and-management/dna-center/2-1-2/admin_guide/b_cisco_dna_center_admin_guide_2_1_2/
b_cisco_dna_center_admin_guide_2_1_1_chapter_0110.html

QUESTION 280
Refer the exhibit.



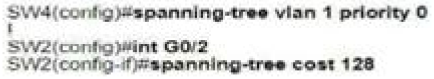
Which configuration elects SW4 as the root bridge for VLAN 1 and puts G0/2 on SW2 into a blocking state?

A.



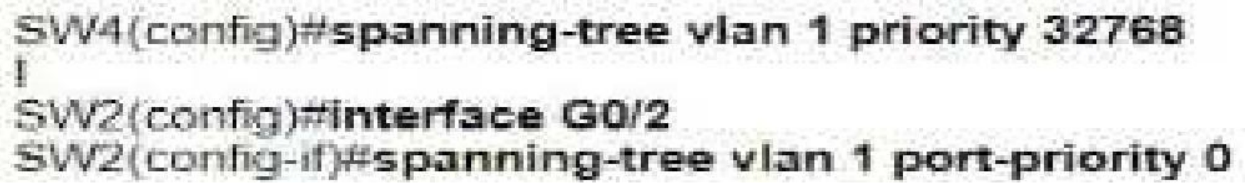
```
SW4(config)#spanning-tree vlan 1 priority 0
!
SW2(config)#interface G0/2
SW2(config-if)#spanning-tree vlan 1 port-priority 64
```

B.



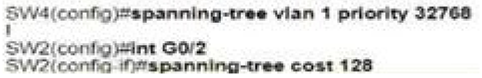
```
SW4(config)#spanning-tree vlan 1 priority 0
!
SW2(config)#int G0/2
SW2(config-if)#spanning-tree cost 128
```

C.



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

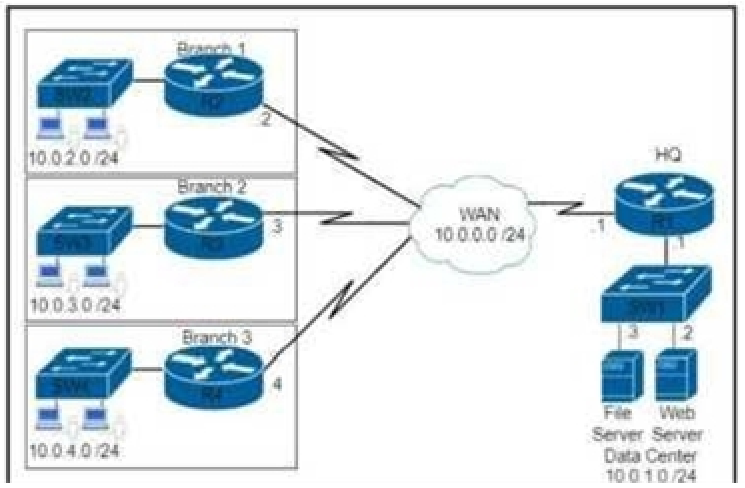
D.



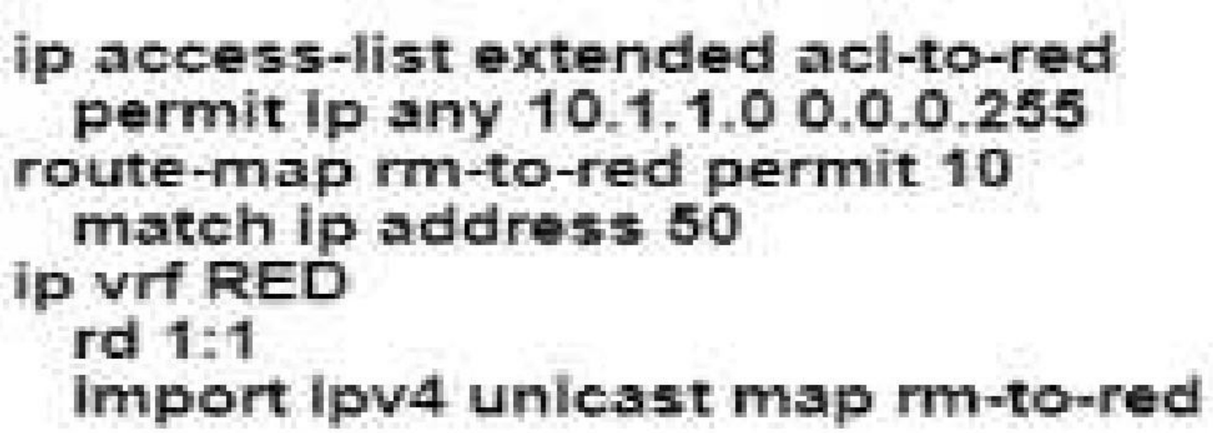
```
SW4(config)#spanning-tree vlan 1 priority 32768
!
SW2(config)#int G0/2
SW2(config-if)#spanning-tree cost 128
```

Correct Answer: B
Section:

QUESTION 281
An engineer must configure a router to leak routes between two VRFs Which configuration must the engineer apply?

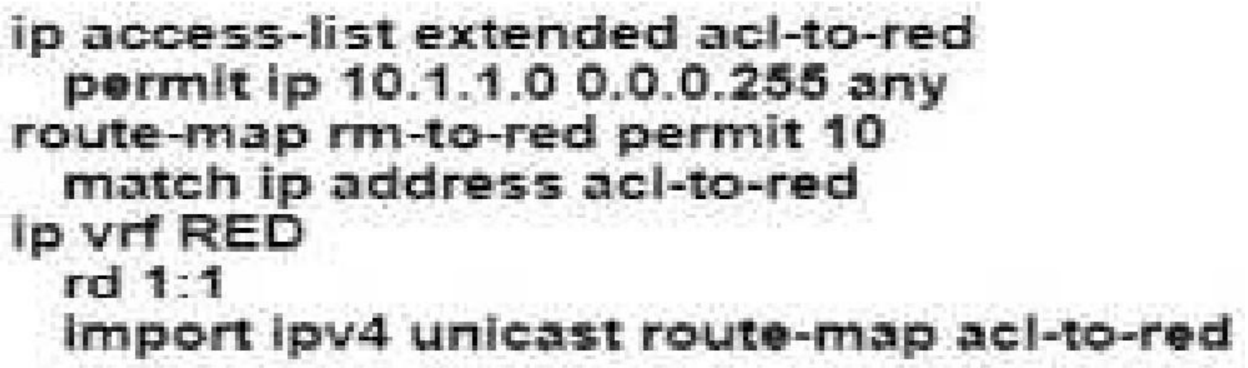


A.



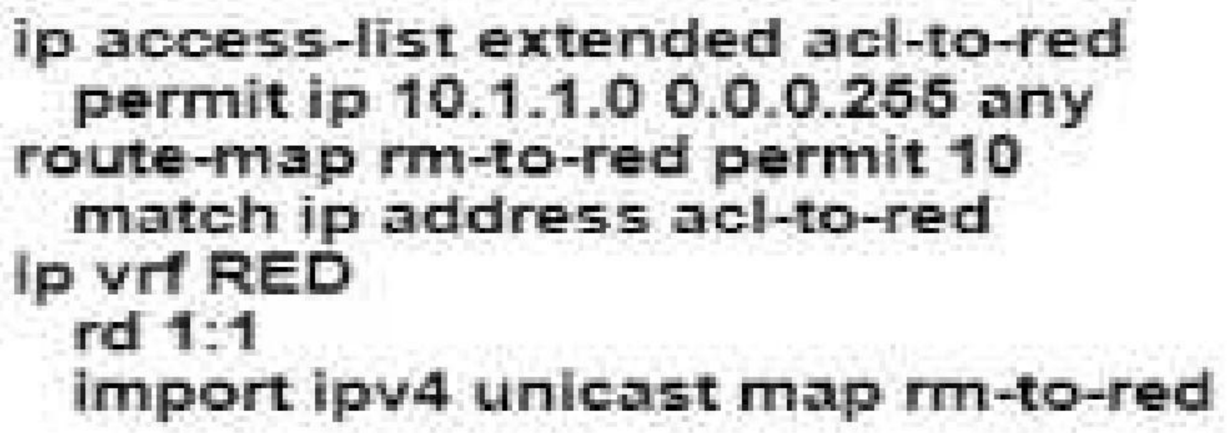
```
ip access-list extended acl-to-red
   permit ip any 10.1.1.0 0.0.0.255
route-map rm-to-red permit 10
   match ip address 50
ip vrf RED
   rd 1:1
   import ipv4 unicast map rm-to-red
```

B.



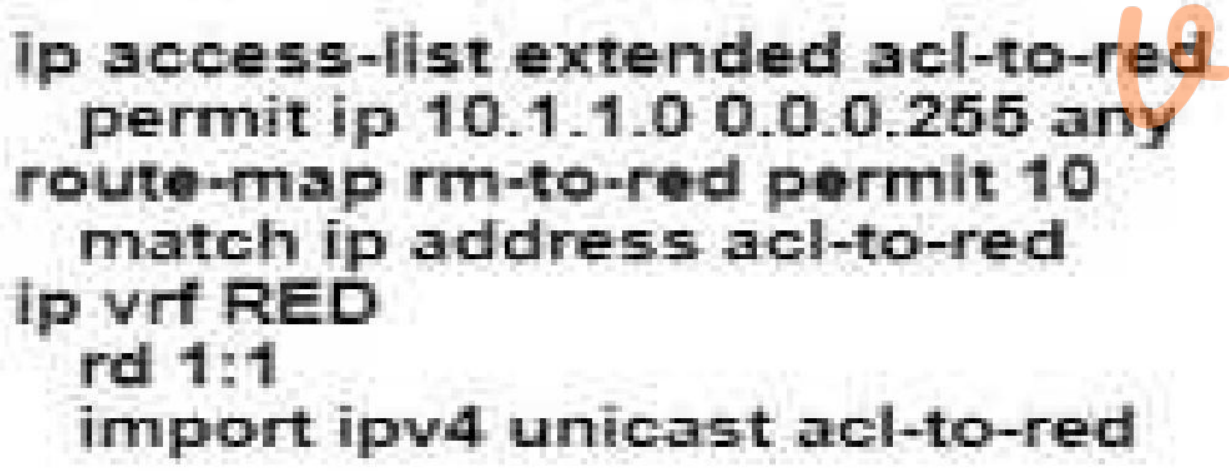
```
ip access-list extended acl-to-red
   permit ip 10.1.1.0 0.0.0.255 any
route-map rm-to-red permit 10
   match ip address acl-to-red
ip vrf RED
   rd 1:1
   import ipv4 unicast route-map acl-to-red
```

C.



```
ip access-list extended acl-to-red
   permit ip 10.1.1.0 0.0.0.255 any
route-map rm-to-red permit 10
   match ip address acl-to-red
ip vrf RED
   rd 1:1
   import ipv4 unicast map rm-to-red
```

D.



```
ip access-list extended acl-to-red
   permit ip 10.1.1.0 0.0.0.255 any
route-map rm-to-red permit 10
   match ip address acl-to-red
ip vrf RED
   rd 1:1
   import ipv4 unicast acl-to-red
```

Correct Answer: B
Section:

QUESTION 282
What are the main components of Cisco TrustSec?

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

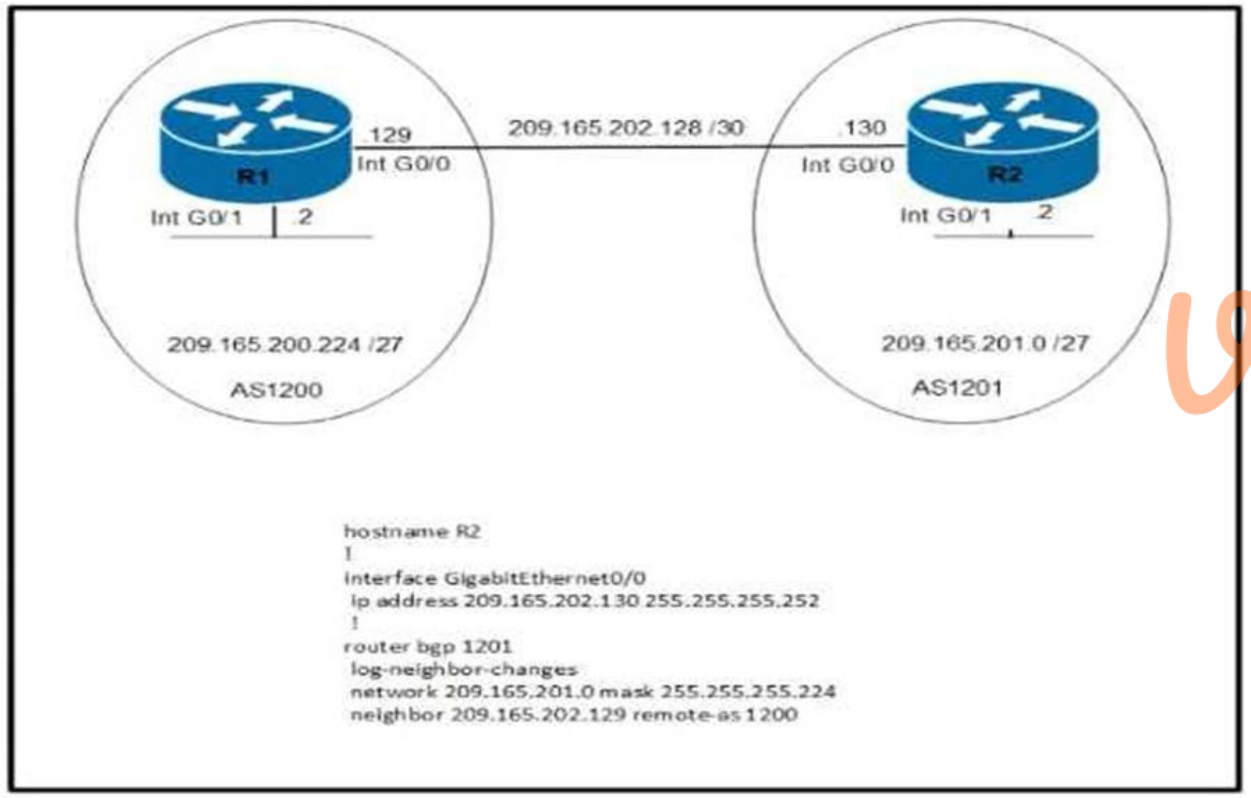
Correct Answer: B
Section:

QUESTION 283
Which three resources must the hypervisor make available to the virtual machines? (Choose three)

A. memory
B. bandwidth
C. IP address
D. processor
E. storage
F. secure access

Correct Answer: A, D, E
Section:

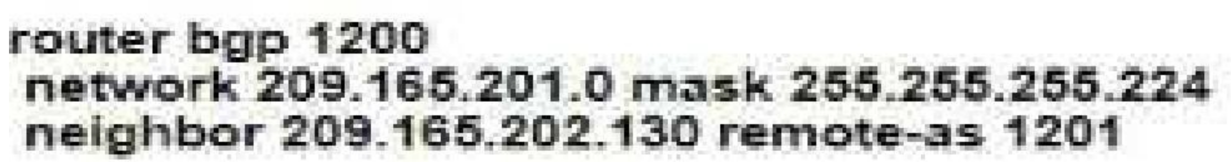
QUESTION 284
Refer to the exhibit.



```
hostname R2
!
interface GigabitEthernet0/0
 ip address 209.165.202.130 255.255.255.252
 !
router bgp 1201
 log-neighbor-changes
 network 209.165.201.0 mask 255.255.255.224
 neighbor 209.165.202.129 remote-as 1200
```

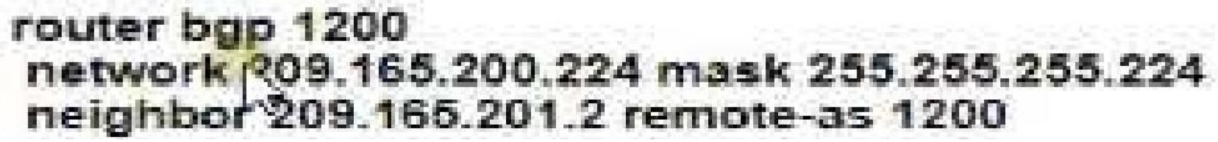
Which command set must be applied on R1 to establish a BGP neighborship with R2 and to allow communication from R1 to reach the networks?

A.



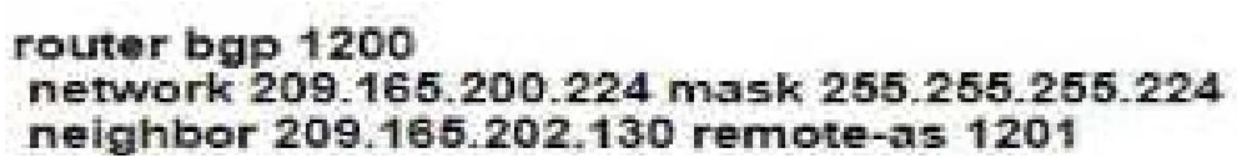
```
router bgp 1200
 network 209.165.201.0 mask 255.255.255.224
 neighbor 209.165.202.130 remote-as 1201
```

B.



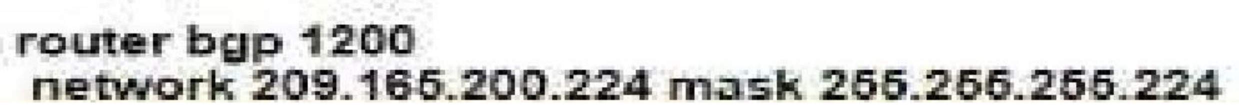
```
router bgp 1200
 network 209.165.200.224 mask 255.255.255.224
 neighbor 209.165.201.2 remote-as 1200
```

C.



```
router bgp 1200
 network 209.165.200.224 mask 255.255.255.224
 neighbor 209.165.202.130 remote-as 1201
```

D.



```
router bgp 1200
 network 209.165.200.224 mask 255.255.255.224
```

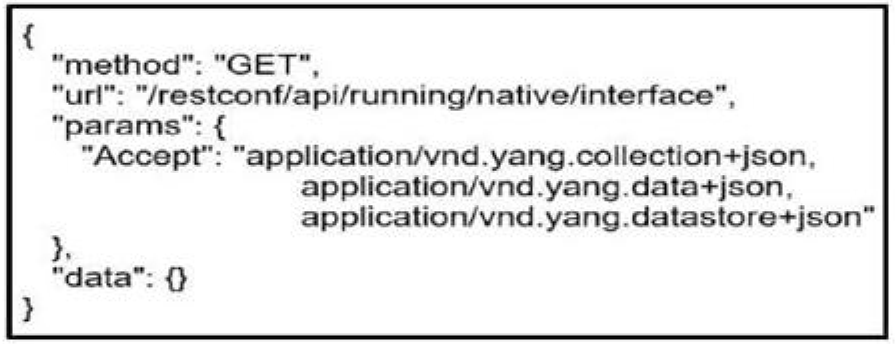
Correct Answer: A
Section:

QUESTION 285
What is the purpose of an RP in PIM?

A. send join messages toward a multicast source SPT
B. ensure the shortest path from the multicast source to the receiver
C. receive IGMP joins from multicast receivers
D. secure the communication channel between the multicast sender and receiver

Correct Answer: A
Section:

QUESTION 286
Refer to the exhibit.



```
{
   "method": "GET",
   "url": "/restconf/api/running/native/interface",
   "params": {
      "Accept": "application/vnd.yang.collection+json,
                      application/vnd.yang.data+json,
                      application/vnd.yang.datastore+json"
   },
   "data": {}
}
```

What is the result of the API request?

A. The "params" variable sends data fields to the network appliance.
B. The native interface information is read from the network appliance.
C. The Information for all interfaces is read from the network appliance.
D. The "params" variable reads data fields from the network appliance

Correct Answer: D
Section:

QUESTION 287
Which definition describes JWT in regard to REST API security?

A. an encrypted JSON token that is used for authentication
B. an encrypted JSON token that is used for authorization

C. an encoded JSON token that is used to securely exchange information

D. an encoded JSON token that is used for authentication

Correct Answer: D
Section:

QUESTION 288
What happens when a FlexConnect AP changes to standalone mode?

A. All controller-dependent activities stop working except the DFS.

B. All client roaming continues to work

C. Only clients on central switching WLANs stay connected.

D. All clients on an WLANs are disconnected

Correct Answer: A
Section:

QUESTION 289
Which protocol is implemented to establish secure control plane adjacencies between Cisco SD-WAN nodes?

A. IKF

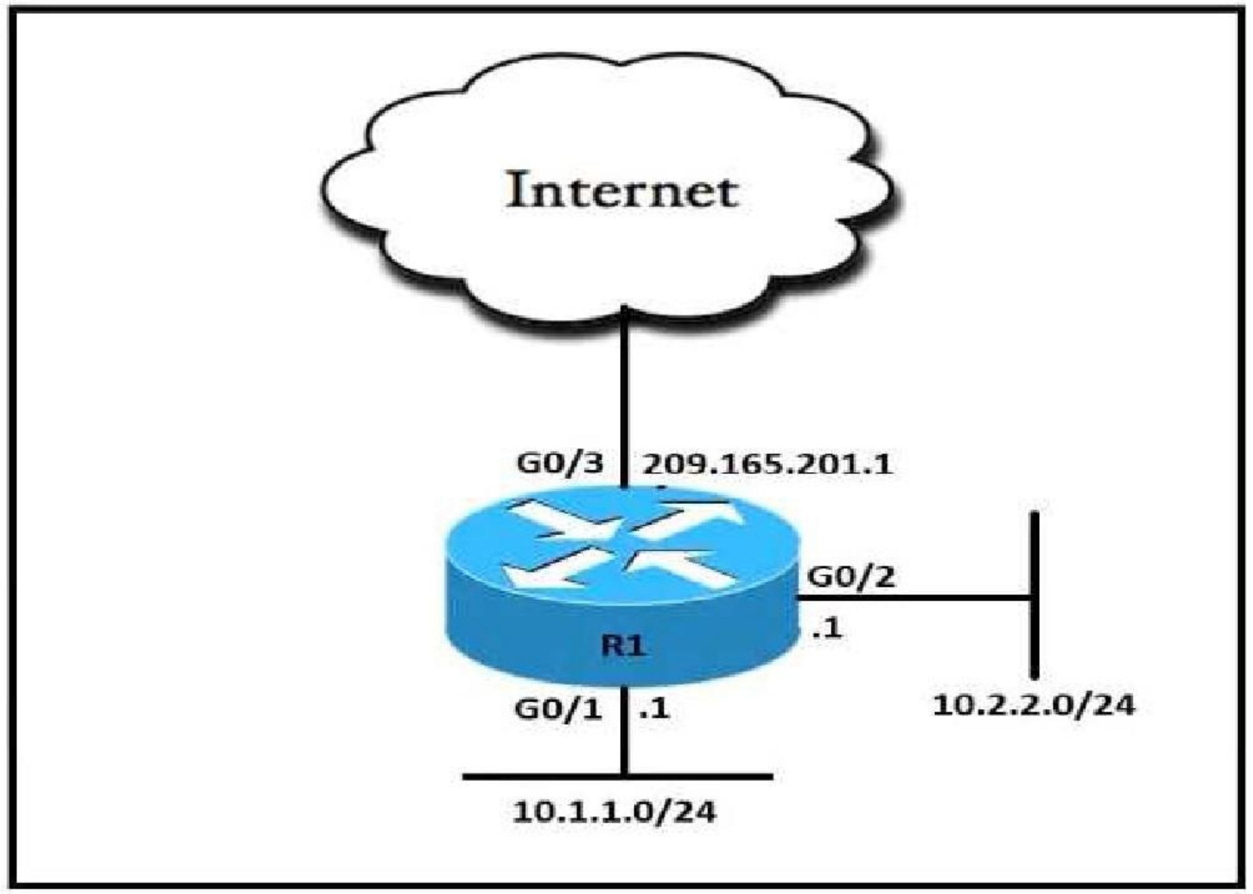
B. TLS

C. IPsec

D. ESP

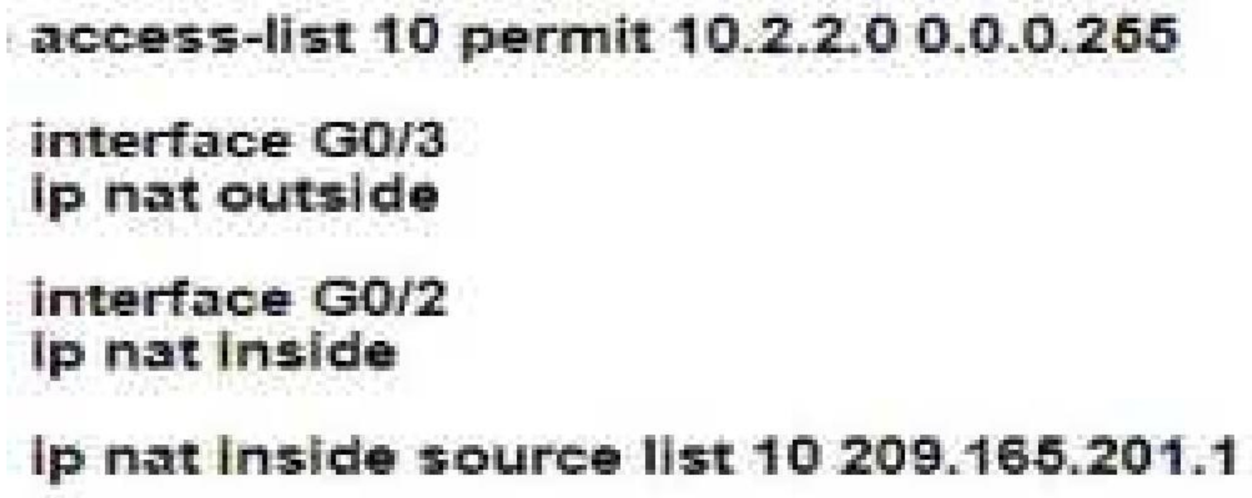
Correct Answer: B
Section:

QUESTION 290
Refer to the exhibit.



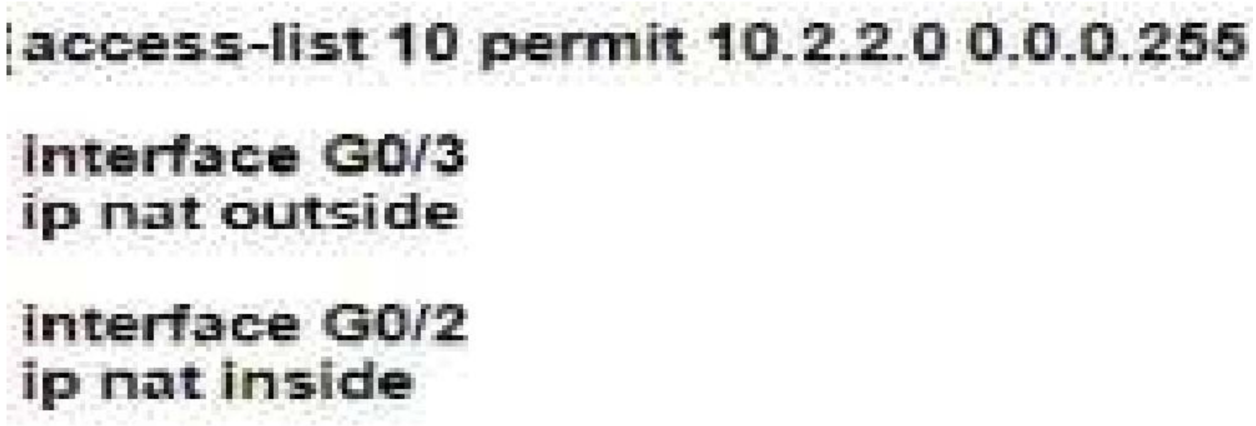
An engineer must allow all users in the 10.2.2.0/24 subnet to access the Internet. To conserve address space the public Interface address of 209 165 201.1 must be used for all external communication.
Which command set accomplishes these requirements?

A.



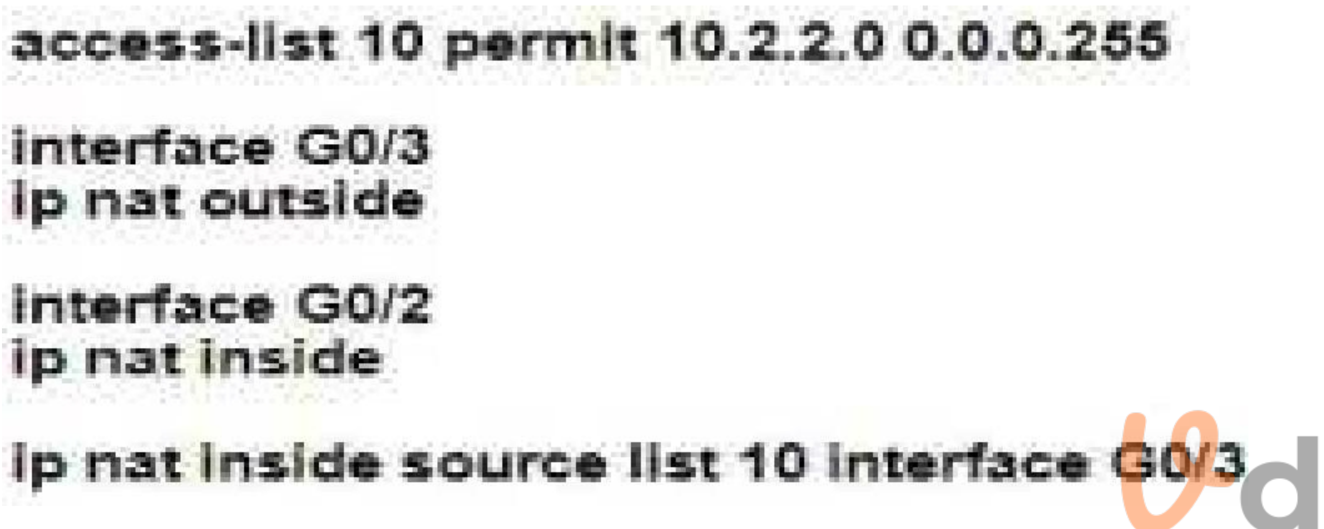
```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 209.165.201.1
```

B.



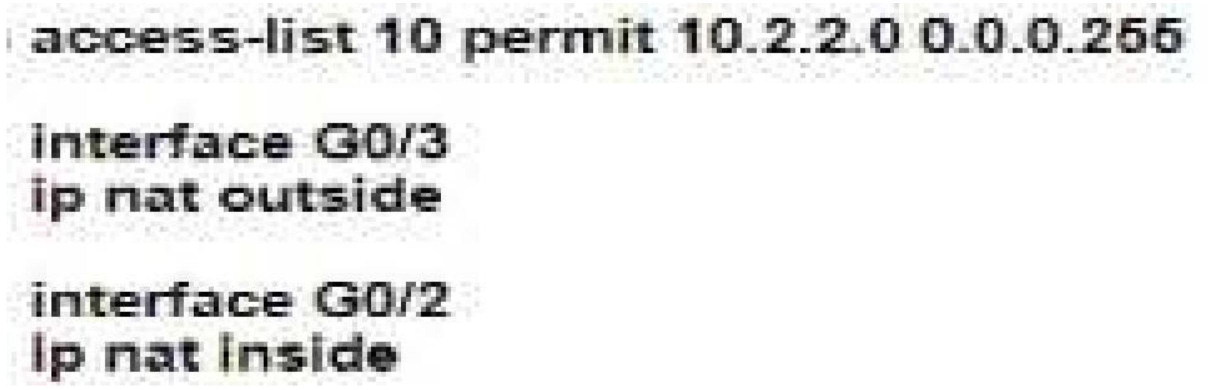
```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside
```

C.



```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 interface G0/3
```

D.



```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside
```

Correct Answer: C
Section:

QUESTION 291
Which benefit is realized by implementing SSO?

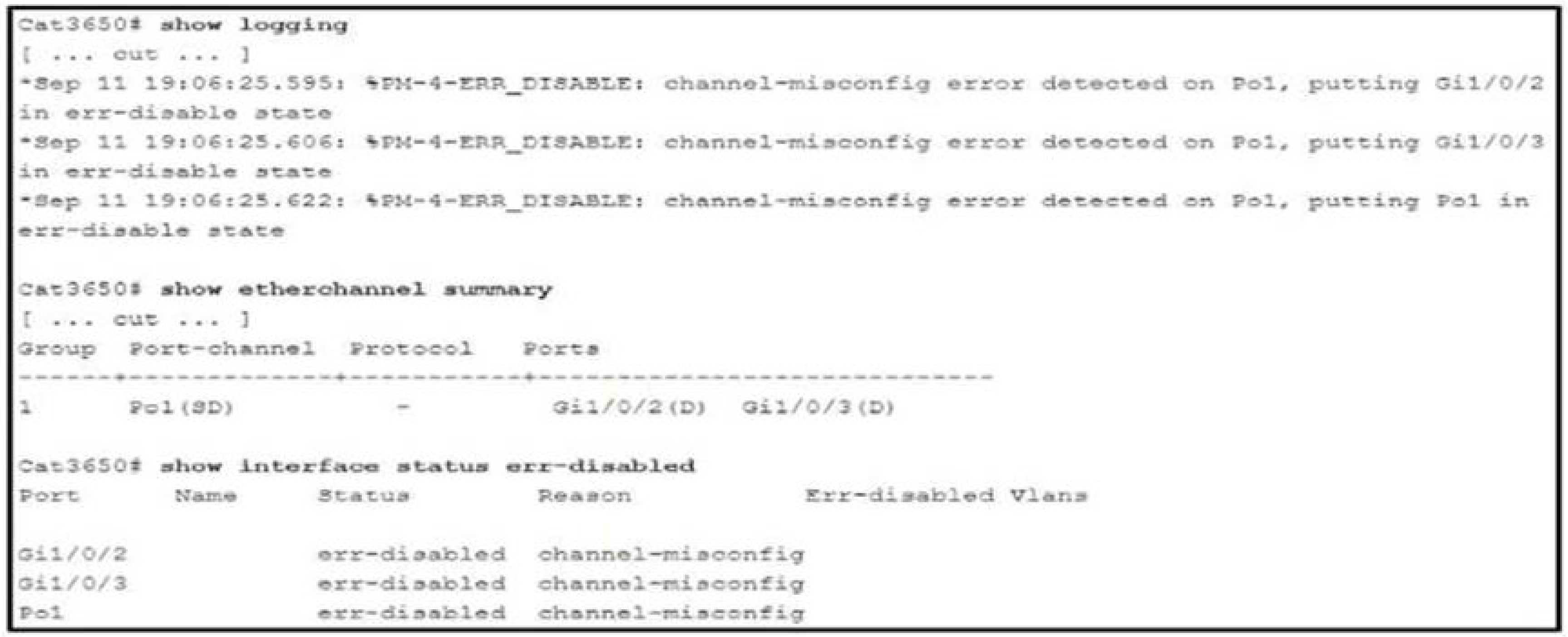
A. IP first-hop redundancy
B. communication between different nodes for cluster setup
C. physical link redundancy
D. minimal network downtime following an RP switchover

Correct Answer: D

Section:

QUESTION 292

Refer to the exhibit.



```
Cat3650# show logging
[ ... cut ... ]
*Sep 11 19:06:25.595: %PM-4-ERR_DISABLE: channel-misconfig error detected on Po1, putting Gi1/0/2
in err-disable state
*Sep 11 19:06:25.606: %PM-4-ERR_DISABLE: channel-misconfig error detected on Po1, putting Gi1/0/3
in err-disable state
*Sep 11 19:06:25.622: %PM-4-ERR_DISABLE: channel-misconfig error detected on Po1, putting Po1 in
err-disable state

Cat3650# show etherchannel summary
[ ... cut ... ]
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------
1      Po1(SD)          -         Gi1/0/2(D)   Gi1/0/3(D)

Cat3650# show interface status err-disabled
Port       Name      Status          Reason              Err-disabled Vlans

Gi1/0/2              err-disabled   channel-misconfig
Gi1/0/3              err-disabled   channel-misconfig
Po1                  err-disabled   channel-misconfig
```

The administrator troubleshoots an EtherChannel that keeps moving to err-disabled. Which two actions must be taken to resolve the issue? (Choose two.)

A. Reload the switch to force EtherChannel renegotiation

B. Ensure that interfaces Gi1/0/2 and Gi1/0/3 connect to the same neighboring switch.

C. Ensure that the switchport parameters of Port channel1 match the parameters of the port channel on the neighbor switch

D. Ensure that the corresponding port channel interface on the neighbor switch is named Portchannel1.

E. Ensure that the neighbor interfaces of Gi1/0/2 and Gi/0/3 are configured as members of the same EtherChannel

Correct Answer: B, E
Section:
Explanation:

Causes of Errdisable

This feature was first implemented in order to handle special collision situations in which the switch detected excessive or late collisions on a port. Excessive collisions occur when a frame is dropped because the switch encounters 16 collisions in a row. Late collisions occur after every device on the wire should have recognized that the wire was in use. Possible causes of these types of errors include:

A cable that is out of specification (either too long, the wrong type, or defective) A bad network interface card (NIC) card (with physical problems or driver problems) A port duplex misconfiguration A port duplex misconfiguration is a common cause of the errors because of failures to negotiate the speed and duplex properly between two directly connected devices (for example, a NIC that connects to a switch). Only half-duplex connections should ever have collisions in a LAN. Because of the carrier sense multiple access (CSMA) nature of Ethernet, collisions are normal for half duplex, as long as the collisions do not exceed a small percentage of traffic.

QUESTION 293

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

A. The MAC address table supports partial matches. TCAM requires an exact match.

B. The MAC address table is contained in TCAM ACL and QoS information is stored in CAM.

C. Router prefix lookups happen in TCAM. MAC address table lookups happen In CAM.

D. TCAM is used to make L2 forwarding decisions. CAM is used to build routing tables

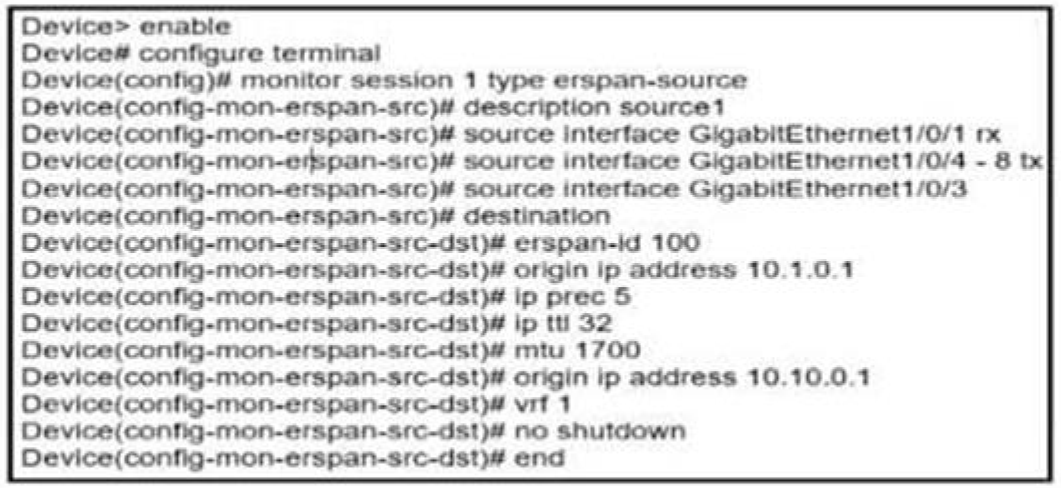
Correct Answer: C
Section:
Explanation:
"TCAM is most useful for building tables for searching on longest matches such as IP routing tables organized by IP prefixes. The TCAM table stores ACL, QoS and other information generally associated with upper-layer processing. As a result of using TCAM, applying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

QUESTION 294
Which two features does the Cisco SD-Access architecture add to a traditional campus network?
(Choose two.)

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

Correct Answer: A, E
Section:
Explanation:
https://www.aspiretransforms.com/2018/06/06/insider-guide-cisco-sd-access/

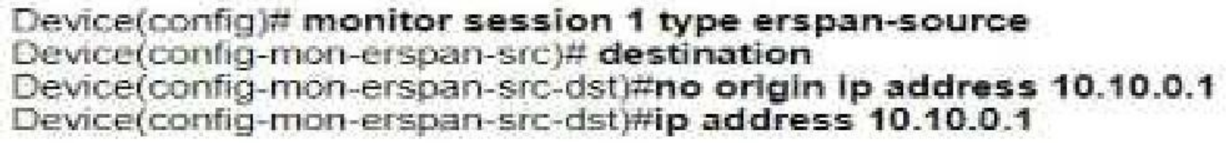
QUESTION 295
Refer to the exhibit.



```
Device> enable
Device# configure terminal
Device(config)# monitor session 1 type erspan-source
Device(config-mon-erspan-src)# description source1
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/1 rx
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/4 - 8 tx
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/3
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# erspan-id 100
Device(config-mon-erspan-src-dst)# origin ip address 10.1.0.1
Device(config-mon-erspan-src-dst)# ip prec 5
Device(config-mon-erspan-src-dst)# ip ttl 32
Device(config-mon-erspan-src-dst)# mtu 1700
Device(config-mon-erspan-src-dst)# origin ip address 10.10.0.1
Device(config-mon-erspan-src-dst)# vrf 1
Device(config-mon-erspan-src-dst)# no shutdown
Device(config-mon-erspan-src-dst)# end
```

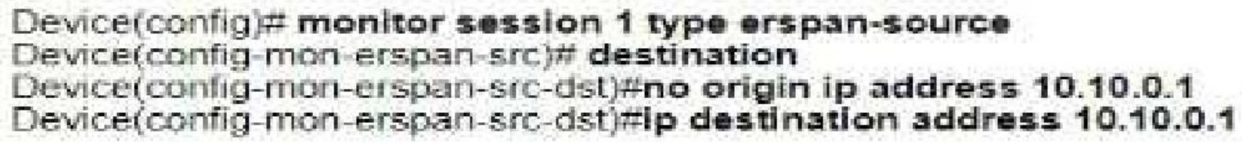
An engineer must configure an ERSPAN session with the remote end of the session 10.10.0.1. Which commands must be added to complete the configuration?

A.



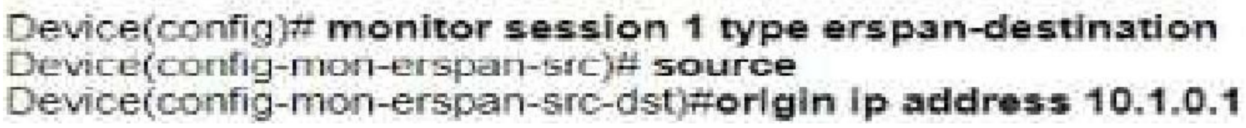
```
Device(config)# monitor session 1 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)#no origin ip address 10.10.0.1
Device(config-mon-erspan-src-dst)#ip address 10.10.0.1
```

B.



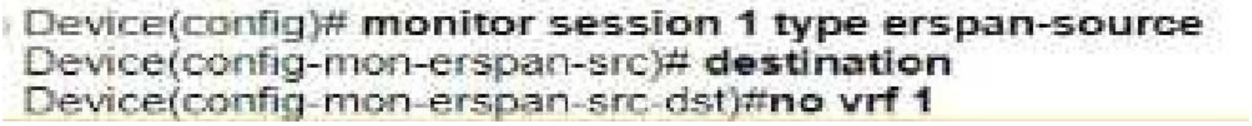
```
Device(config)# monitor session 1 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)#no origin ip address 10.10.0.1
Device(config-mon-erspan-src-dst)#ip destination address 10.10.0.1
```

C.



```
Device(config)# monitor session 1 type erspan-destination
Device(config-mon-erspan-src)# source
Device(config-mon-erspan-src-dst)#origin ip address 10.1.0.1
```

D.

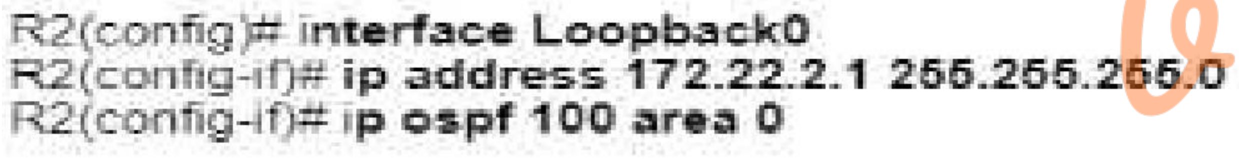


```
Device(config)# monitor session 1 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)#no vrf 1
```

Correct Answer: A
Section:
Explanation:
Example: Configuring an ERSPAN Source Session on a WAN Interface
The following example shows how to configure more than one WAN interface in a single ERSPAN source monitor session. Multiple interfaces have been separated by a commas. monitor session 100 type erspan-source source interface
Serial 0/1/0:0, Serial 0/1/0:6 Example: Configuring an ERSPAN Destination Session The following example shows how to configure an ERSPAN destination session: monitor session 2 type erspan-destination destination interface
GigabitEthernet1/3/2 destination interface GigabitEthernet2/2/0 source erspan-id 100 ip address 10.10.0.1

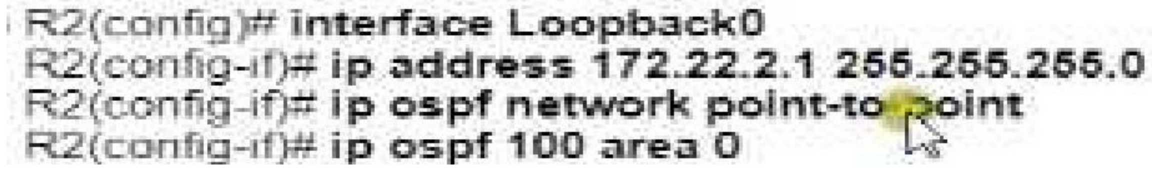
QUESTION 296
An engineer must configure a new loopback Interface on a router and advertise the interface as a fa4 in OSPF. Which command set accomplishes this task?

A.



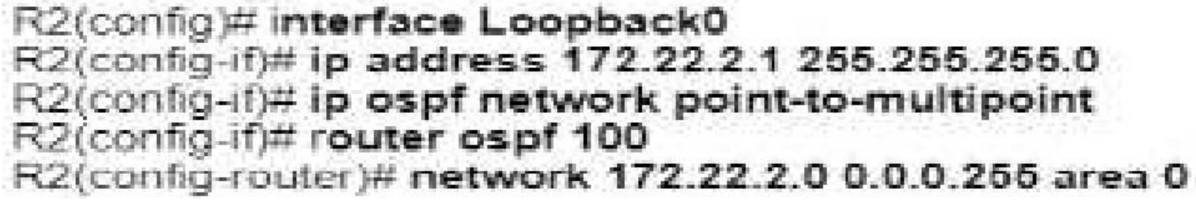
```
R2(config)# interface Loopback0
R2(config-if)# ip address 172.22.2.1 255.255.255.0
R2(config-if)# ip ospf 100 area 0
```

B.



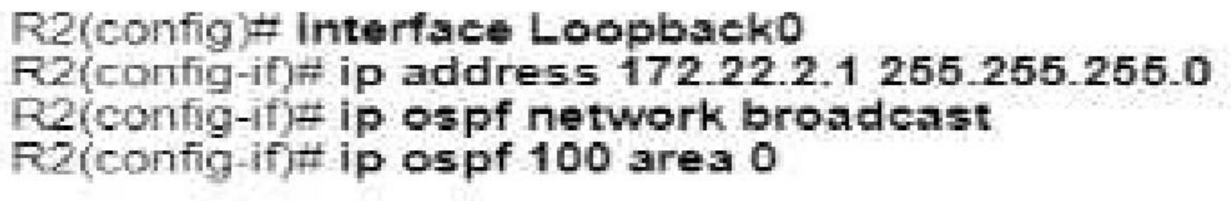
```
R2(config)# interface Loopback0
R2(config-if)# ip address 172.22.2.1 255.255.255.0
R2(config-if)# ip ospf network point-to-point
R2(config-if)# ip ospf 100 area 0
```

C.



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

D.



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

Correct Answer: A
Section:

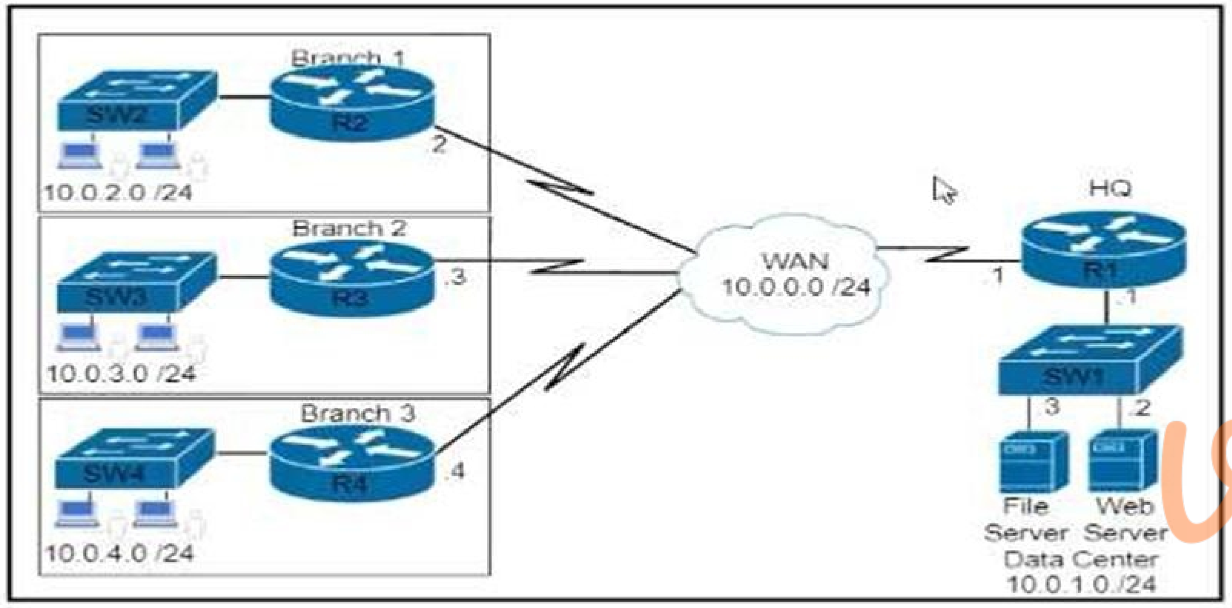
Explanation:

Step 1. Create the loopback interface using the interface loopback number global configuration command.
Step 2. Add a description. Although optional, it is a necessary component for documenting a network.
Step 3. Configure the IP address.
For example, the following commands configure a loopback interface of the R1 router shown in (shown earlier in the chapter):

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

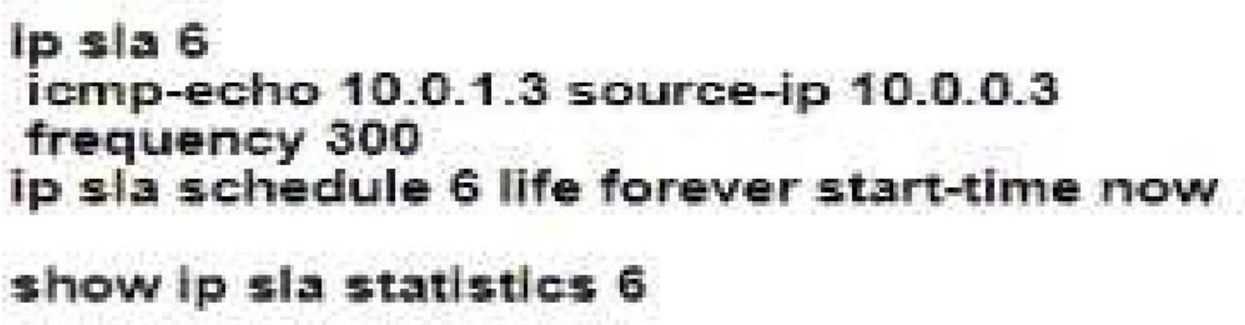
QUESTION 297

Refer to the exhibit.



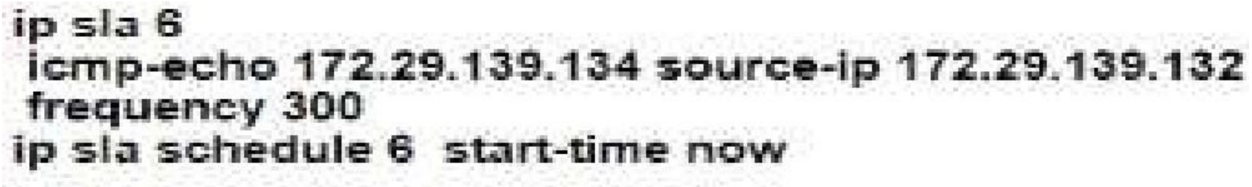
Which command set is needed to configure and verify router R3 to measure the response time from router R3 to the file server located in the data center?

A.



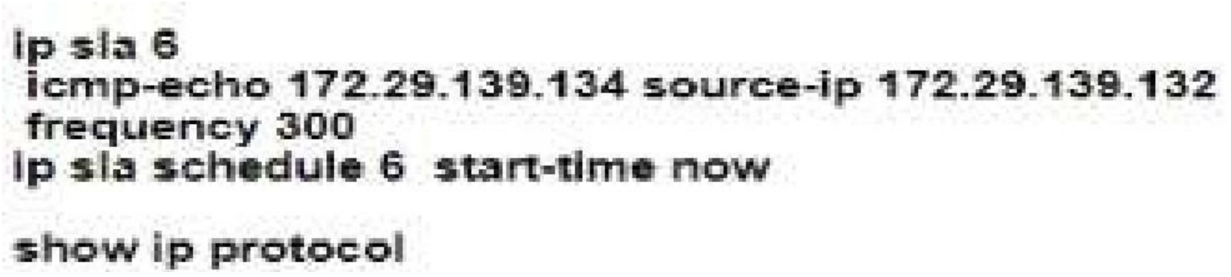
```
ip sla 6
 icmp-echo 10.0.1.3 source-ip 10.0.0.3
 frequency 300
ip sla schedule 6 life forever start-time now

show ip sla statistics 6
```

B.



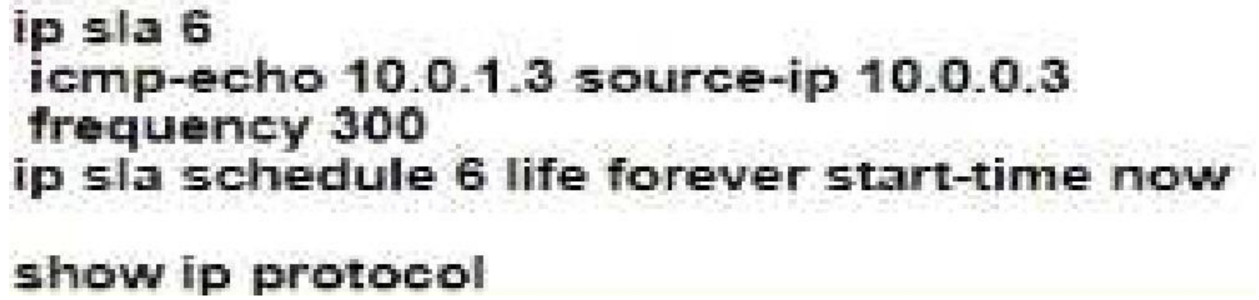
```
ip sla 6
 icmp-echo 172.29.139.134 source-ip 172.29.139.132
 frequency 300
ip sla schedule 6  start-time now
```

C.



```
ip sla 6
 icmp-echo 172.29.139.134 source-ip 172.29.139.132
 frequency 300
ip sla schedule 6  start-time now

show ip protocol
```

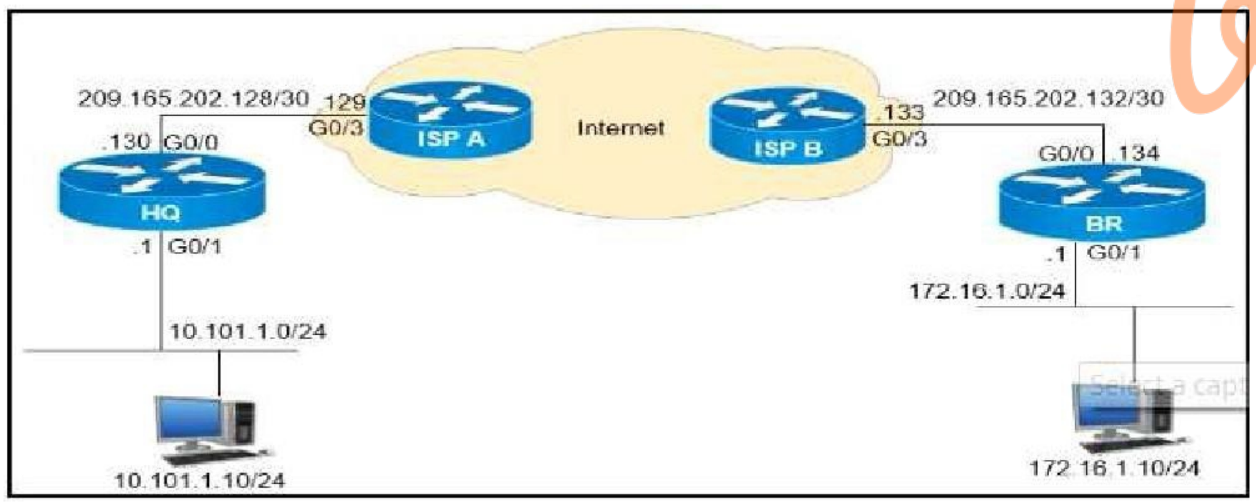
D.



```
ip sla 6
 icmp-echo 10.0.1.3 source-ip 10.0.0.3
 frequency 300
ip sla schedule 6 life forever start-time now

show ip protocol
```

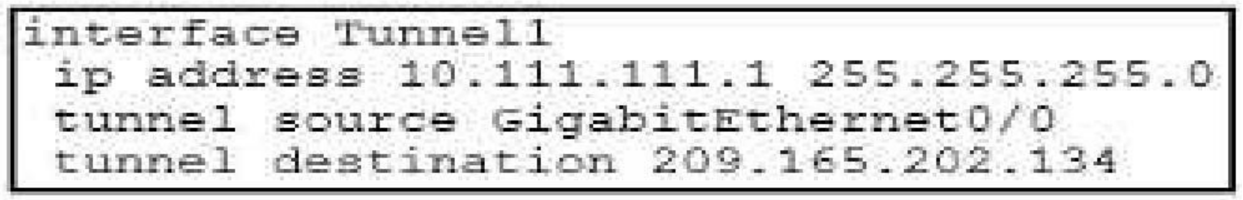
Correct Answer: A
Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-550x-series-stackable-managedswitches/smb5797-configure-ip-sla-tracking-for-ipv4-static-routes-on-an-sg550.html

QUESTION 298
Refer to the exhibit.



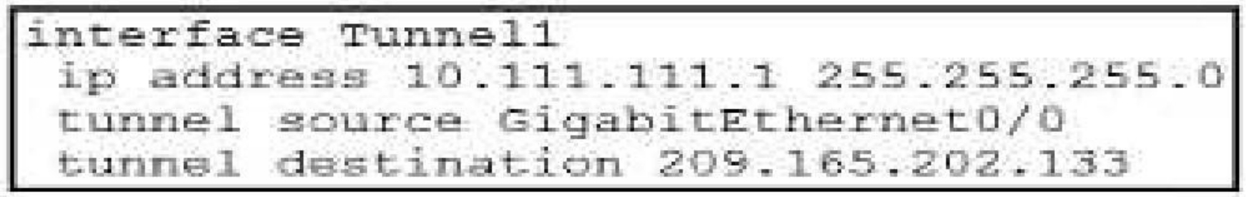
Which configuration must be applied to the HQ router to set up a GRE tunnel between the HQ and BR routers?

A.



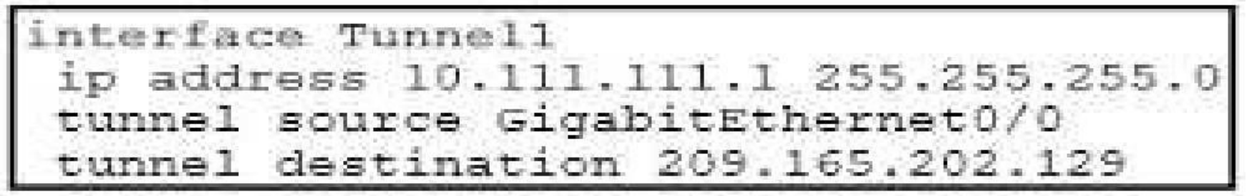
```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.134
```

B.



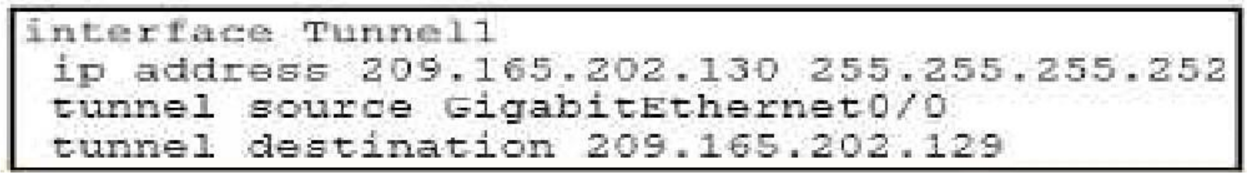
```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.133
```

C.



```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.129
```

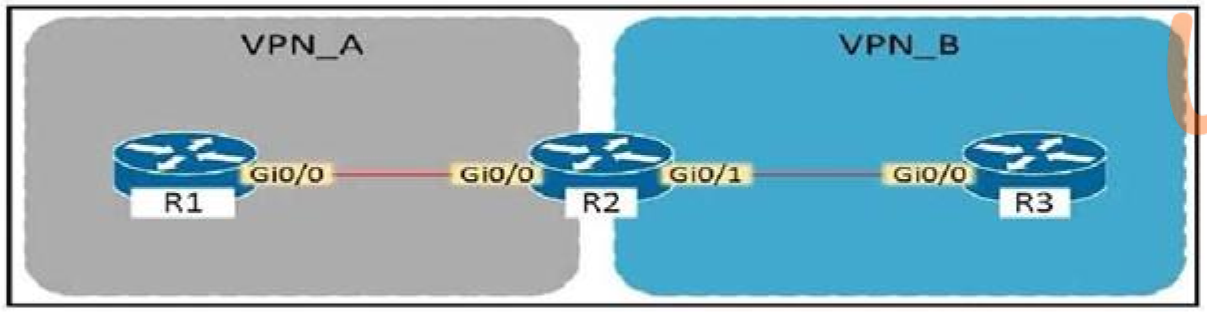
D.



```
interface Tunnel1
 ip address 209.165.202.130 255.255.255.252
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.129
```

Correct Answer: A
Section:

QUESTION 299
Refer to The exhibit.



Assuming that R1 is a CE router, which VRF is assigned to Gi0/0 on R1?

A. VRF VFN_A
B. VRF VPN_B
C. management VRF
D. default VRF

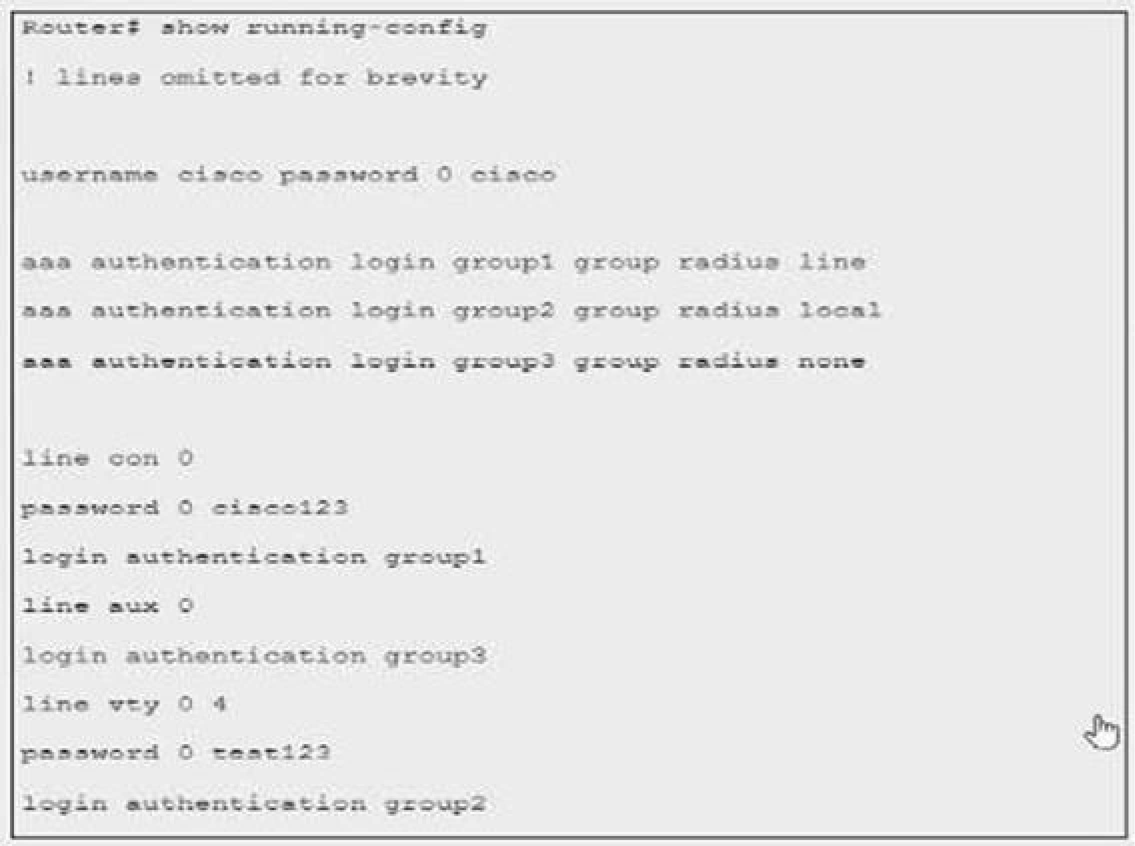
Correct Answer: D
Section:

QUESTION 300
How do EIGRP metrics compare to OSPF metrics?

A. EIGRP metrics are based on a combination of bandwidth and packet loss, and OSPF metrics are based on interface bandwidth.
B. EIGRP uses the Dijkstra algorithm, and OSPF uses The DUAL algorithm
C. The EIGRP administrative distance for external routes is 170. and the OSPF administrative distance for external routes is undefined
D. The EIGRP administrative distance for external routes is 170. and the OSPF administrative distance for external routes is 110

Correct Answer: A
Section:

QUESTION 301
Refer to the exhibit.



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

username cisco password 0 cisco

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

line con 0
password 0 cisco123
login authentication group1
line aux 0
login authentication group3
line vty 0 4
password 0 test123
login authentication group2
```

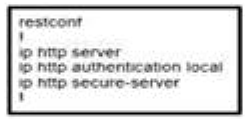
A network engineer must log in to the router via the console, but the RADIUS servers are not reachable Which credentials allow console access1?

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

Correct Answer: D
Section:

QUESTION 302

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

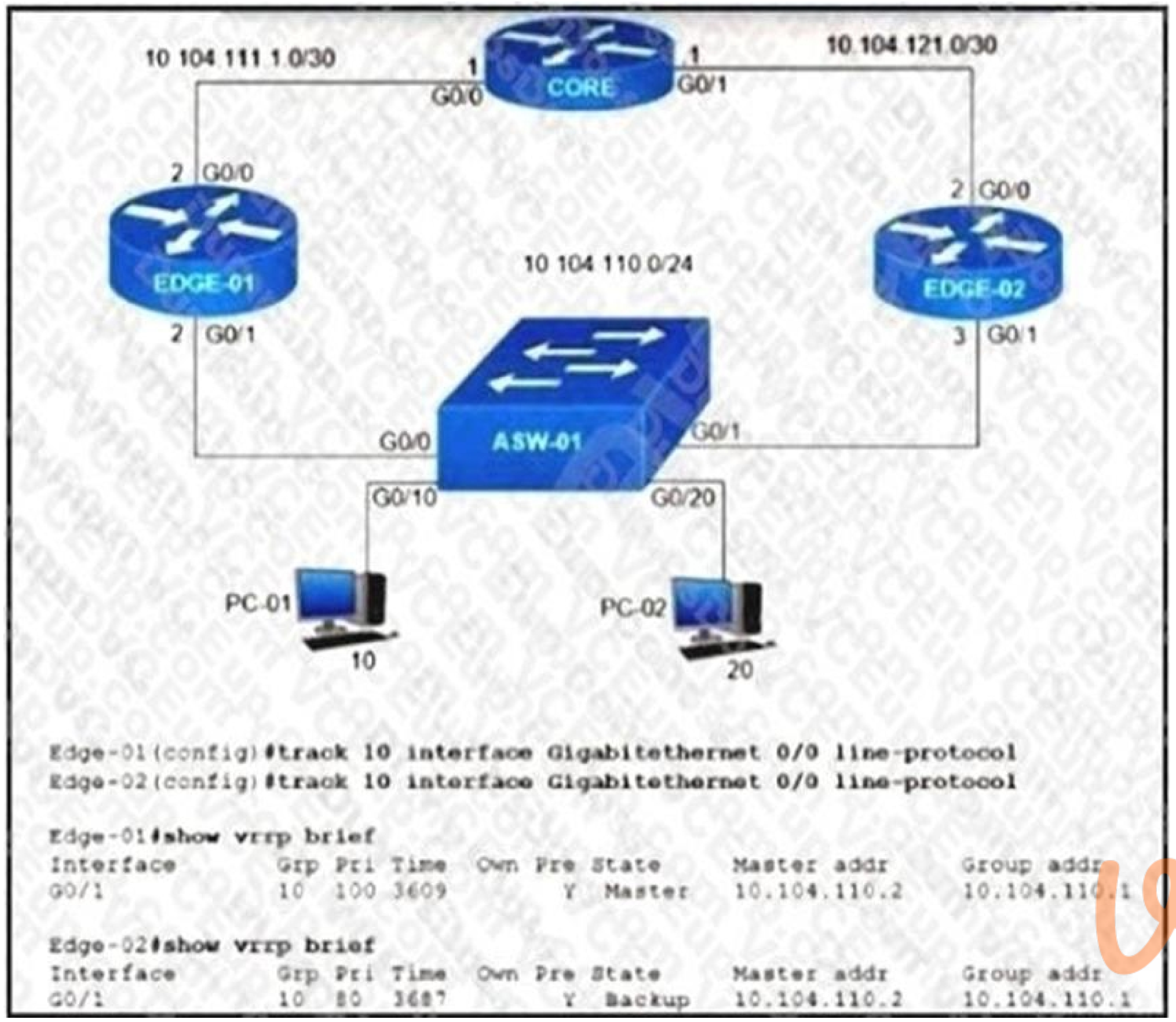
Correct Answer: A
Section:

QUESTION 303
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

Correct Answer: B
Section:
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

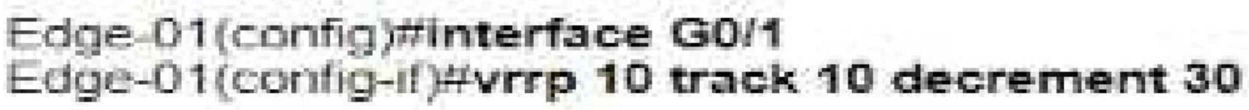
QUESTION 304
Refer to the exhibit.



```
Edge-01(config)#track 10 interface Gigabitethernet 0/0 line-protocol
Edge-02(config)#track 10 interface Gigabitethernet 0/0 line-protocol

Edge-01#show vrrp brief
Interface        Grp Pri Time  Own Pre State    Master addr    Group addr
G0/1             10  100 3609       Y  Master   10.104.110.2   10.104.110.1

Edge-02#show vrrp brief
Interface        Grp Pri Time  Own Pre State    Master addr    Group addr
G0/1             10  80  3687       Y  Backup   10.104.110.2   10.104.110.1
```

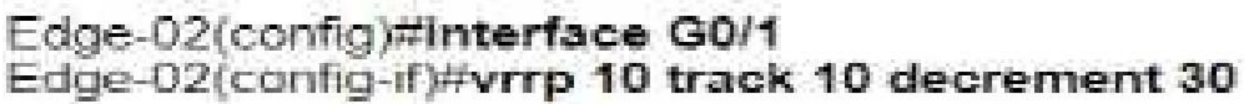
Object tracking has been configured for VRRP-enabled routers Edge-01 and Edge-02 Which commands cause Edge-02 to preempt Edge-01 in the event that interface G0/0 goes down on Edge- 01?

A.



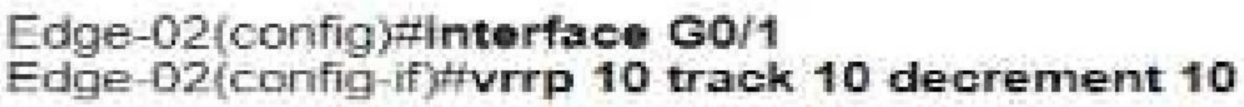
```
Edge-01(config)#interface G0/1
Edge-01(config-if)#vrrp 10 track 10 decrement 30
```

B.



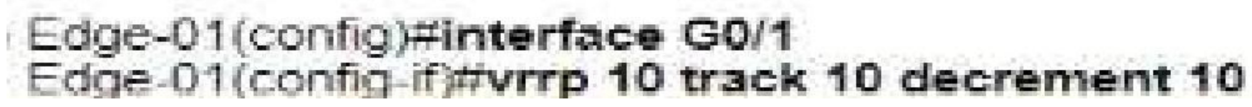
```
Edge-02(config)#interface G0/1
Edge-02(config-if)#vrrp 10 track 10 decrement 30
```

C.



```
Edge-02(config)#interface G0/1
Edge-02(config-if)#vrrp 10 track 10 decrement 10
```

D.



```
Edge-01(config)#interface G0/1
Edge-01(config-if)#vrrp 10 track 10 decrement 10
```

Correct Answer: A
Section:

QUESTION 305

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

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

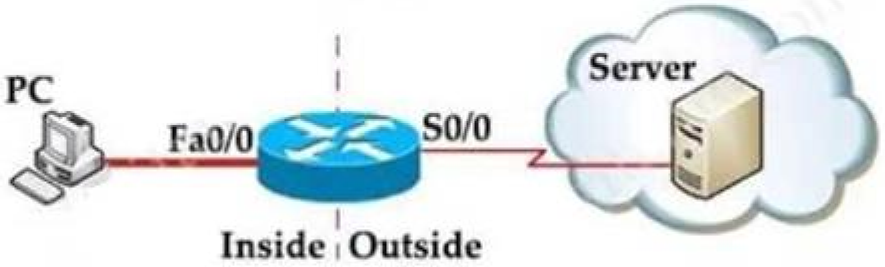
Correct Answer: B
Section:
Explanation:
Layer2 Flooding
Cisco SD-Access fabric provides many optimizations to improve unicast traffic flow, and to reduce the unnecessary flooding of data such as broadcasts. But, for some traffic and applications, it may be desirable to enable broadcast forwarding within the fabric.
By default, this is disabled in the Cisco SD-Access architecture. If broadcast, Link local multicast and Arp flooding is required, it must be specifically enabled on a per-subnet basis using Layer 2 flooding feature.
Layer 2 flooding can be used to forward broadcasts for certain traffic and application types which may require leveraging of Layer 2 connectivity, such as silent hosts, card readers, door locks, etc.

QUESTION 306

An engineer must configure an ACL that permits packets which include an ACK in the TCP header Which entry must be included in the ACL?

A. access-list 10 permit ip any any eq 21 tcp-ack
B. access-list 110 permit tcp any any eq 21 tcp-ack
C. access-list 10 permit tcp any any eq 21 established
D. access-list 110 permit tcp any any eq 21 established

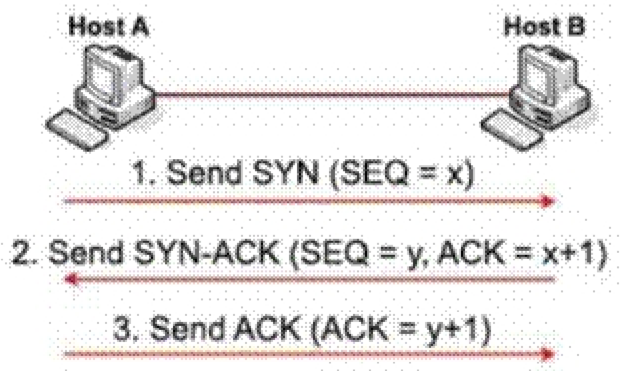
Correct Answer: D
Section:
Explanation:
The established keyword is only applicable to TCP access list entries to match TCP segments that have the ACK and/or RST control bit set (regardless of the source and destination ports), which assumes that a TCP connection has already been established in one direction only. Let's see an example below:



Suppose you only want to allow the hosts inside your company to telnet to an outside server but not vice versa, you can simply use an - "established" access-list like this:

```
access-list 100 permit tcp any any established
access-list 101 permit tcp any any eq telnet
!
interface S0/0
ip access-group 100 in
ip access-group 101 out
```

Note: Suppose host A wants to start communicating with host B using TCP. Before they can send real data, a three-way handshake must be established first. Let's see how this process takes place:



1. First host A will send a SYN message (a TCP segment with SYN flag set to 1, SYN is short for SYNchronize) to indicate it wants to setup a connection with host B. This message includes a sequence (SEQ) number for tracking purpose. This sequence number can be any 32-bit number (range from 0 to 232) so we use -"x" to represent it.
2. After receiving SYN message from host A, host B replies with SYN-ACK message (some books may call it -SYN/ACK? or -SYN, ACK? message. ACK is short for ACKnowledge). This message includes a SYN sequence number and an ACK number:
+ SYN sequence number (let's called it "y") is a random number and does not have any relationship with Host A's SYN SEQ number.
+ ACK number is the next number of Host A's SYN sequence number it received, so we represent it with "x+1". It means -I received your part. Now send me the next part (x + 1)".
The SYN-ACK message indicates host B accepts to talk to host A (via ACK part). And ask if host A still wants to talk to it as well (via SYN part).
3. After Host A received the SYN-ACK message from host B, it sends an ACK message with ACK number "y+1" to host B. This confirms host A still wants to talk to host B.

QUESTION 307
By default, which virtual MAC address does HSRP group 14 use?

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

Correct Answer: D
Section:

QUESTION 308
What is one characteristic of the Cisco SD-Access control plane?

A. It is based on VXLAN technology.
B. Each router processes every possible destination and route
C. It allows host mobility only in the wireless network.
D. It stores remote routes in a centralized database server

Correct Answer: D
Section:
Explanation:
A control plane node maintains a host tracking database (HTDB), and also uses Locator/ID Separation Protocol (LISP) to provide a map server, populating the HTDB from fabric edge registration messages; and a map resolver to respond to queries from edge devices requesting location information about destination nodes.

QUESTION 309
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

Correct Answer: C
Section:

QUESTION 310
In a Cisco SD-Access wireless architecture which device manages endpoint ID to edge node bindings?

A. fabric control plane node
B. fabric wireless controller
C. fabric border node
D. fabric edge node

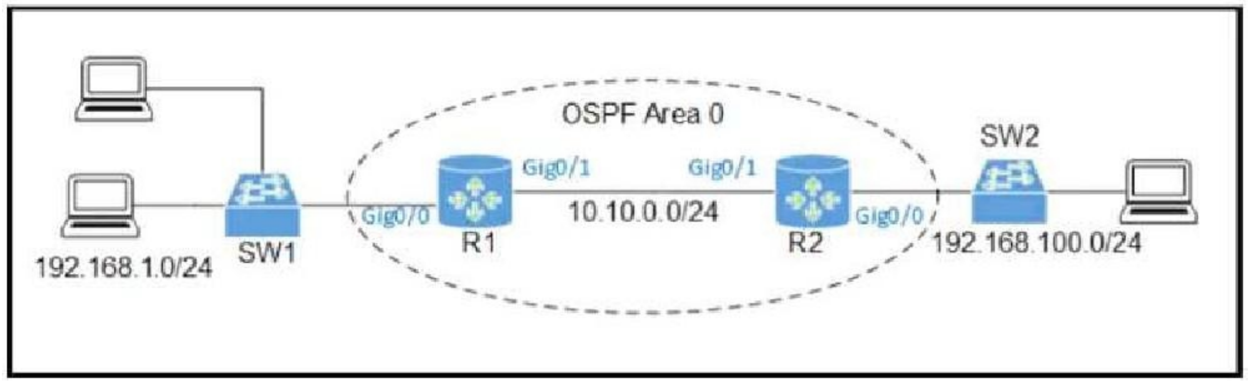
Correct Answer: A
Section:
Explanation:
SD-Access Wireless Architecture Control Plane Node –A Closer Look
Fabric Control-Plane Node is based on a LISP Map Server / Resolver
Runs the LISP Endpoint ID Database to provide overlay reachability information + A simple Host Database, that tracks Endpoint ID to Edge Node bindings (RLOCs)+ Host Database supports multiple types of Endpoint ID (EID), such as IPv4/32, IPv6 /128* or MAC/48 + Receives prefix registrations from Edge Nodes for wired clients, and from Fabric mode WLCs for wireless clients + Resolves lookup requests from FE to locate Endpoints + Updates Fabric Edge nodes, Border nodes with wireless client mobility and RLOC information

QUESTION 311
If the maximum power level assignment for global TPC 802.11a/n/ac is configured to 10 dBm, which power level effectively doubles the transmit power?

A. 13dBm
B. 14 dBm
C. 17dBm
D. 20 dBm

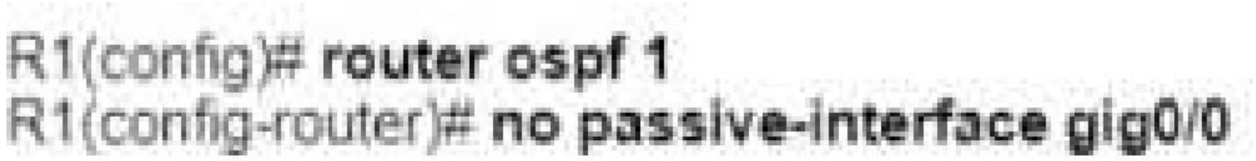
Correct Answer: A
Section:
Explanation:
Suppose a transmitter is configured for a power level of 10 dBm. A cable with 5-dB loss connects the transmitter to an antenna with an 8-dBi gain. The resulting EIRP of the system is EIRP = 10 dBm – 5 dB + 8 dBi = 13 dBm

QUESTION 312
Refer to the exhibit.



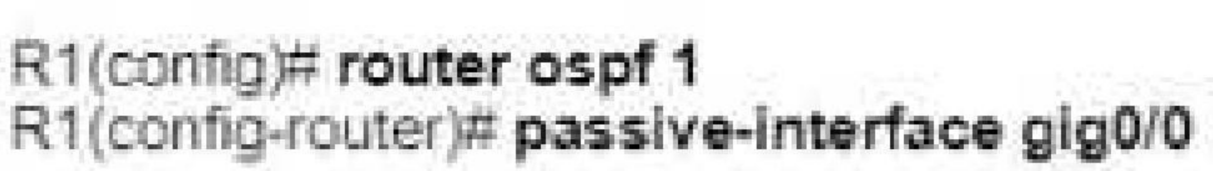
An engineer must allow R1 to advertise the 192 168.1 0/24 network to R2 R1 must perform this action without sending OSPF packets to SW1 Which command set should be applied?

A.



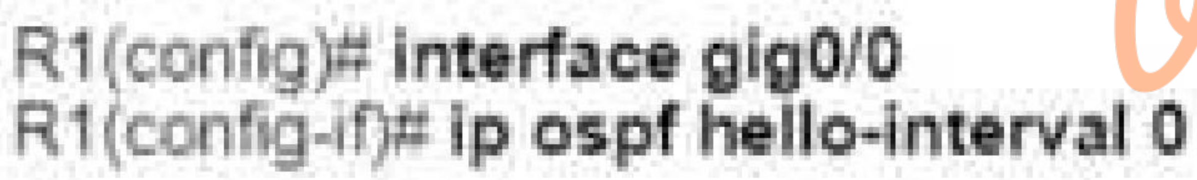
```
R1(config)# router ospf 1
R1(config-router)# no passive-interface gig0/0
```

B.



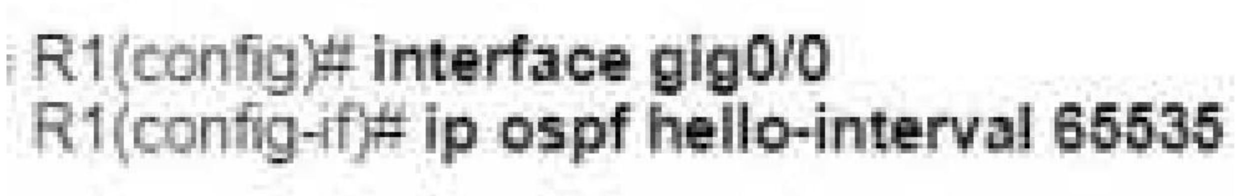
```
R1(config)# router ospf 1
R1(config-router)# passive-interface gig0/0
```

C.



```
R1(config)# interface gig0/0
R1(config-if)# ip ospf hello-interval 0
```

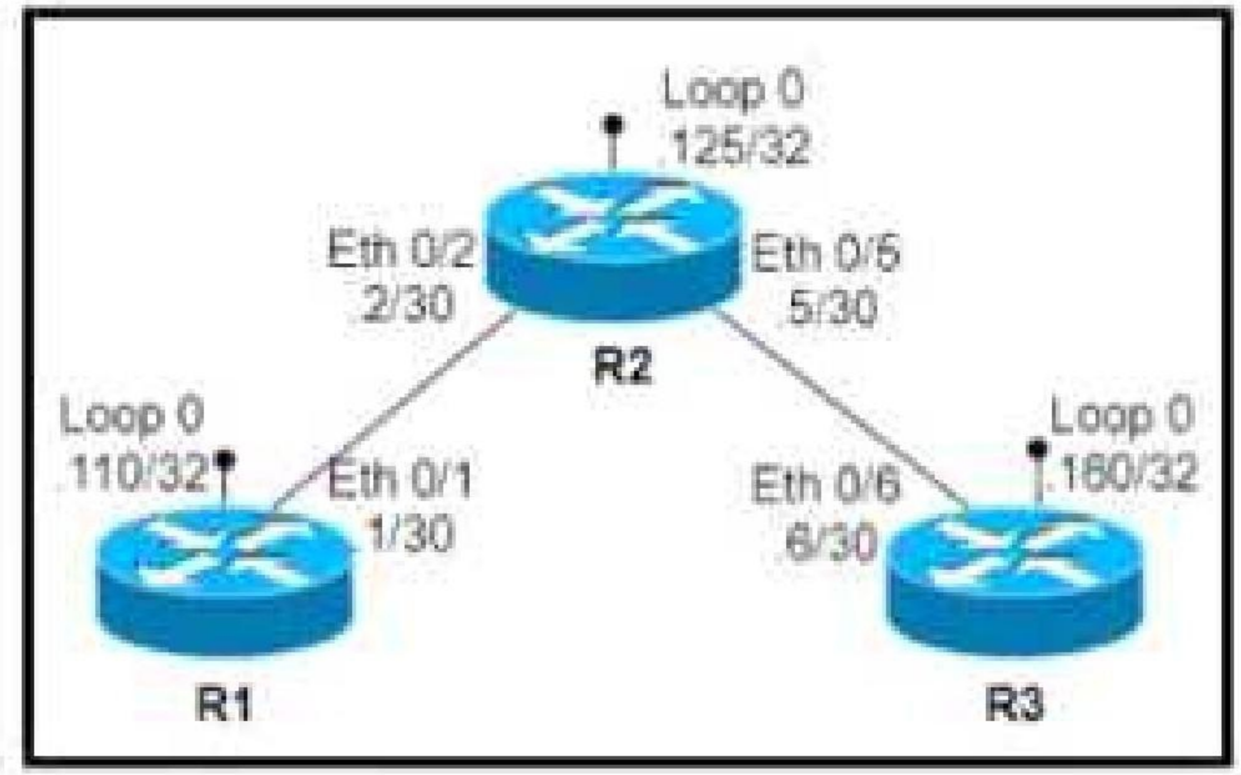
D.



```
R1(config)# interface gig0/0
R1(config-if)# ip ospf hello-interval 65535
```

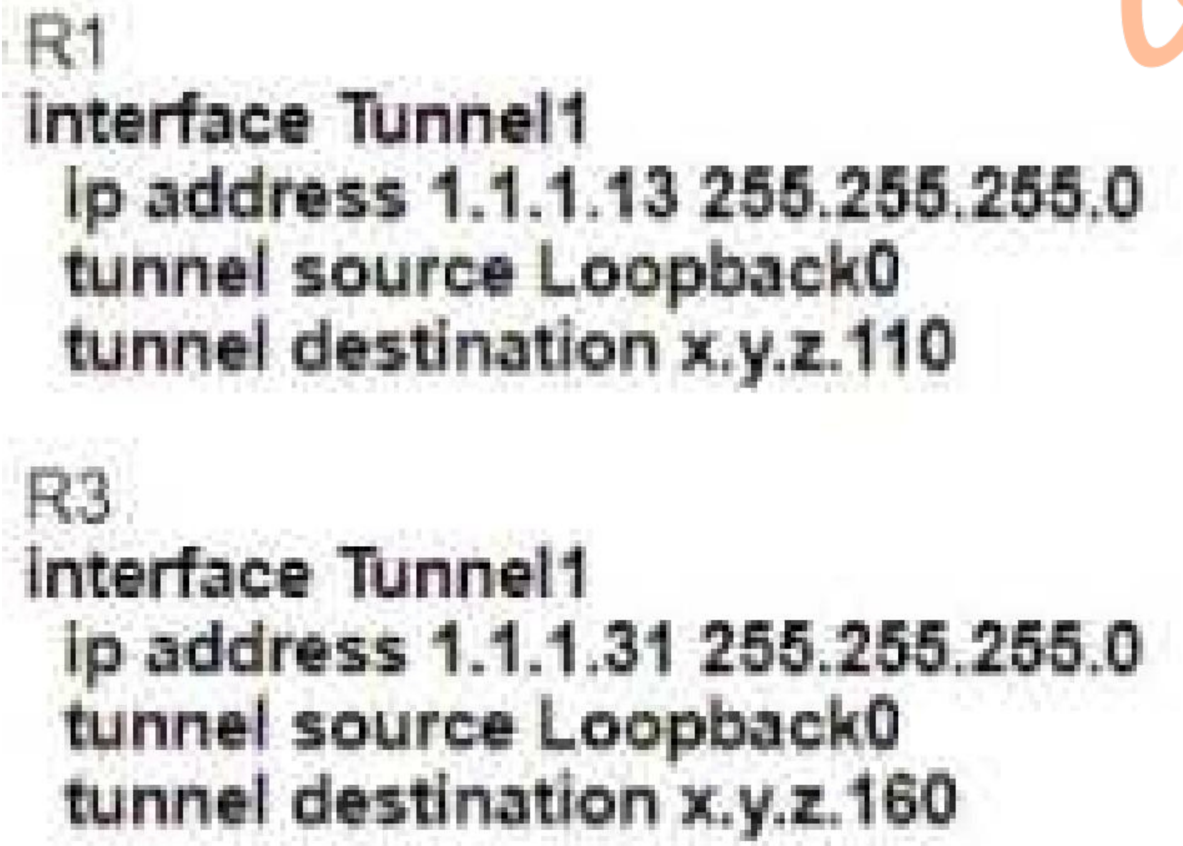
Correct Answer: B
Section:

QUESTION 313
Refer to the exhibit.



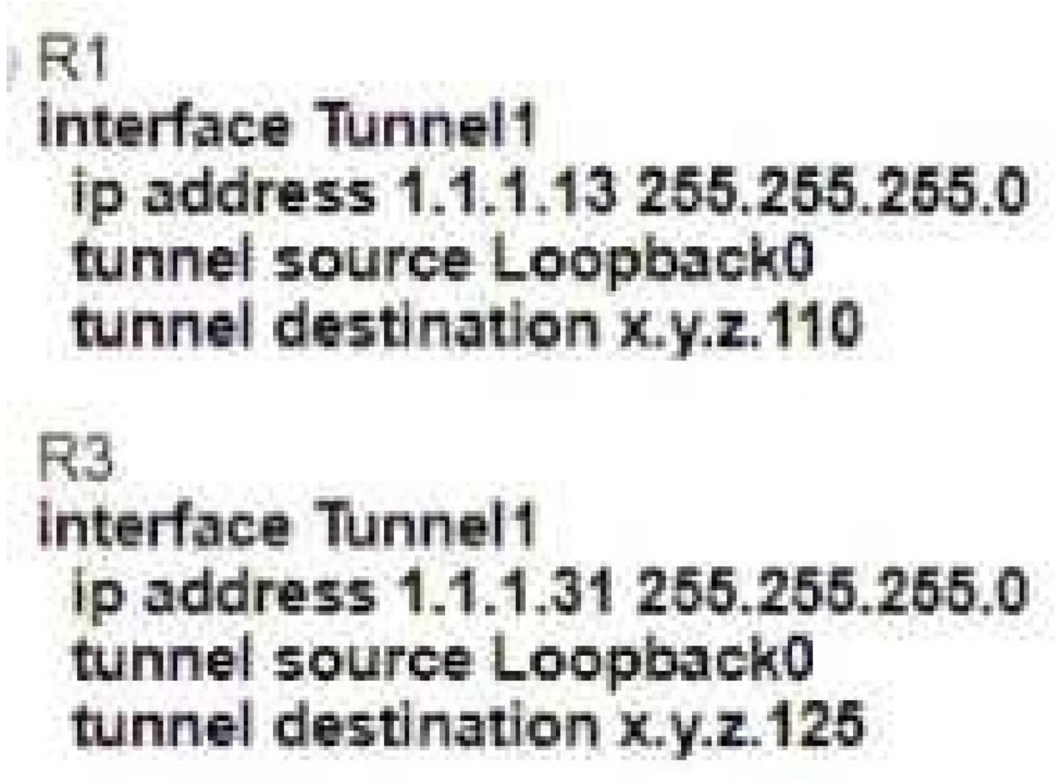
An engineer configures routing between all routers and must build a configuration to connect R1 to R3 via a GRE tunnel Which configuration must be applied?

A.



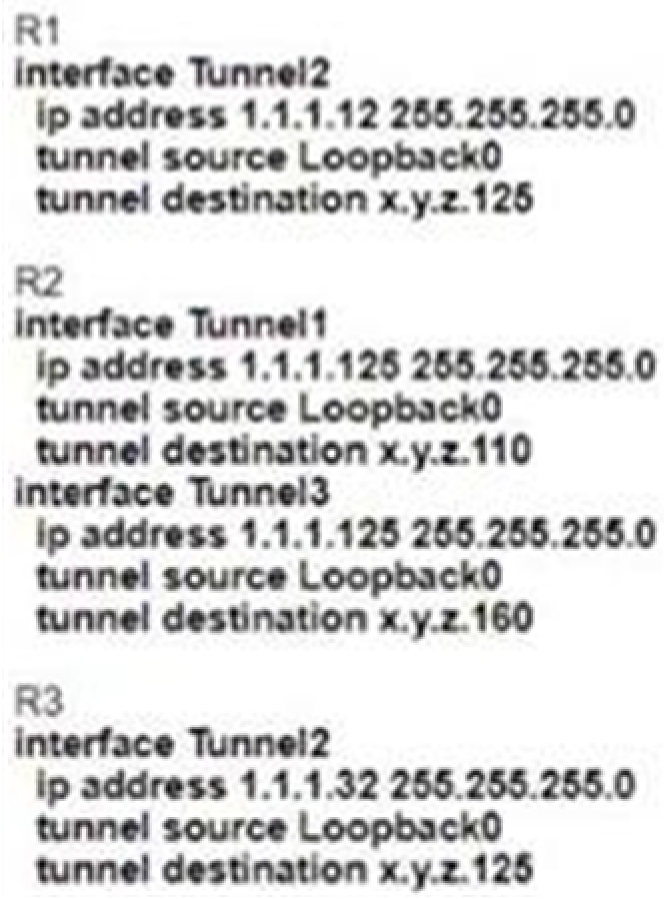
```
R1
interface Tunnel1
 ip address 1.1.1.13 255.255.255.0
 tunnel source Loopback0
 tunnel destination x.y.z.110

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

B.



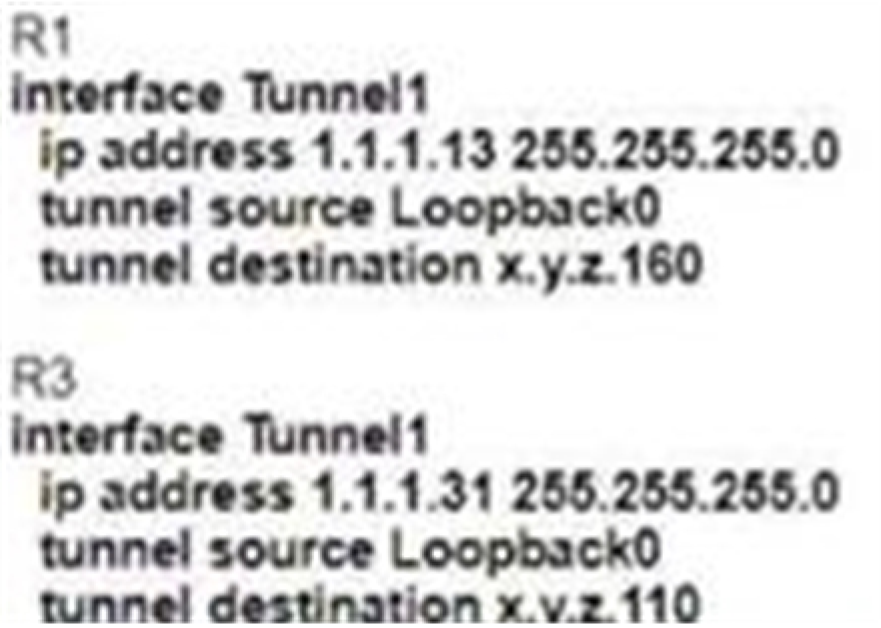
```
R1
interface Tunnel1
 ip address 1.1.1.13 255.255.255.0
 tunnel source Loopback0
 tunnel destination x.y.z.110

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.

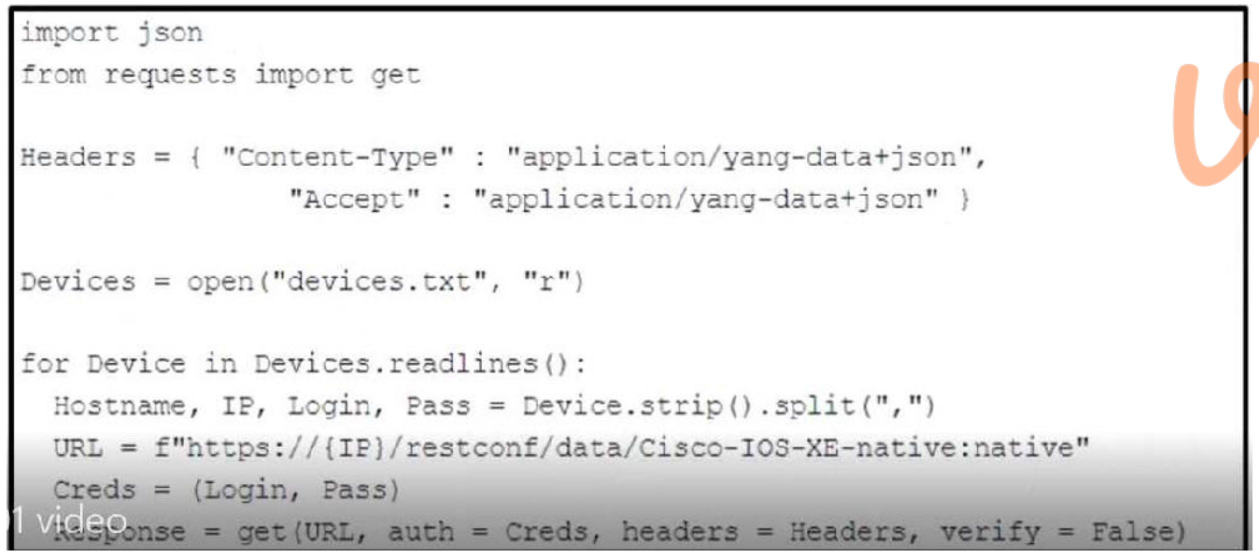


```
R1
interface Tunnel1
 ip address 1.1.1.13 255.255.255.0
 tunnel source Loopback0
 tunnel destination x.y.z.160

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

Correct Answer: D
Section:

QUESTION 314

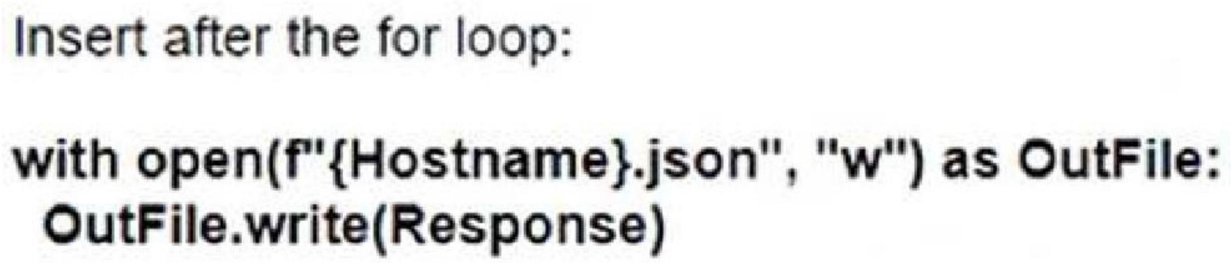
Refer to the exhibit.



```
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?

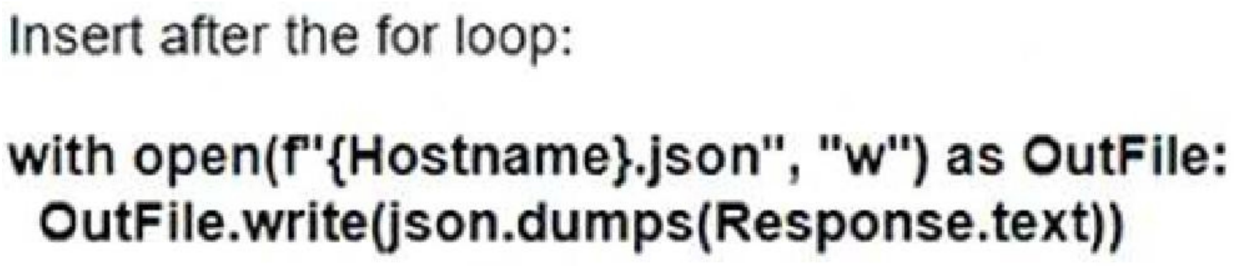
A.



Insert after the for loop:

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

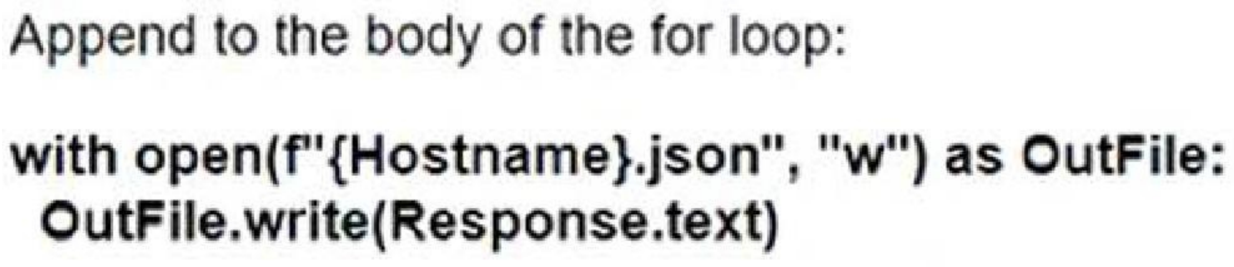
B.



Insert after the for loop:

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

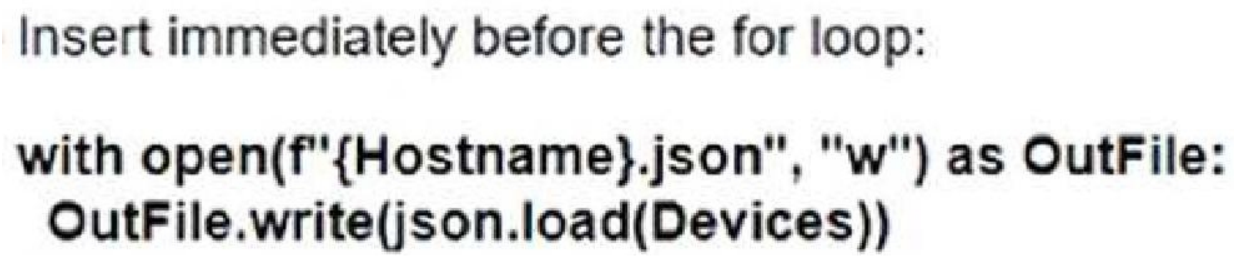
C.



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))
```

Correct Answer: A
Section:

QUESTION 315
Which option works with a DHCP server to return at least one WLAN management interface IP address during the discovery phase and is dependent upon the VCI of the AP?

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

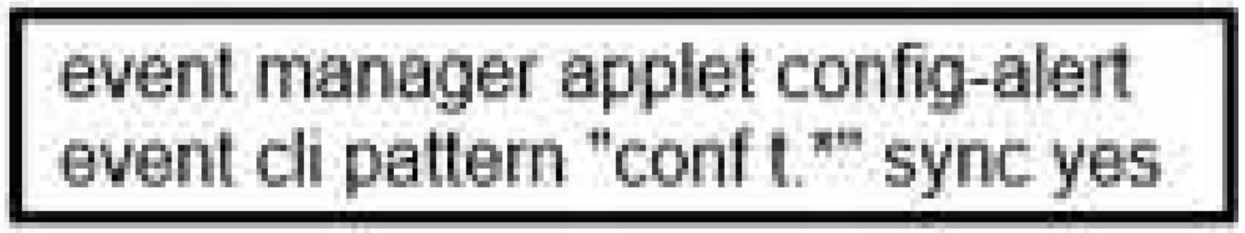
Correct Answer: D
Section:

QUESTION 316
What is a characteristics of traffic policing?

A. lacks support for marking or remarking
B. must be applied only to outgoing traffic
C. can be applied in both traffic directions
D. queues out-of-profile packets until the buffer is full

Correct Answer: D
Section:

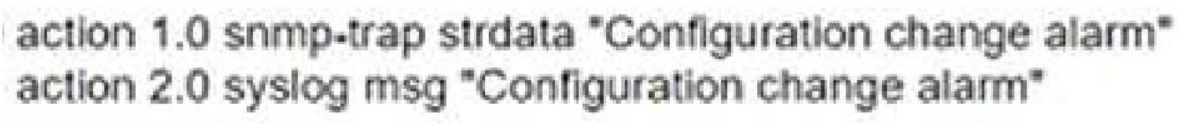
QUESTION 317
Reter to the exhibit.



```
event manager applet config-alert
event cli pattern "conf t.*" sync yes
```

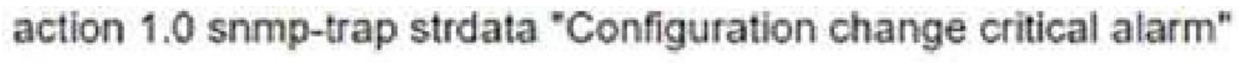
Refer to the exhibit. A network engineer must be notified when a user switches to configuration mode. Which script should be applied to receive an SNMP trap and a critical-level log message?

A.



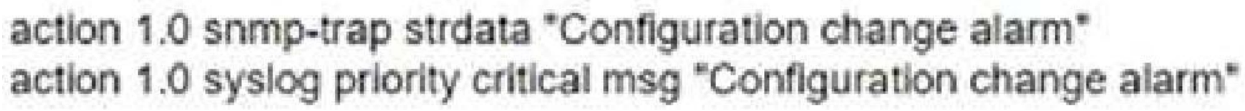
```
action 1.0 snmp-trap strdata "Configuration change alarm"
action 2.0 syslog msg "Configuration change alarm"
```

B.



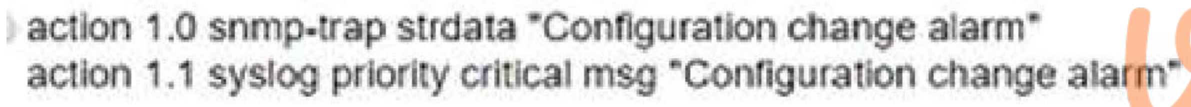
```
action 1.0 snmp-trap strdata "Configuration change critical alarm"
```

C.



```
action 1.0 snmp-trap strdata "Configuration change alarm"
action 1.0 syslog priority critical msg "Configuration change alarm"
```

D.



```
action 1.0 snmp-trap strdata "Configuration change alarm"
action 1.1 syslog priority critical msg "Configuration change alarm"
```

Correct Answer: D
Section:

QUESTION 318
A Cisco DNA Center REST API sends a PUT to the /dna/intent/api/v1/network-device endpoint A response code of 504 is received What does the code indicate?

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

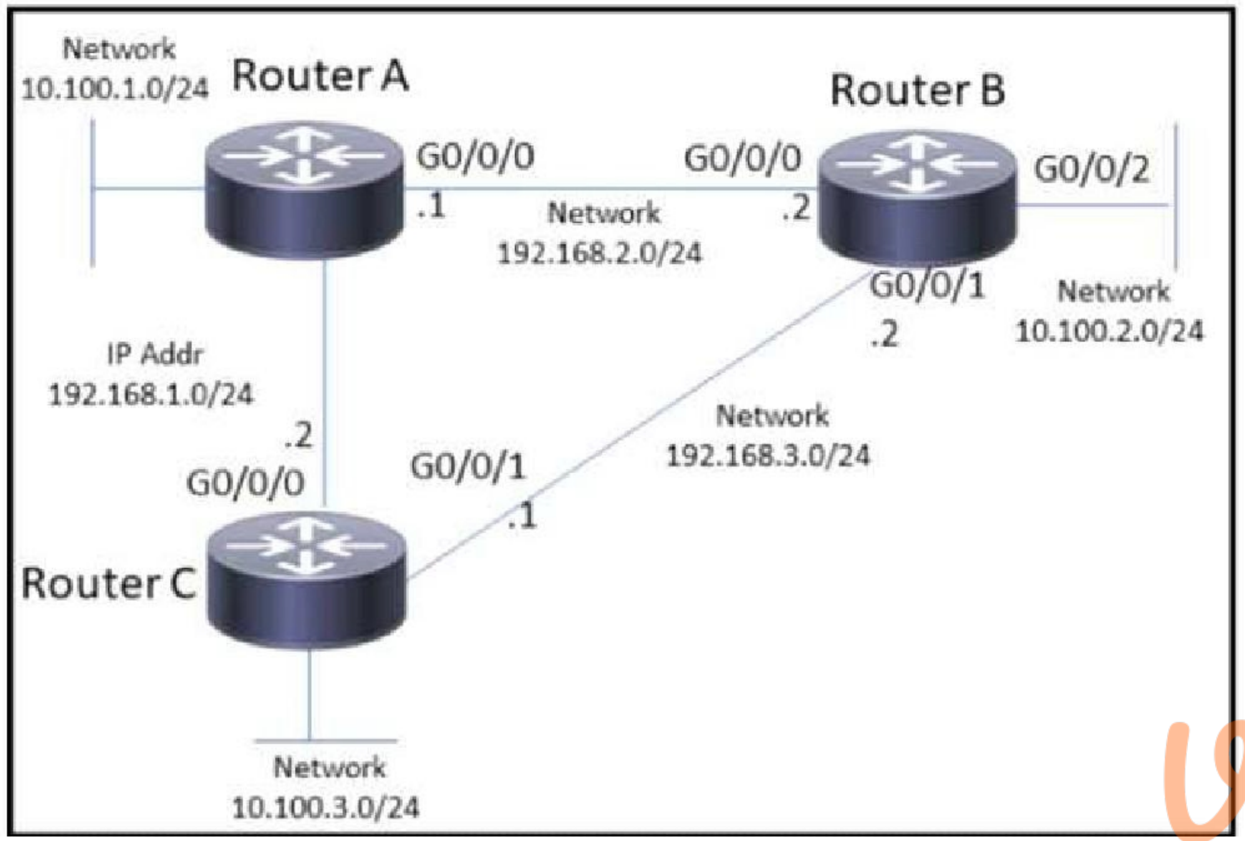
Correct Answer: A
Section:

QUESTION 319
Which component transports data plane traffic across a Cisco SD-WAN network?

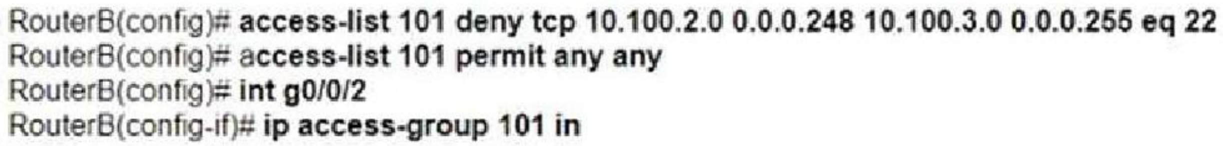
A. vSmart
B. vManage
C. cEdge
D. vBond

Correct Answer: D
Section:

QUESTION 320
Refer to the exhibit. A network engineer must block Telnet traffic from hosts in the range of 10.100 2.248 to 10.100.2 255 to the network 10.100.3.0 and permit everything else. Which configuration must the engineer apply'?

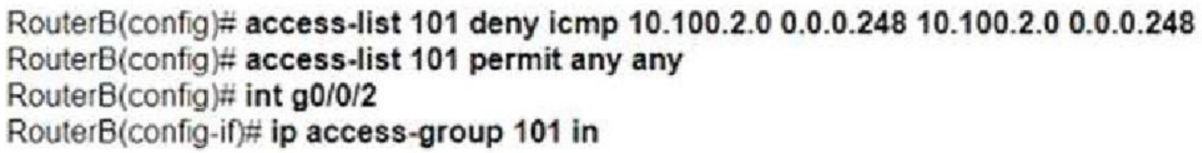


A.



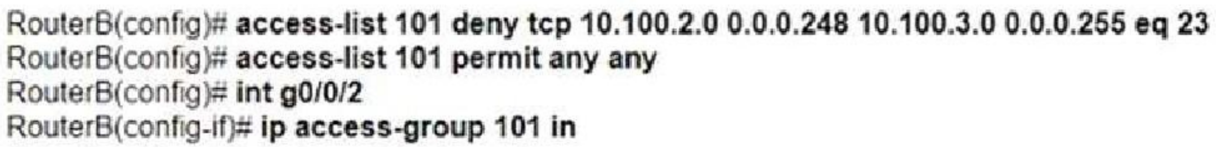
```
RouterB(config)# access-list 101 deny tcp 10.100.2.0 0.0.0.248 10.100.3.0 0.0.0.255 eq 22
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

B.



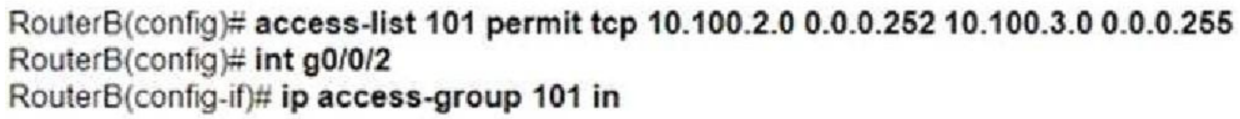
```
RouterB(config)# access-list 101 deny icmp 10.100.2.0 0.0.0.248 10.100.2.0 0.0.0.248
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

C.



```
RouterB(config)# access-list 101 deny tcp 10.100.2.0 0.0.0.248 10.100.3.0 0.0.0.255 eq 23
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

D.



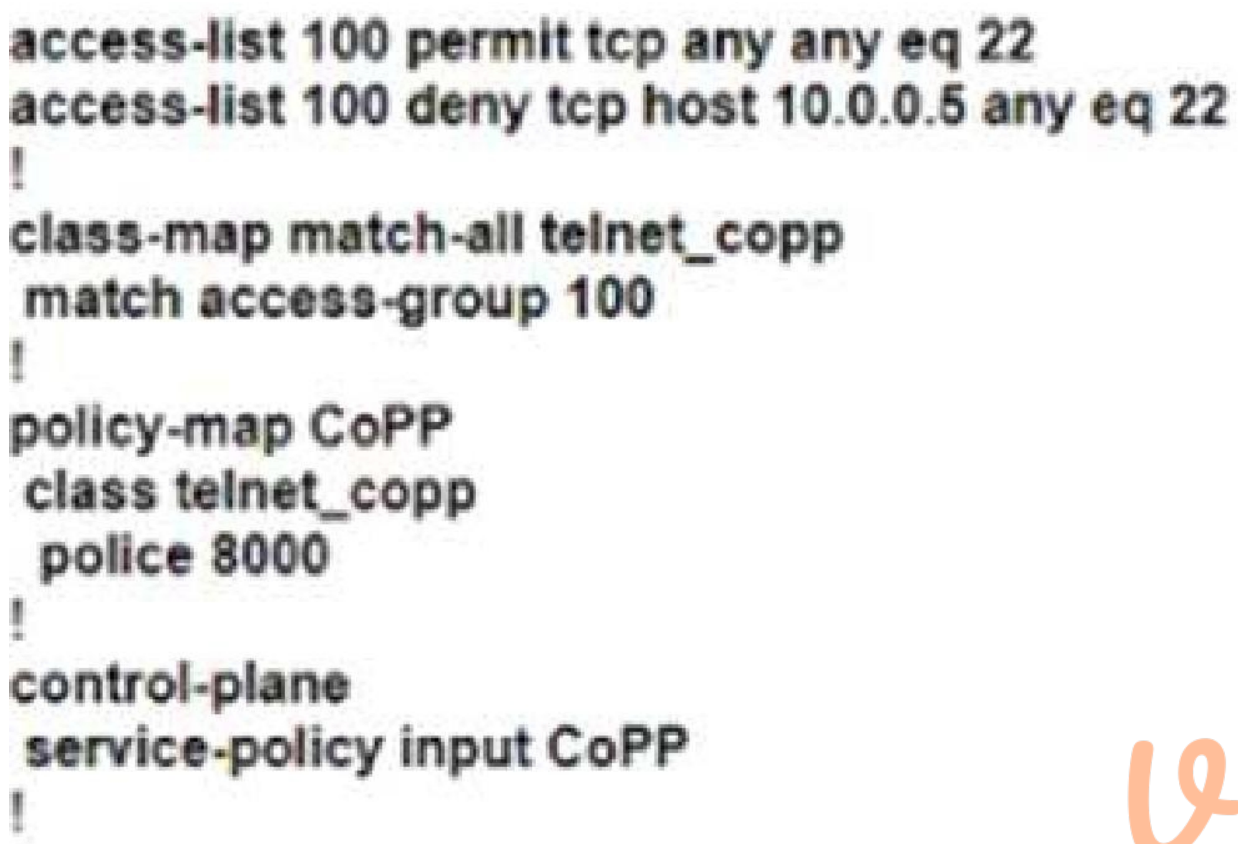
```
RouterB(config)# access-list 101 permit tcp 10.100.2.0 0.0.0.252 10.100.3.0 0.0.0.255
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

Correct Answer: C
Section:

QUESTION 321

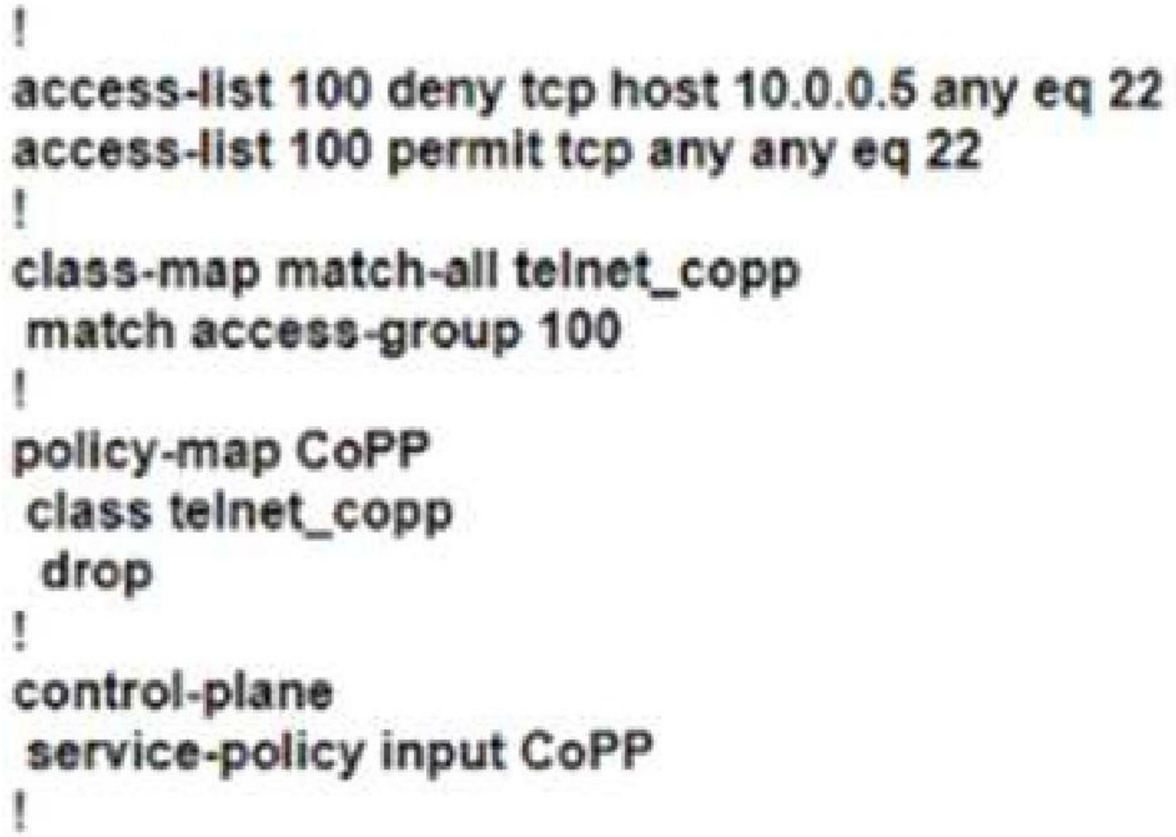
Which configuration creates a CoPP policy that provides unlimited SSH access from dient 10.0.0.5 and denies access from all other SSH clients'?

A.



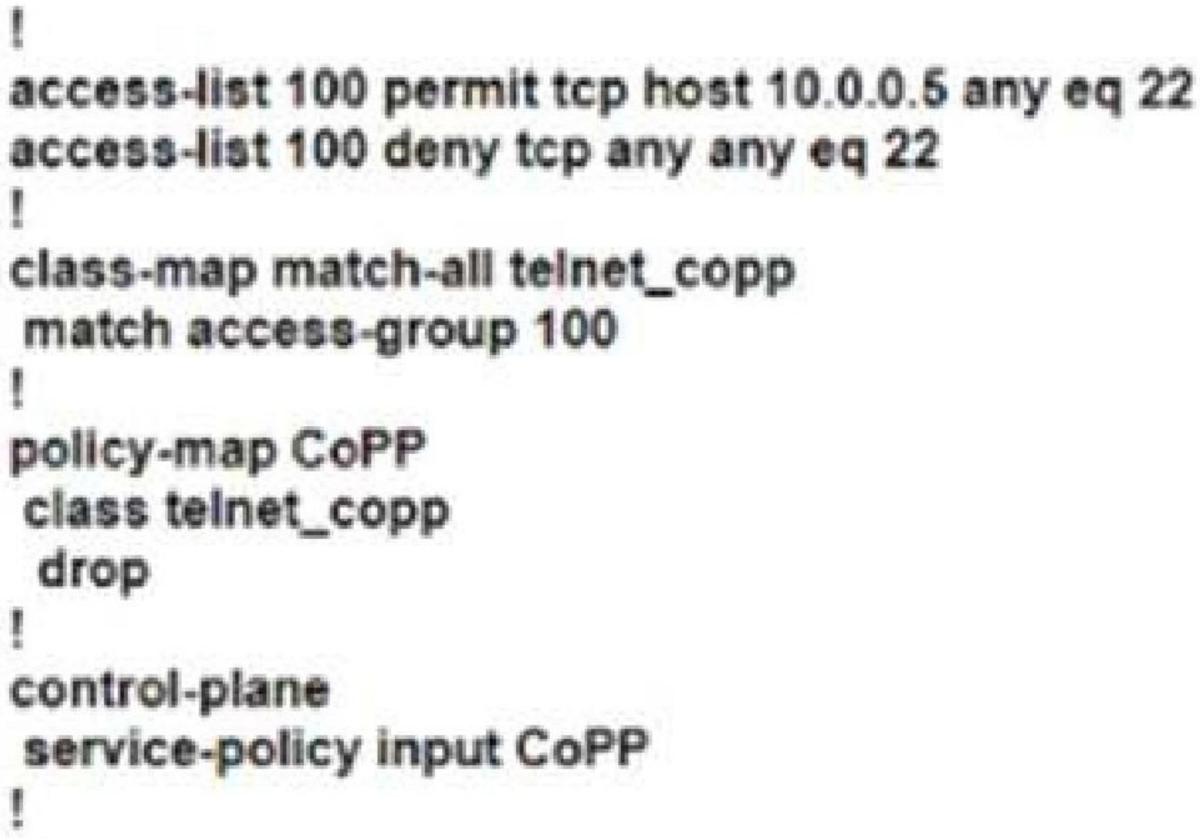
```
access-list 100 permit tcp any any eq 22
access-list 100 deny tcp host 10.0.0.5 any eq 22
!
class-map match-all telnet_copp
 match access-group 100
!
policy-map CoPP
 class telnet_copp
  police 8000
!
control-plane
 service-policy input CoPP
!
```

B.



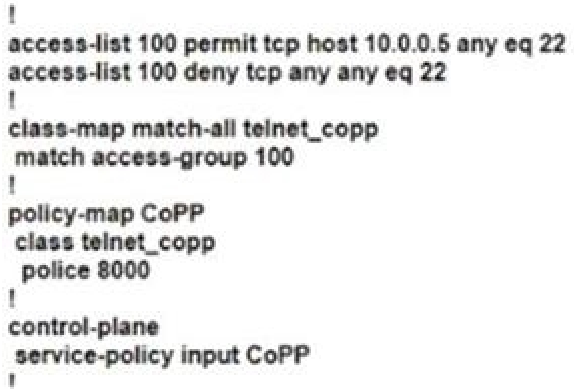
```
!
access-list 100 deny tcp host 10.0.0.5 any eq 22
access-list 100 permit tcp any any eq 22
!
class-map match-all telnet_copp
 match access-group 100
!
policy-map CoPP
 class telnet_copp
  drop
!
control-plane
 service-policy input CoPP
!
```

C.



```
!
access-list 100 permit tcp host 10.0.0.5 any eq 22
access-list 100 deny tcp any any eq 22
!
class-map match-all telnet_copp
 match access-group 100
!
policy-map CoPP
 class telnet_copp
  drop
!
control-plane
 service-policy input CoPP
!
```

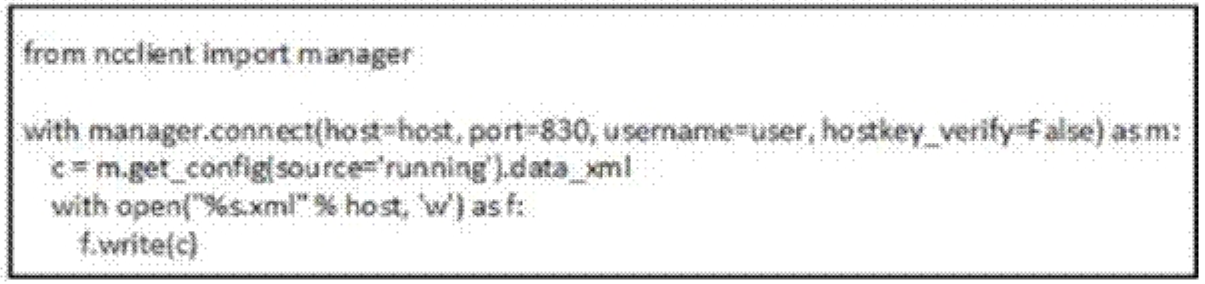
D.



```
!
access-list 100 permit tcp host 10.0.0.5 any eq 22
access-list 100 deny tcp any any eq 22
!
class-map match-all telnet_copp
 match access-group 100
!
policy-map CoPP
 class telnet_copp
  police 8000
!
control-plane
 service-policy input CoPP
!
```

Correct Answer: B
Section:

QUESTION 322
Refer to the exhibit. What is generated by the script?



```
from ncclient import manager

with manager.connect(host=host, port=830, username=user, hostkey_verify=False) as m:
  c = m.get_config(source='running').data_xml
  with open("%s.xml" % host, 'w') as f:
    f.write(c)
```

A. the cdp neighbors

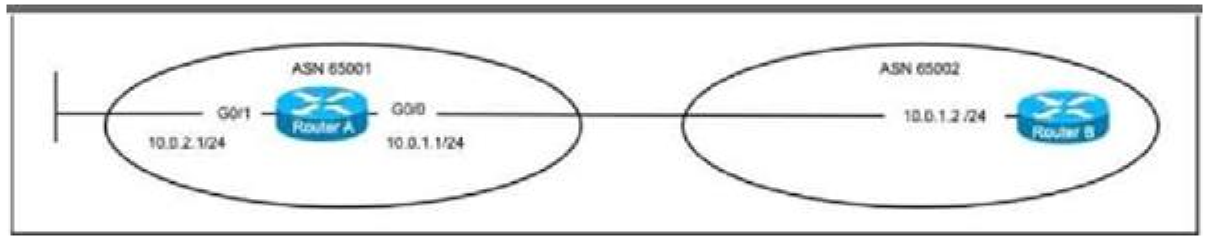
B. the routing table

C. the router processes

D. the running configuration

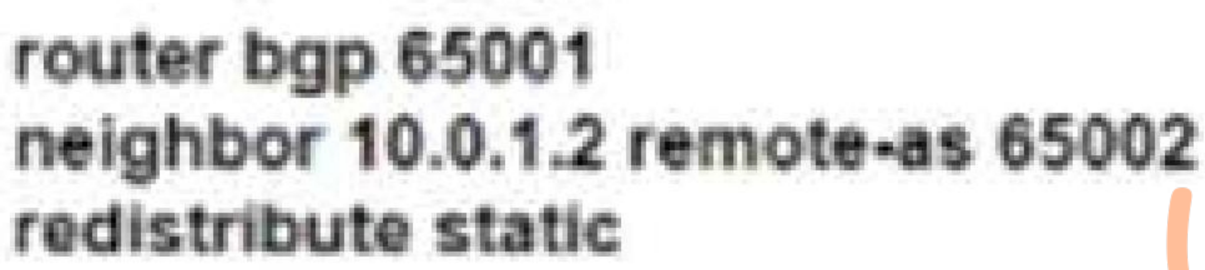
Correct Answer: D
Section:

QUESTION 323
Reter to the exhibit.



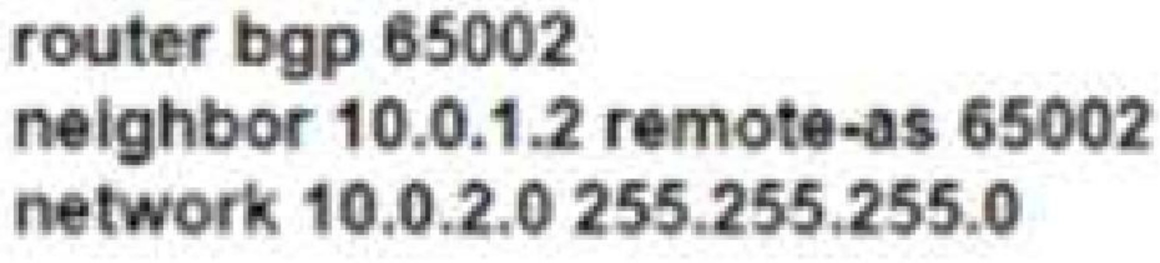
Refer to the exhibit. An engineer must configure an eBGP neighborship to Router B on Router A.
The network that is connected to GO/1 on Router A must be advertised to Router B. Which configuration should be applied?

A)



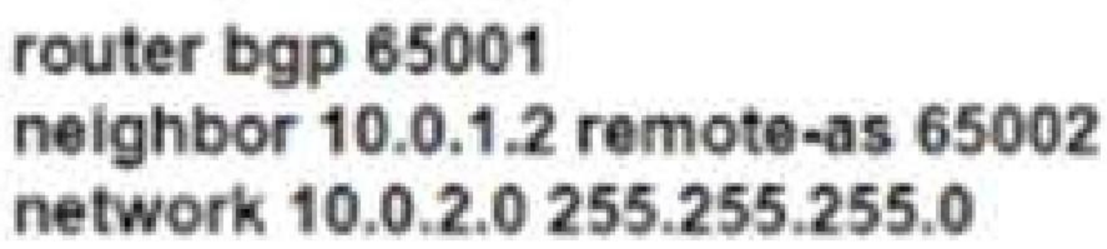
```
router bgp 65001
neighbor 10.0.1.2 remote-as 65002
redistribute static
```

B)



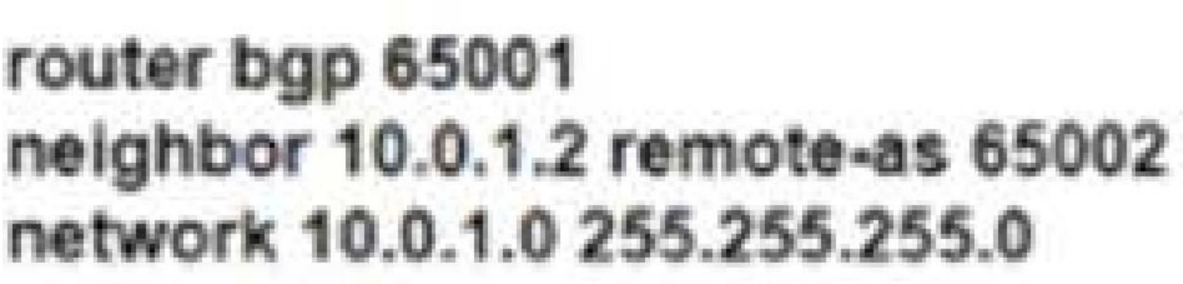
```
router bgp 65002
neighbor 10.0.1.2 remote-as 65002
network 10.0.2.0 255.255.255.0
```

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
```

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

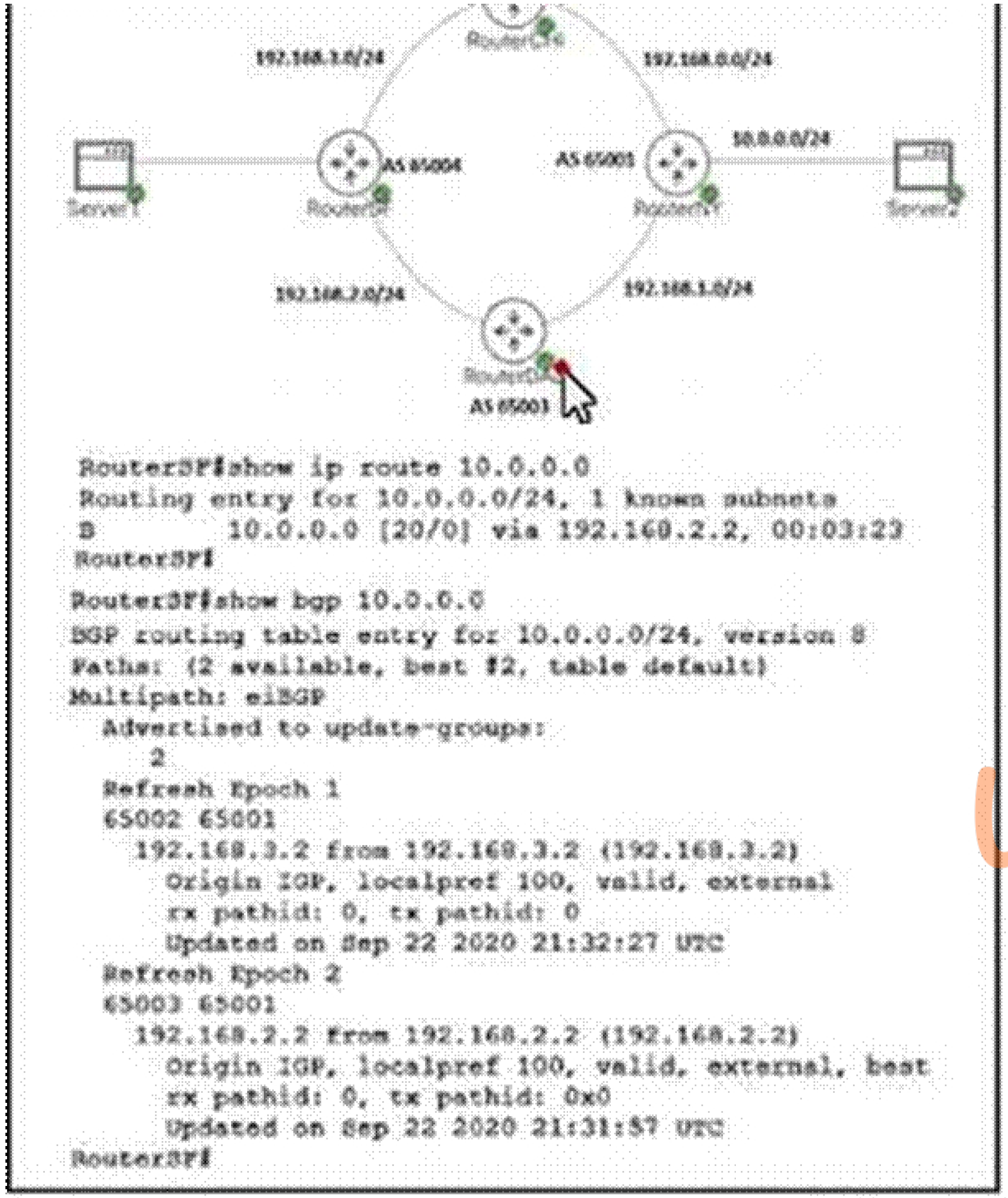
Correct Answer: C
Section:

QUESTION 324
Which benefit is provided by the Cisco DNA Center telemetry feature?

A. provides improved network security
B. inventories network devices
C. aids In the deployment network configurations
D. improves the user experience

Correct Answer: B
Section:

QUESTION 325
Refer to the exhibit.



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

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

A. The Router-ID Tor Router DAL is lower than the Roter-ID for RouterCHI.

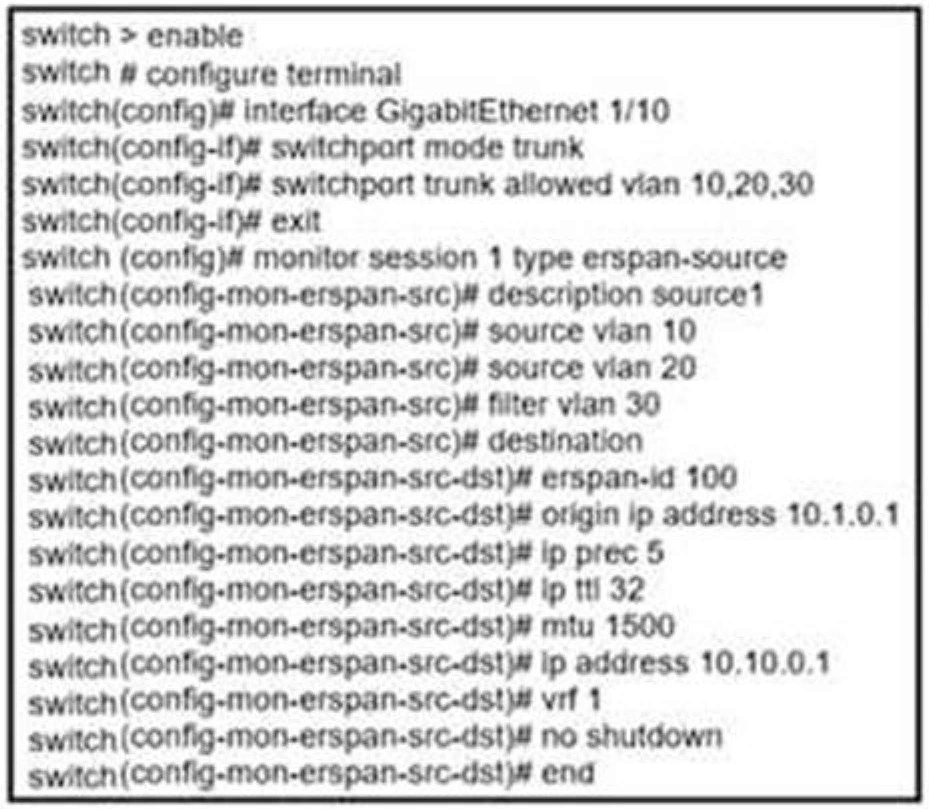
B. The route from RouterOAL has a lower MED.

C. BGP is not running on RouterCHI.

D. There is a static route in RouterSF for 10.0.0.0/24.

Correct Answer: A
Section:

QUESTION 326
Reter to the exhibit.



```
switch > enable
switch # configure terminal
switch(config)# interface GigabitEthernet 1/10
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 10,20,30
switch(config-if)# exit
switch (config)# monitor session 1 type erspan-source
 switch(config-mon-erspan-src)# description source1
 switch(config-mon-erspan-src)# source vlan 10
 switch(config-mon-erspan-src)# source vlan 20
 switch(config-mon-erspan-src)# filter vlan 30
 switch(config-mon-erspan-src)# destination
 switch(config-mon-erspan-src-dst)# erspan-id 100
 switch(config-mon-erspan-src-dst)# origin ip address 10.1.0.1
 switch(config-mon-erspan-src-dst)# ip prec 5
 switch(config-mon-erspan-src-dst)# ip ttl 32
 switch(config-mon-erspan-src-dst)# mtu 1500
 switch(config-mon-erspan-src-dst)# ip address 10.10.0.1
 switch(config-mon-erspan-src-dst)# vrf 1
 switch(config-mon-erspan-src-dst)# no shutdown
 switch(config-mon-erspan-src-dst)# end
```

An engineer configures the trunk and proceeds to configure an ESPAN session to monitor VLANs10. 20. and 30. Which command must be added to complete this configuration?

A. Device(config.mon.erspan.stc)# no filter vlan 30
B. Devic(config.mon.erspan.src-dst)# no vrf 1
C. Devic(config.mon.erspan.src-dst)# erspan id 6
D. Device(config.mon-erspan.Src-dst)# mtu 1460

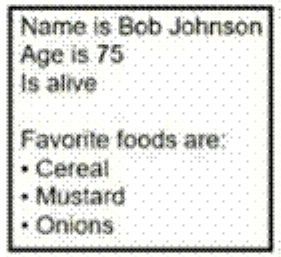
Correct Answer: A
Section:

QUESTION 327
By default, which virtual MAC address Goes HSRP group 25 use?

A. 05:5c:5e:ac:0c:25
B. 04:16:6S:96:1C:19
C. 00:00:0c:07:ac:19
D. 00:00:0c:07:ac:25

Correct Answer: C
Section:
Explanation:
https://www.rapidtables.com/convert/number/hex-to-decimal.html (19) = $(1 \times 16^1) + (9 \times 16^0)$ = (25)

QUESTION 328
Reter to the exhibit.



Name is Bob Johnson
Age is 75
Is alive

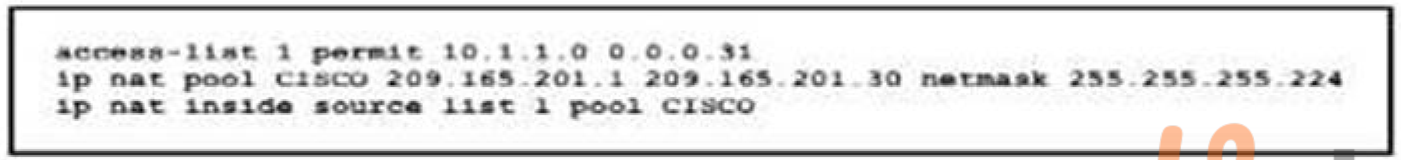
Favorite foods are:
- Cereal
- Mustard
- Onions

What is the JSON syntax that is formed the data?

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

Correct Answer: B
Section:

QUESTION 329
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.

Correct Answer: A, E
Section:

QUESTION 330
In a Cisco Catalyst switch equipped with two supervisor modules an administrator must temporally remove the active supervisor from the chassis to perform hardware maintenance on it. Which mechanism ensure that the active supervisor removal is not disruptive to the network operation?

A. NSF/NSR
B. SSO
C. HSRP
D. VRRP

Correct Answer: B
Section:

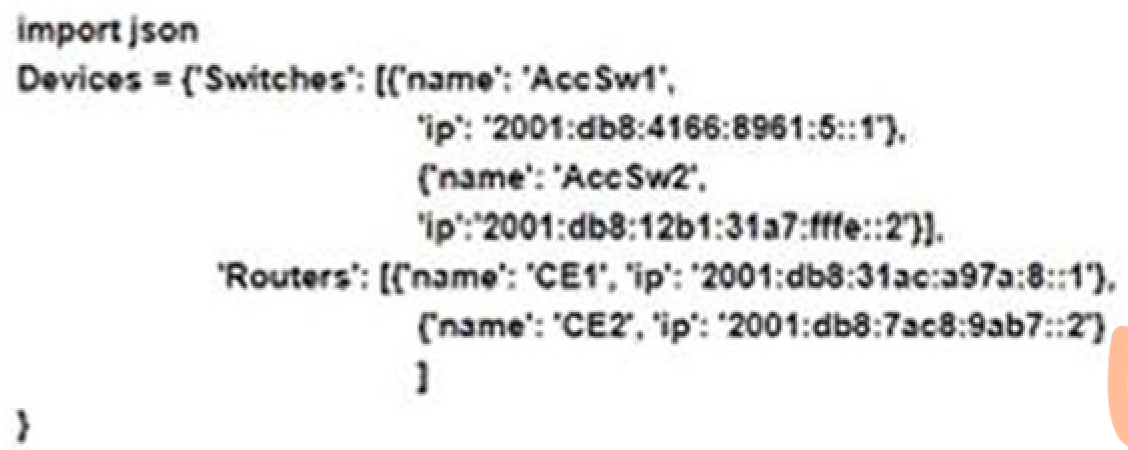
QUESTION 331

A company requires a wireless solution to support its mam office and multiple branch locations. All sites have local Internet connections and a link to the main office lor corporate connectivity. The branch offices are managed centrally.
Which solution should the company choose?

A. Cisco United Wireless Network
B. Cisco DNA Spaces
C. Cisco Catalyst switch with embedded controller
D. Cisco Mobility Express

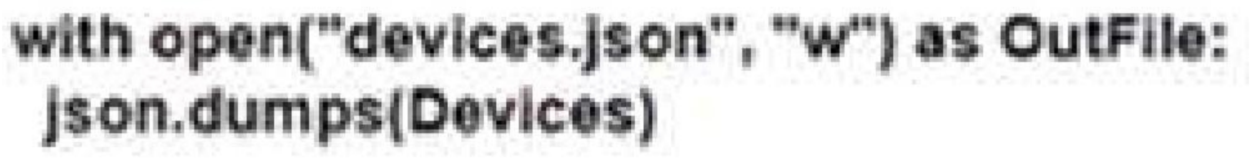
Correct Answer: B
Section:

QUESTION 332
Which Python snippet should be used to store the devices data structure in a JSON file?



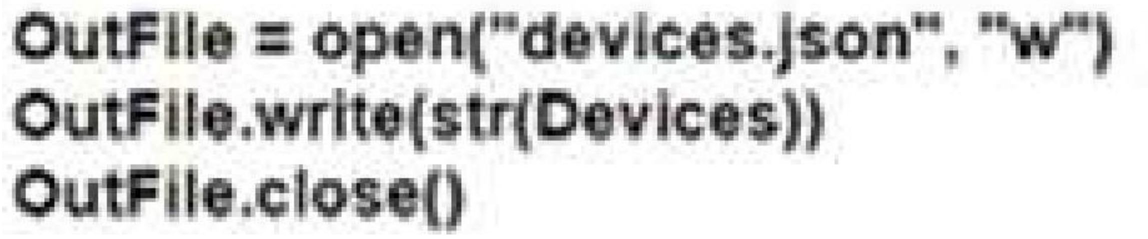
```
import json
Devices = {'Switches': [{'name': 'AccSw1',
                         'ip': '2001:db8:4166:8961:5::1'},
                         {'name': 'AccSw2',
                         'ip':'2001:db8:12b1:31a7:fffe::2'}],
           'Routers': [{'name': 'CE1', 'ip': '2001:db8:31ac:a97a:8::1'},
                         {'name': 'CE2', 'ip': '2001:db8:7ac8:9ab7::2'}
                         ]
}
```

A.



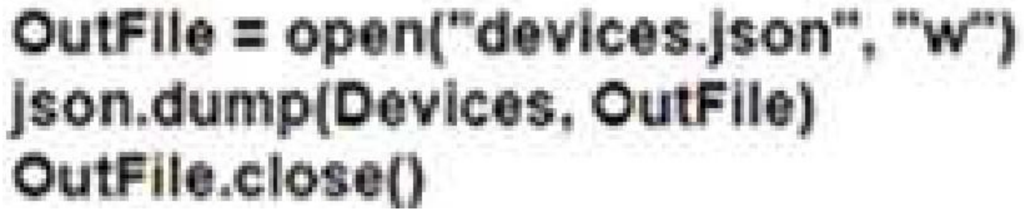
```
with open("devices.json", "w") as OutFile:
  json.dumps(Devices)
```

B.



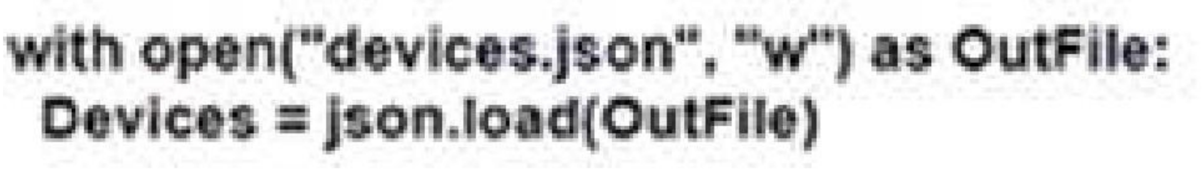
```
OutFile = open("devices.json", "w")
OutFile.write(str(Devices))
OutFile.close()
```

C.



```
OutFile = open("devices.json", "w")
json.dump(Devices, OutFile)
OutFile.close()
```

D.



```
with open("devices.json", "w") as OutFile:
  Devices = json.load(OutFile)
```

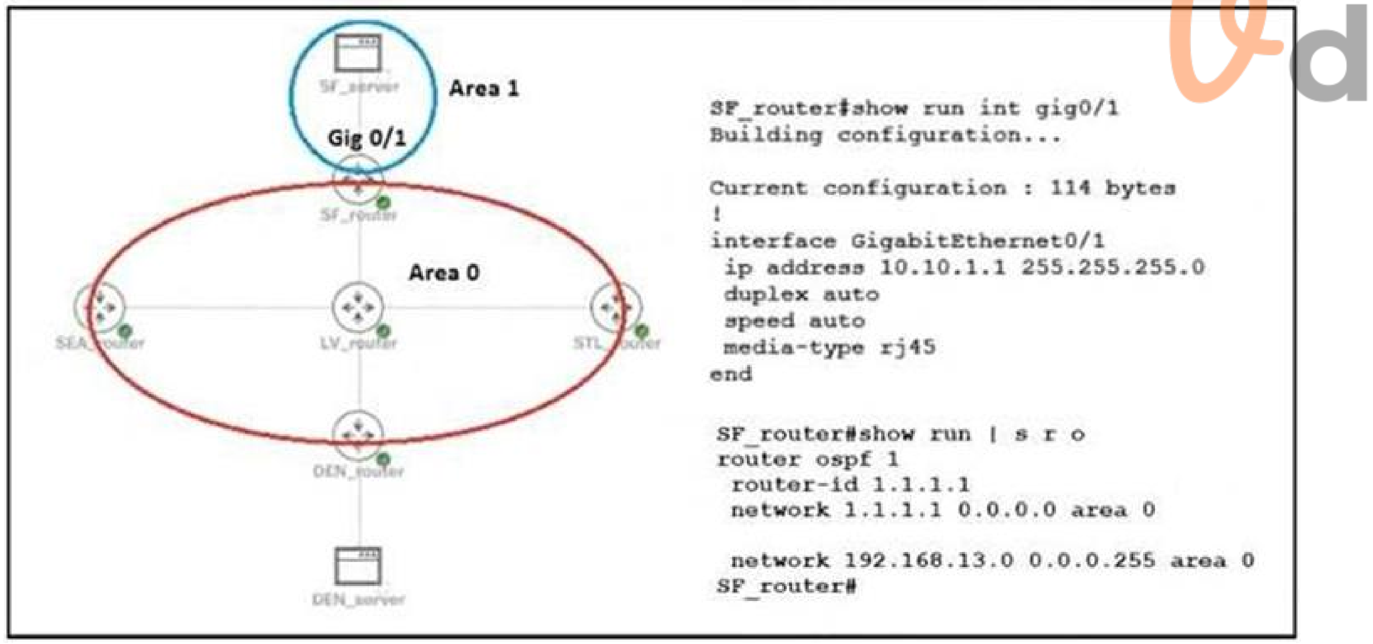
Correct Answer: A
Section:

QUESTION 333
Which type of tunnel Is required between two WLCs to enable Intercontroller roaming?

A. mobility
B. LWAPP
C. CAPWAP
D. iPsec

Correct Answer: A
Section:

QUESTION 334
Reter to the exhibit.



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

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

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

  network 192.168.13.0 0.0.0.255 area 0
 SF_router#
```

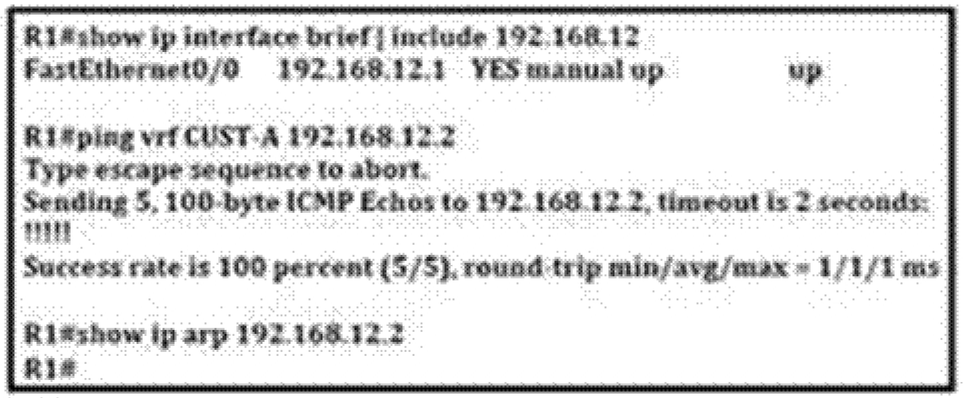
Refer to the exhibit. Which configuration must be added to enable GigabitEthemet 0/1 to participate in OSPF?

A. SF_router (config-router)# network 10.10.1.0 0.0.0.255 area 0
B. SF_rouier (conng)# network 10.10.1.0 0.0.0.255 area 1
C. SF_router (conflg-routerp) network 10.10.1.0 0.0.0.255 area 1
D. SF_rouler (contlg-rouler)# network 10.10.1.0 255.255.255.0 area 0

Correct Answer: C
Section:

QUESTION 335

Reter to the exhibit.



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

R1#ping vrf CUST-A 192.168.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R1#show ip arp 192.168.12.2
R1#
```

Refer to the exhibit. A network engineer checks connectivity between two routers. The engineer can ping the remote endpoint but cannot see an ARP entry. Why is there no ARP entry?

A. The ping command must be executed in the global routing table.

B. Interface FastEthernet0/0 Is configured in VRF CUST-A, so the ARP entry is also in that VRF.

C. When VRFs are used. ARP protocol must be enabled In each VRF.

D. When VRFs are used. ARP protocol is disabled in the global routing table.

Correct Answer: B

Section:

QUESTION 336

Which protocol is responsible for data plane forwarding in a Cisco SD-Access deployment?

A. VXLAN

B. IS-IS

C. OSPF

D. LISP

Correct Answer: A

Section:

QUESTION 337

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

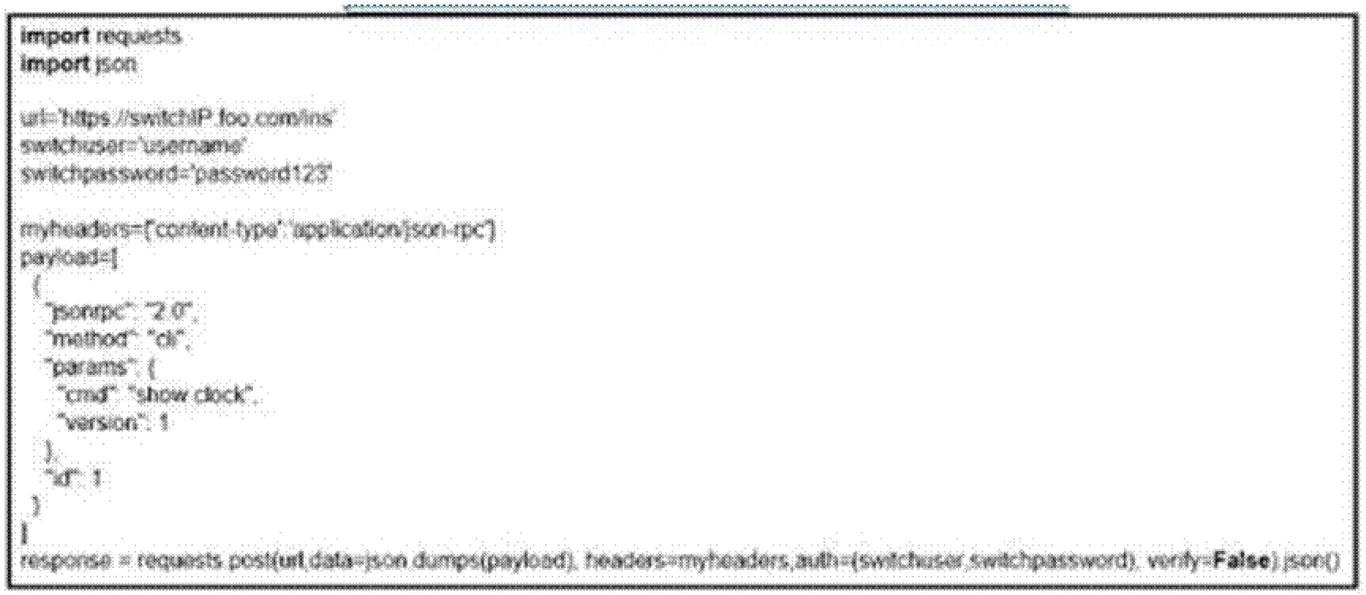
D. It configures security policies down to wireless clients in the fabric.

Correct Answer: B

Section:

QUESTION 338

Reter to the exhibit.



```
import requests
import json

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

myheaders={'content-type':'application/json-rpc'}
payload=[
 {
  "jsonrpc": "2.0",
  "method": "cli",
  "params": {
   "cmd": "show clock",
   "version": 1
  },
  "id": 1
 }
]
response = requests.post(url,data=json.dumps(payload), headers=myheaders,auth=(switchuser,switchpassword), verify=False).json()
```

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

A. print(response['resut'][0||'simple_time']}

B. print(response[result']['body']['simple_time']}

C. print(response['body']['simple_time']}

D. print(response[jresult']['body']['simple_time']}

Correct Answer: B
Section:

QUESTION 339
what is a benefit of using a Type 2 hypervisor instead of a Type 1 hypervisor?

A. better application performance

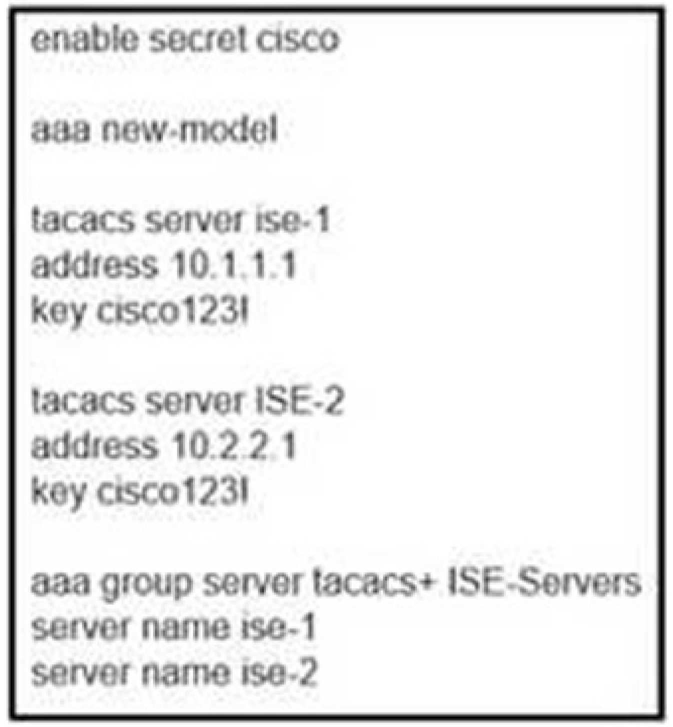
B. Improved security because the underlying OS is eliminated

C. Improved density and scalability

D. ability to operate on hardware that is running other OSs

Correct Answer: D
Section:

QUESTION 340
Refer to the exhibit.



```
enable secret cisco

aaa new-model

tacacs server ise-1
address 10.1.1.1
key cisco123l

tacacs server ISE-2
address 10.2.2.1
key cisco123l

aaa group server tacacs+ ISE-Servers
server name ise-1
server name ise-2
```

A network engineer must configure the router to use the ISE-Servers group for authentication. If both ISE servers are unavailable, the local username database must be used. If no usernames are defined in the configuration, then the enable password must be the last resort to log in. Which configuration must be applied to achieve this result?

A. aaa authentication login default group ISE-Servers local enable

B. aaa authentication login default group enable local ISE-Servers

C. aaa authorization exec default group ISE-Servers local enable

D. aaa authentication login error-enable aaa authentication login default group enable local ISE-Servers

Correct Answer: A
Section:

QUESTION 341
A large campus network has deployed two wireless LAN controllers to manage the wireless network.
WLC1 and WLC2 have been configured as mobility peers. A client device roams from AP1 on WLC1 to AP2 on WLC2, but the controller's client interfaces are on different VLANs. How do the wireless LAN controllers handle the inter-subnet roaming?

A. WLC1 marks me diem with an anchor entry In Its own database. The database entry is copied to the new controller and marked with a foreign entry on VVLC2.

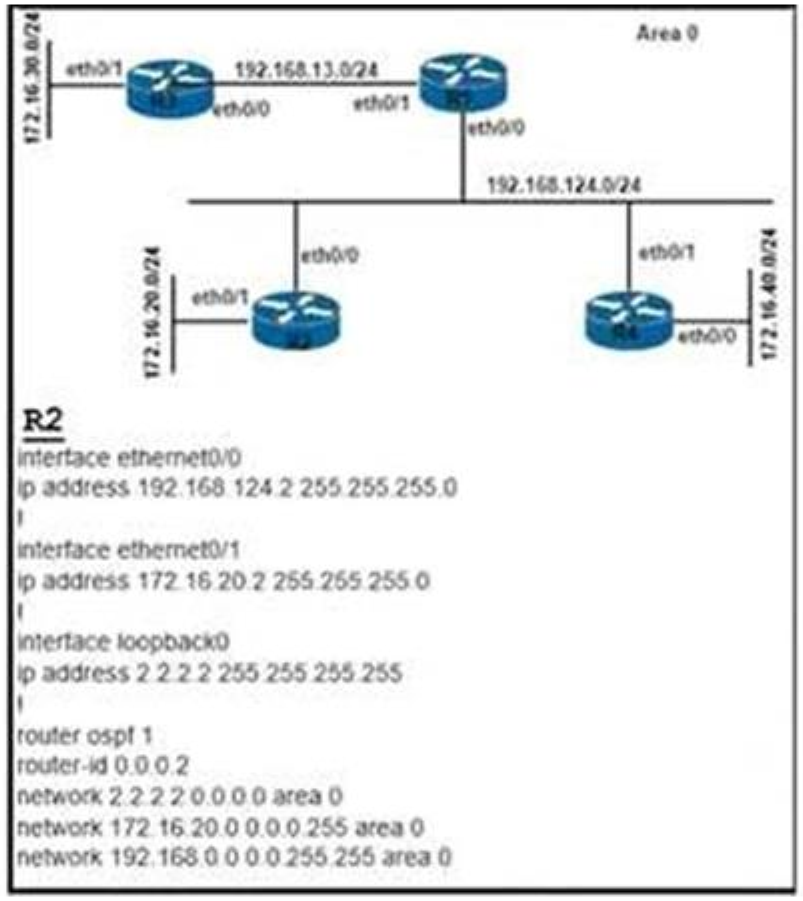
B. WLC2 marks the client with an anchor entry In Its own database. The database entry Is copied to the new controller and marked with a foreign entry on WLC1

C. WLCl marks the client with a foreign entry in its own database. The database entry is copied to the new controller and marked with an anchor entry on WLC2.

D. WLC2 marks the client with a foreign entry In its own database. The database entry Is copied to the new controller and marked with an anchor entry on WLC1.

Correct Answer: B
Section:

QUESTION 342
Reter to the exhibit.



R2

```
interface ethernet0/0
ip address 192.168.124.2 255.255.255.0
!
interface ethernet0/1
ip address 172.16.20.2 255.255.255.0
!
interface loopback0
ip address 2.2.2.2 255.255.255.255
!
router ospf 1
router-id 0.0.0.2
network 2.2.2.2 0.0.0.0 area 0
network 172.16.20.0 0.0.0.255 area 0
network 192.168.0.0 0.0.255.255 area 0
```

Refer to the exhibit. An attacker can advertise OSPF fake routes from 172.16.20.0 network to the OSPF domain and black hole traffic. Which action must be taken to avoid this attack and still be able to advertise this subnet into OSPF?

A. Configure 172.16.20.0 as a stub network.
B. Apply a policy to filter OSPF packets on R2.
C. Configure a passive Interface on R2 toward 172.16.20.0.
D. Configure graceful restart on the 172.16.20.0 interface.

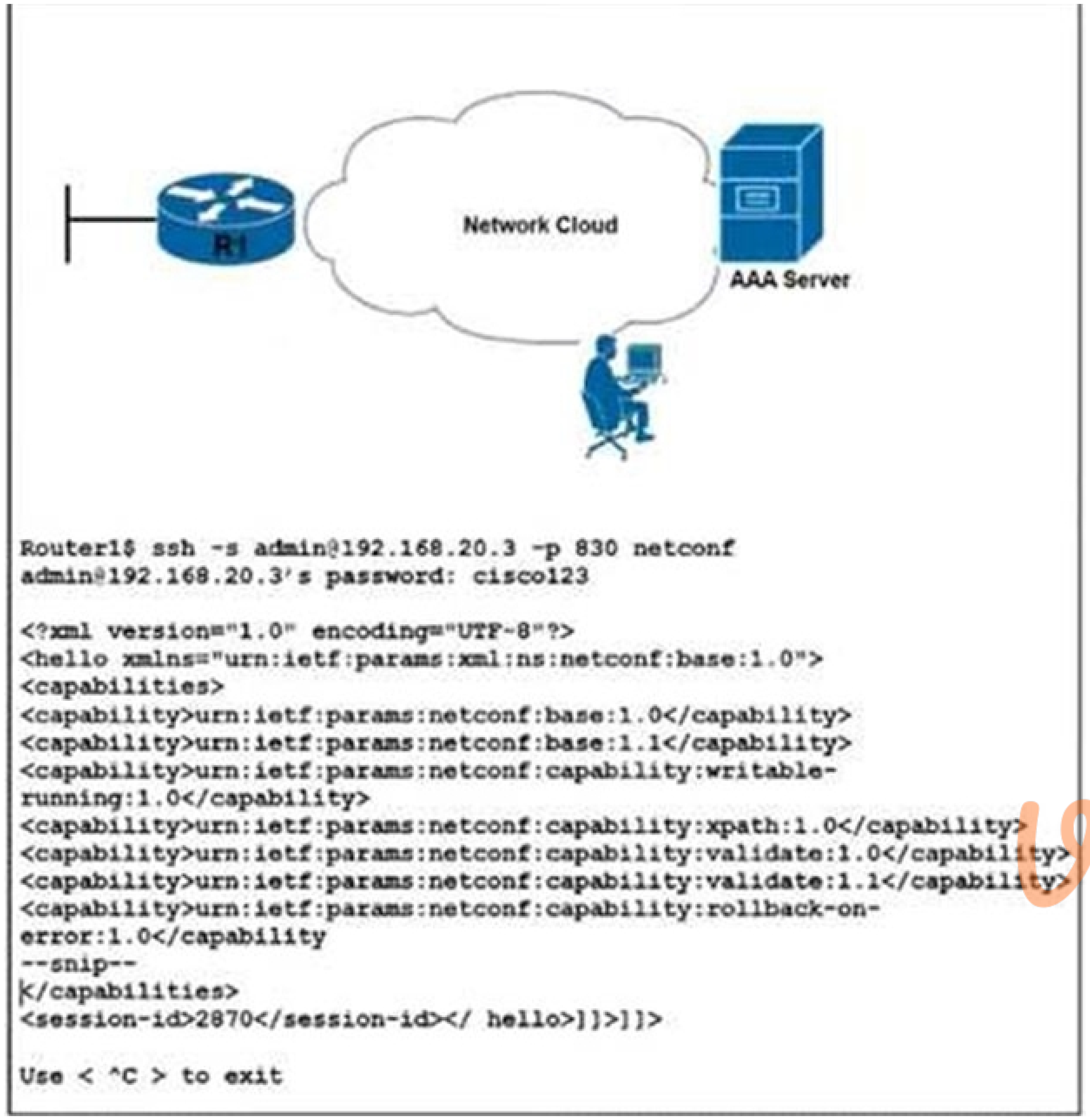
Correct Answer: C
Section:

QUESTION 343
What is the calculation that is used to measure the radiated power of a signal after it has gone through the radio, antenna cable, and antenna?

A. EIRP
B. mW
C. dBm
D. dBi

Correct Answer: A
Section:

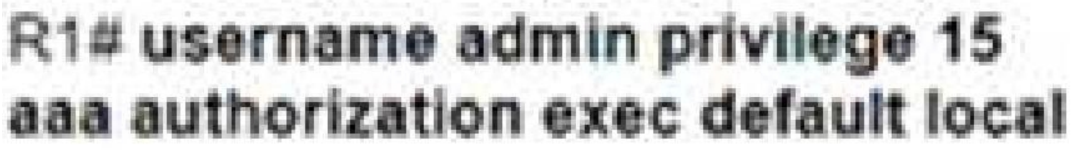
QUESTION 344
Reter to the exhibit.



```
Router1$ ssh -s admin@192.168.20.3 -p 830 netconf
admin@192.168.20.3's password: cisco123

<?xml version="1.0" encoding="UTF-8"?>
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<capabilities>
<capability>urn:ietf:params:netconf:base:1.0</capability>
<capability>urn:ietf:params:netconf:base:1.1</capability>
<capability>urn:ietf:params:netconf:capability:writable-
running:1.0</capability>
<capability>urn:ietf:params:netconf:capability:xpath:1.0</capability>
<capability>urn:ietf:params:netconf:capability:validate:1.0</capability>
<capability>urn:ietf:params:netconf:capability:validate:1.1</capability>
<capability>urn:ietf:params:netconf:capability:rollback-on-
error:1.0</capability
--snip--
</capabilities>
<session-id>2870</session-id></ hello>]]>]]>

Use < ^C > to exit
```

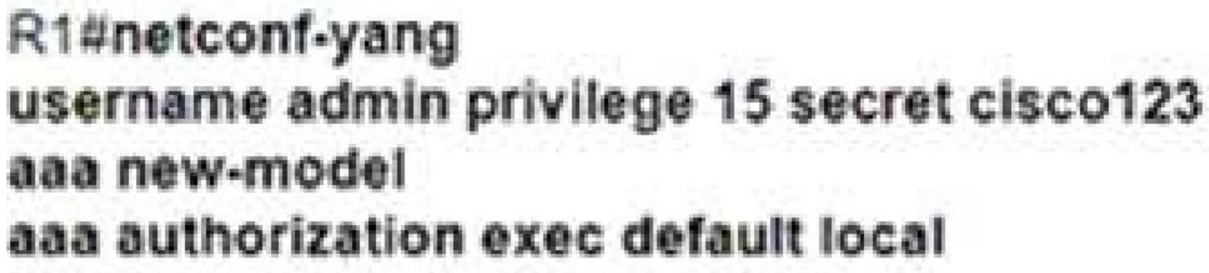
Refer to the exhibit. An engineer tries to log in to router R1. Which configuration enables a successful login?

A.



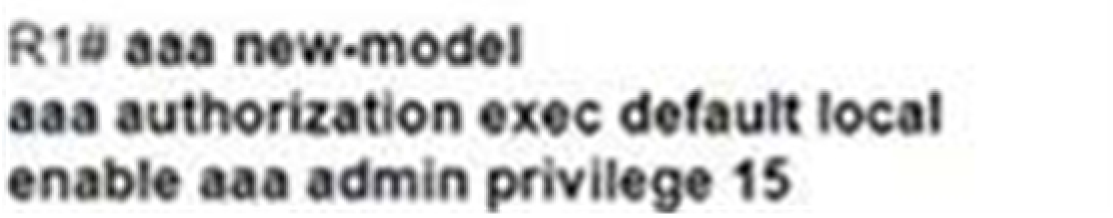
```
R1# username admin privilege 15
aaa authorization exec default local
```

B.



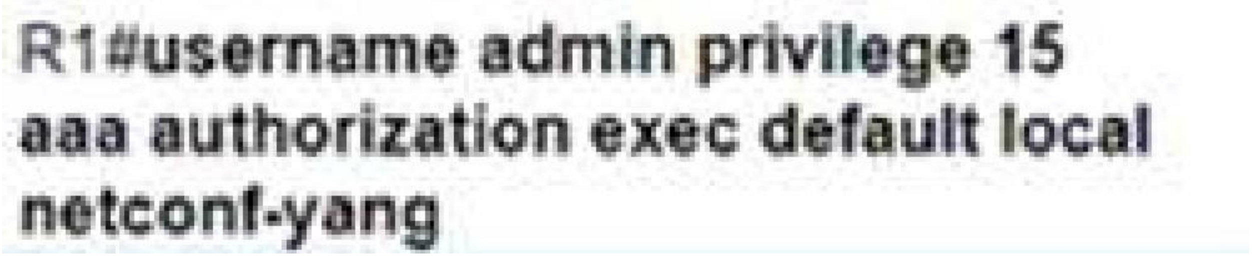
```
R1#netconf-yang
username admin privilege 15 secret cisco123
aaa new-model
aaa authorization exec default local
```

C.



```
R1# aaa new-model
aaa authorization exec default local
enable aaa admin privilege 15
```

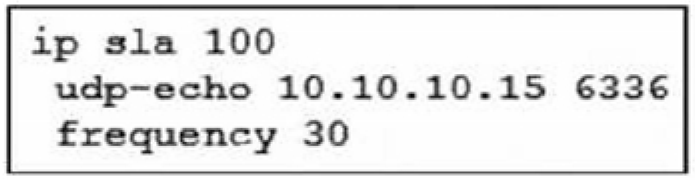
D.



```
R1#username admin privilege 15
aaa authorization exec default local
netconf-yang
```

Correct Answer: B
Section:

QUESTION 345
Reter to the exhibit.



```
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

Correct Answer: A
Section:

QUESTION 346
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'

Correct Answer: B
Section:

QUESTION 347
What is one main REST security design principle?

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

Correct Answer: A
Section:
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/securityessentials/#:~:text=REST%20Security%20Design%20Principles&text=Least%20Privilege%3A%20An%20entity%20should,when%20no%20longer%20in%20use.

QUESTION 348
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

Correct Answer: B
Section:

QUESTION 349
What is the recommended minimum SNR for data applications on wireless networks?

A. 15
B. 20
C. 25
D. 10

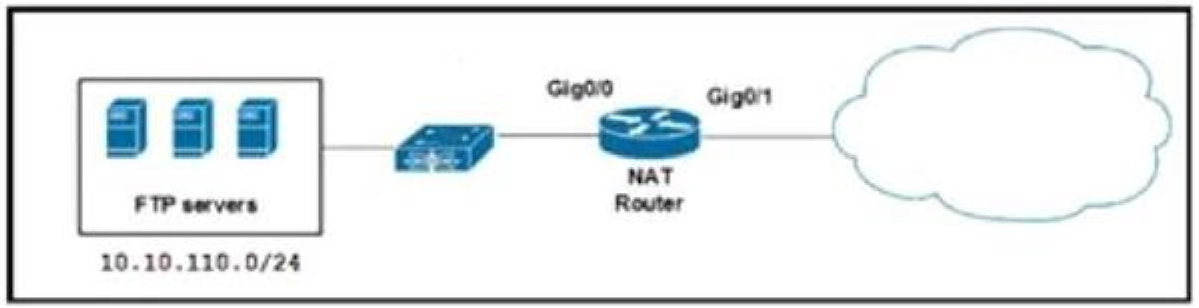
Correct Answer: B
Section:
Explanation:
Generally, a signal with an SNR value of 20 dB or more is recommended for data networks where as an SNR value of 25 dB or more is recommended for networks that use voice applications
https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_(SNR)_and_Wireless_Signal_Strength#:~:text=Generally%2C%20a%20signal%20with%20an,networks%20that%20use%20voice%20applications.

QUESTION 350
A system must validate access rights to all its resources and must not rely on a cached permission matrix. If the access level to a given resource is revoked but is not reflected in the permission matrix, the security is violates Which term refers to this REST security design principle?

A. economy of mechanism
B. complete mediation
C. separation of privilege
D. least common mechanism

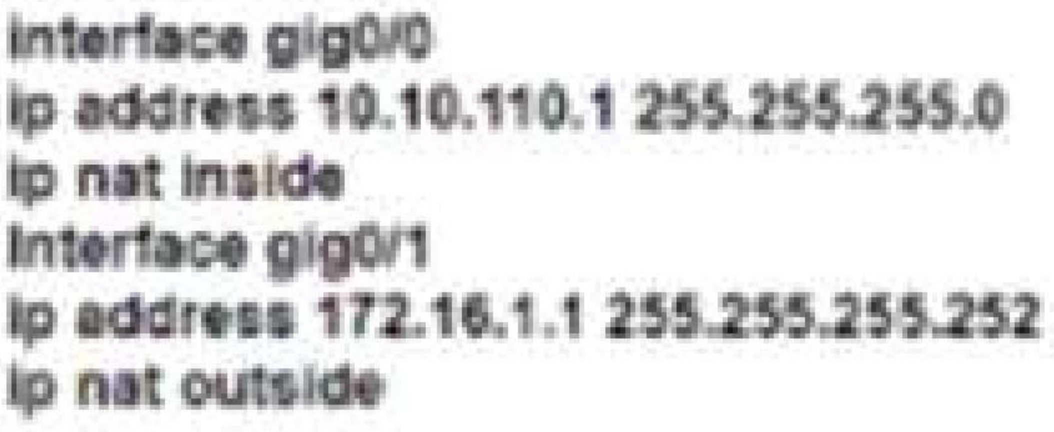
Correct Answer: B
Section:
Explanation:
A system should validate access rights to all its resources to ensure that they are allowed and should not rely on the cached permission matrix. If the access level to a given resource is being revoked, but that is not being reflected in the permission matrix,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

QUESTION 351
Reter to the exhibit.



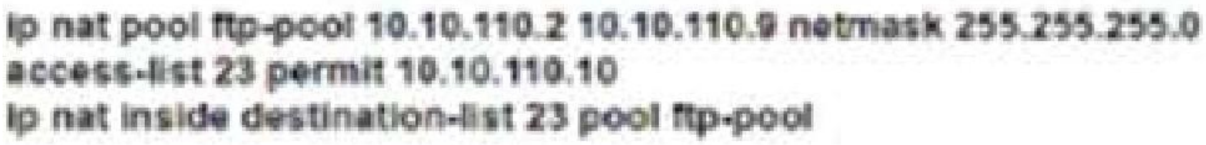
Refer to the exhibit. A network engineer must load balance traffic that comes from the NAT Router and is destined to 10.10.110.10, to several FTP servers. Which two commands sets should be applied? (Choose two).

A.



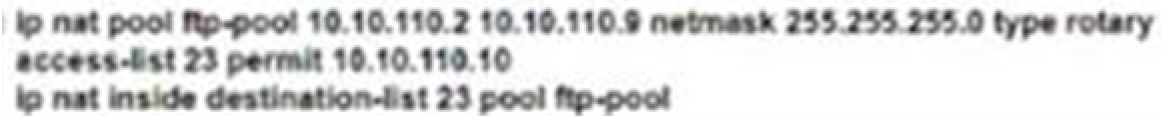
```
interface gig0/0
ip address 10.10.110.1 255.255.255.0
ip nat inside
interface gig0/1
ip address 172.16.1.1 255.255.255.252
ip nat outside
```

B.



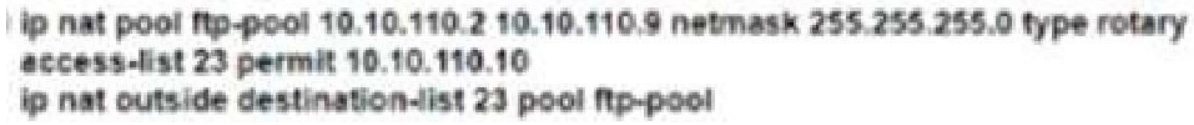
```
ip nat pool ftp-pool 10.10.110.2 10.10.110.9 netmask 255.255.255.0
access-list 23 permit 10.10.110.10
ip nat inside destination-list 23 pool ftp-pool
```

C.



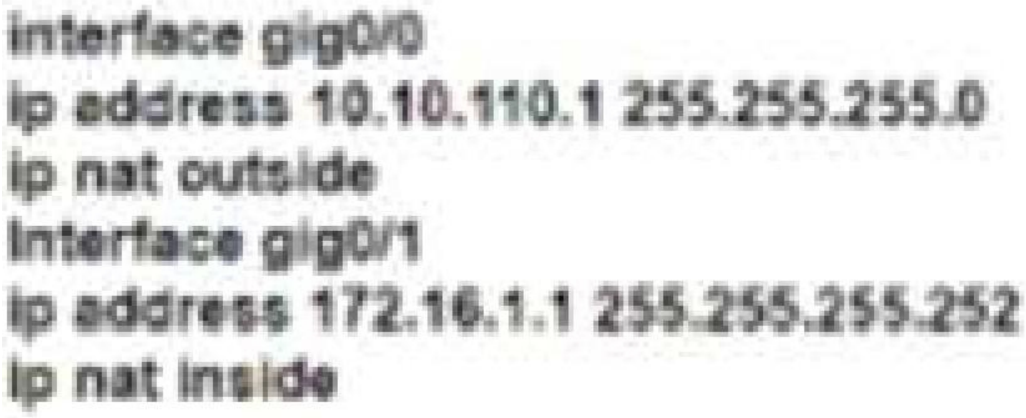
```
ip nat pool ftp-pool 10.10.110.2 10.10.110.9 netmask 255.255.255.0 type rotary
access-list 23 permit 10.10.110.10
ip nat inside destination-list 23 pool ftp-pool
```

D.



```
ip nat pool ftp-pool 10.10.110.2 10.10.110.9 netmask 255.255.255.0 type rotary
access-list 23 permit 10.10.110.10
ip nat outside destination-list 23 pool ftp-pool
```

E.

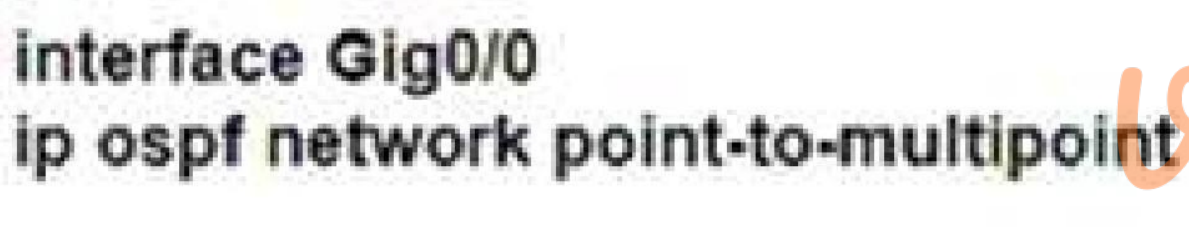


```
interface gig0/0
ip address 10.10.110.1 255.255.255.0
ip nat outside
Interface gig0/1
ip address 172.16.1.1 255.255.255.252
ip nat inside
```

Correct Answer: A, C
Section:

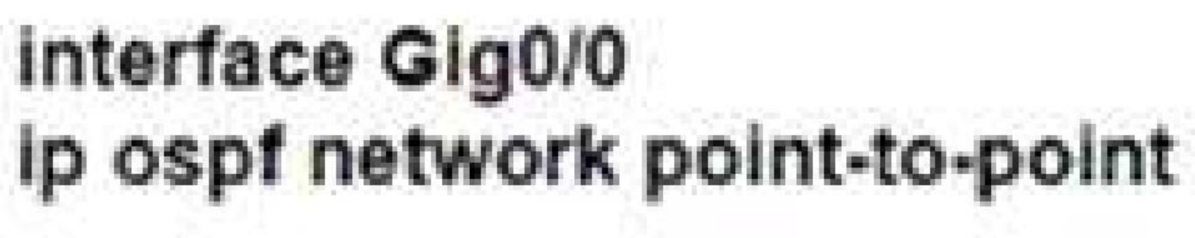
QUESTION 352
The Gig0/0 interface of two routers is directly connected with a 1G Ethernet link. Which configuration must be applied to the interface of both routers to establish an OSPF adjacency without maintaining a DR/BDR relationship?

A.



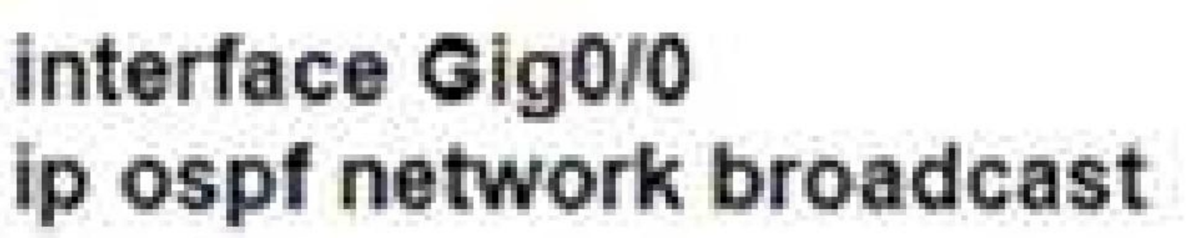
```
interface Gig0/0
ip ospf network point-to-multipoint
```

B.



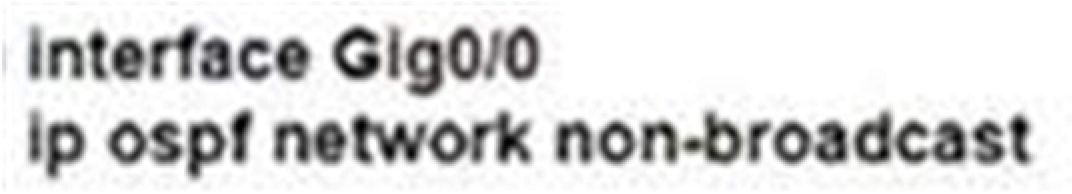
```
interface Gig0/0
ip ospf network point-to-point
```

C.



```
interface Gig0/0
ip ospf network broadcast
```

D.



```
interface Gig0/0
ip ospf network non-broadcast
```

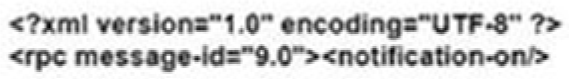
Correct Answer: B
Section:

QUESTION 353
What is a characteristic of the overlay network in the Cisco SD-Access architecture?

A. It uses a traditional routed access design to provide performance and high availability to the network.
B. It consists of a group of physical routers and switches that are used to maintain the network.
C. It provides isolation among the virtual networks and independence from the physical network.
D. It provides multicast support to enable Layer 2 Hooding capability in the underlay network.

Correct Answer: C
Section:

QUESTION 354
An administrator is configuring NETCONF using the following XML string. What must the administrator end the request with?



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

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

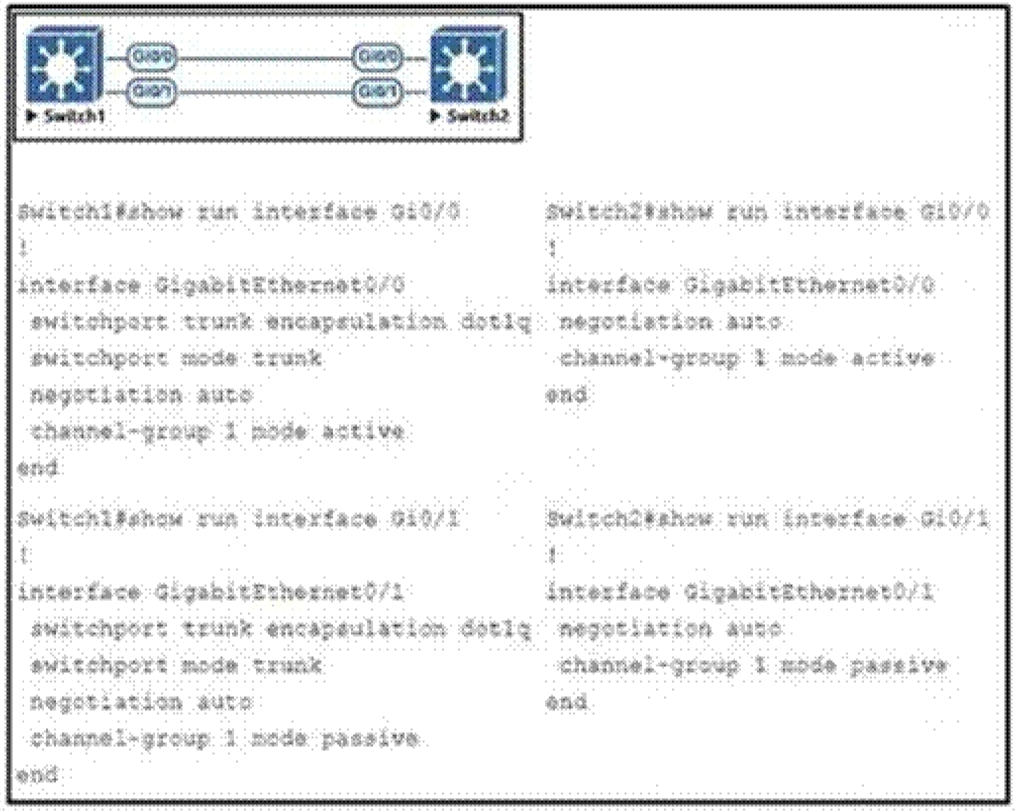
Correct Answer: A
Section:

QUESTION 355
Which VXLAN component is used to encapsulate and decapsulate Ethernet frames?

A. VNI
B. GRE
C. VTEP
D. EVPN

Correct Answer: C
Section:

QUESTION 356
Refer to the exhibit.



```
Switch1#show run interface Gi0/0            Switch2#show run interface Gi0/0
!                                           !
interface GigabitEthernet0/0                interface GigabitEthernet0/0
 switchport trunk encapsulation dot1q        negotiation auto
 switchport mode trunk                       channel-group 1 mode active
 negotiation auto                           end
 channel-group 1 mode active
end
Switch1#show run interface Gi0/1            Switch2#show run interface Gi0/1
!                                           !
interface GigabitEthernet0/1                interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q        negotiation auto
 switchport mode trunk                       channel-group 1 mode passive
 negotiation auto                           end
 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.

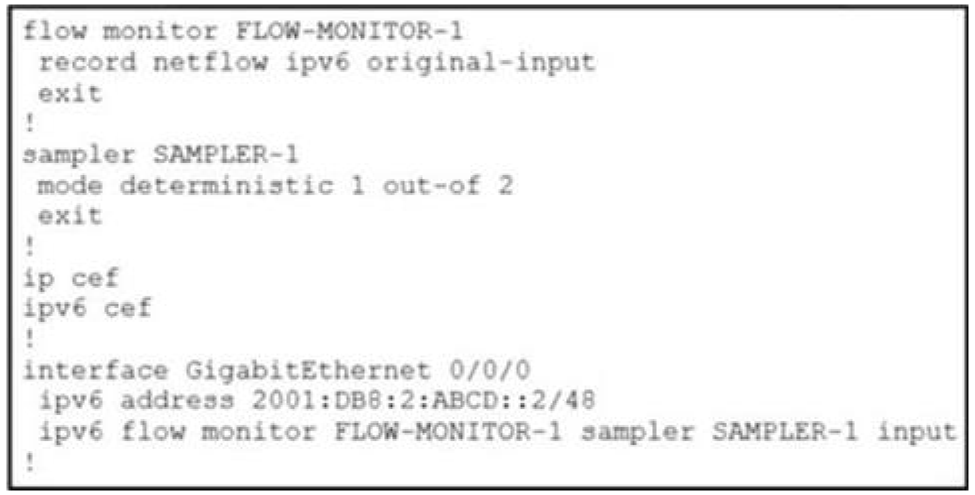
Correct Answer: C
Section:

QUESTION 357
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

Correct Answer: B
Section:

QUESTION 358
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.

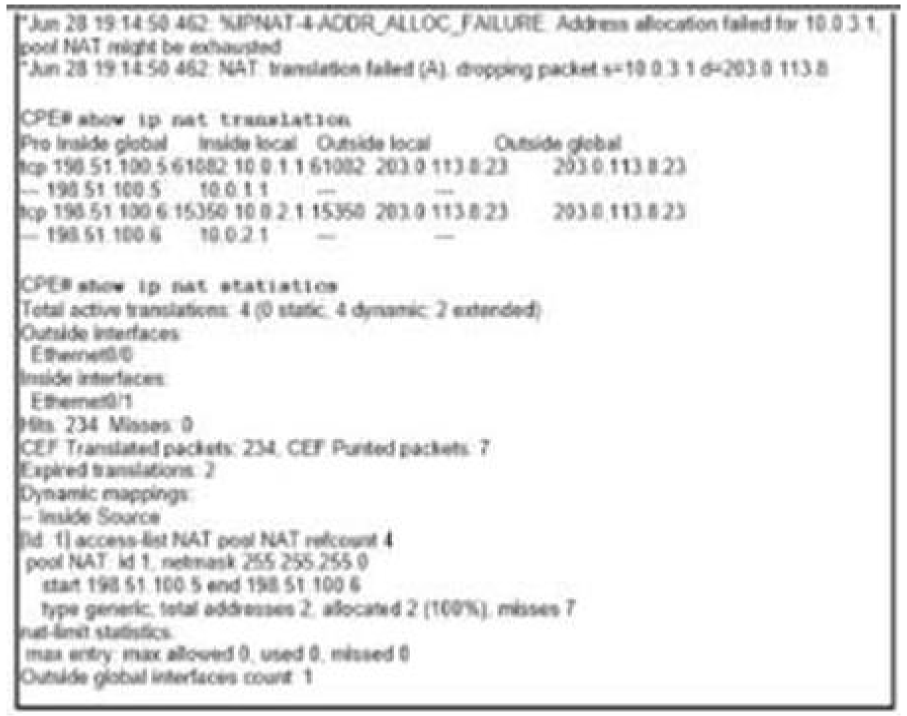
C. CPU and memory utilization are reduced when compared with what is required for full NetFlow.

D. The resolution of sampling data increases, but it requires more performance from the router.

Correct Answer: C
Section:

QUESTION 359

Reter to the exhibit.



```
*Jun 28 19:14:50.462: %IPNAT-4-ADDR_ALLOC_FAILURE: Address allocation failed for 10.0.3.1,
pool NAT might be exhausted
*Jun 28 19:14:50.462: NAT: translation failed (A), dropping packet s=10.0.3.1 d=203.0.113.8

CPE# show ip nat translation
Pro Inside global      Inside local     Outside local         Outside global
tcp 198.51.100.5:61082 10.0.1.1:61082  203.0.113.8:23        203.0.113.8:23
--- 198.51.100.5       10.0.1.1        ---                   ---
tcp 198.51.100.6:15350 10.0.2.1:15350  203.0.113.8:23        203.0.113.8:23
--- 198.51.100.6       10.0.2.1        ---                   ---

CPE# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Ethernet0/1
Hits: 234  Misses: 0
CEF Translated packets: 234, CEF Punted packets: 7
Expired translations: 2
Dynamic mappings:
-- Inside Source
[Id: 1] access-list NAT pool NAT refcount 4
 pool NAT: id 1, netmask 255.255.255.0
    start 198.51.100.5 end 198.51.100.6
    type generic, total addresses 2, allocated 2 (100%), misses 7
nat-limit statistics:
 max entry: max allowed 0, used 0, missed 0
Outside global interfaces count: 1
```

An administrator troubleshoots intermittent connectivity from internal hosts to an external public server. Some internal hosts can connect to the server while others receive an ICMP Host Unreachable message and these hosts change over time. What is the cause of this issue?

A. The translator does not use aOdress overloading

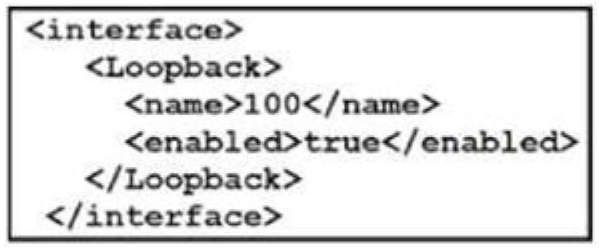
B. The NAT ACL does not match alt internal hosts

C. The NAT ACL and NAT pool share the same name

D. The NAT pool netmask rs excessively wide

Correct Answer: B
Section:

QUESTION 360
Reter to the exhibit.



```
<interface>
   <Loopback>
     <name>100</name>
     <enabled>true</enabled>
   </Loopback>
 </interface>
```

Refer to the exhibit. What is achieved by this code?

A. It unshuts the loopback interface
B. It renames the loopback interface
C. It deletes the loopback interface
D. It displays the loopback interface

Correct Answer: D
Section:

QUESTION 361
An engineer must configure an EXEC authorization list that first checks a AAA server then a local username. If both methods fail, the user is denied. Which configuration should be applied?

A. aaa authorization exec default local group tacacs+
B. aaa authorization exec default local group radius none
C. aaa authorization exec default group radius local none
D. aaa authorization exec default group radius local

Correct Answer: D
Section:

QUESTION 362
What is a characteristics of a vSwitch?

A. supports advanced Layer 3 routing protocols that are not offered by a hardware switch
B. enables VMs to communicate with each other within a virtualized server
C. has higher performance than a hardware switch
D. operates as a hub and broadcasts the traffic toward all the vPorts

Correct Answer: B
Section:

QUESTION 363
What is a characteristic of a Type I hypervisor?

A. It is installed on an operating system and supports other operating systems above it.
B. It is referred to as a hosted hypervisor.
C. Problems in the base operating system can affect the entire system.
D. It is completely independent of the operating system.

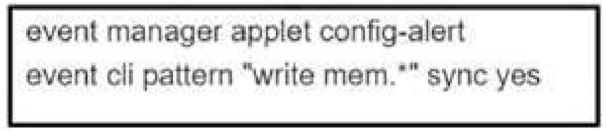
Correct Answer: D
Section:

QUESTION 364
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

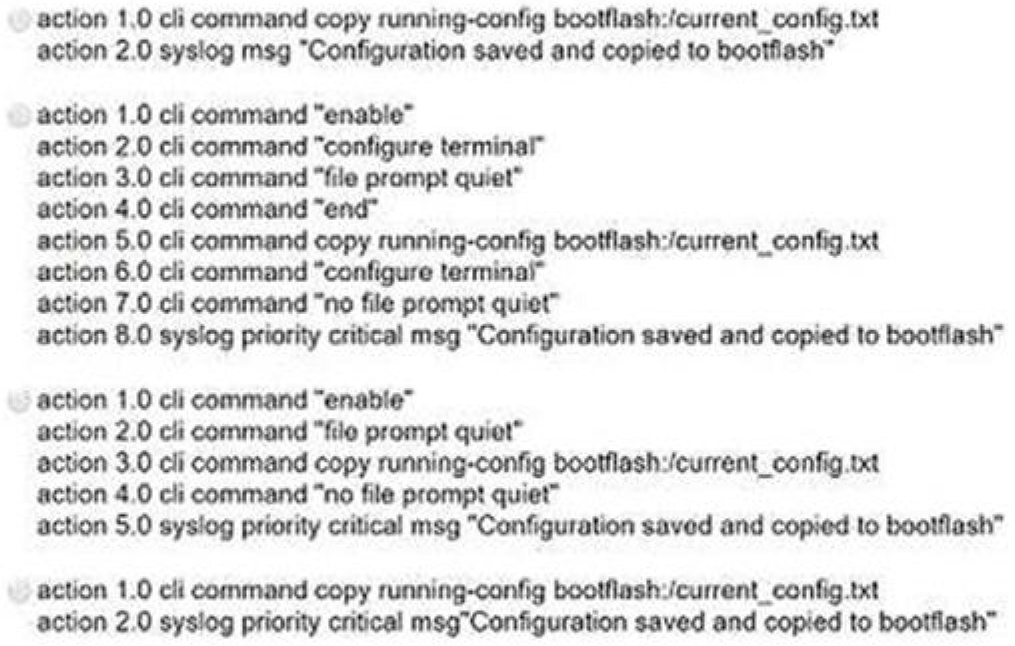
Correct Answer: B, D
Section:

QUESTION 365
Reter to the exhibit.



```
event manager applet config-alert
event cli pattern "write mem.*" sync yes
```

Refer to the exhibit. Which EEM script generates a critical-level syslog message and saves a copy of the running configuration to the bootflash when an administrator saves the running configuration to the startup configuration?



```
○ action 1.0 cli command copy running-config bootflash:/current_config.txt
  action 2.0 syslog msg "Configuration saved and copied to bootflash"

○ action 1.0 cli command "enable"
  action 2.0 cli command "configure terminal"
  action 3.0 cli command "file prompt quiet"
  action 4.0 cli command "end"
  action 5.0 cli command copy running-config bootflash:/current_config.txt
  action 6.0 cli command "configure terminal"
  action 7.0 cli command "no file prompt quiet"
  action 8.0 syslog priority critical msg "Configuration saved and copied to bootflash"

○ action 1.0 cli command "enable"
  action 2.0 cli command "file prompt quiet"
  action 3.0 cli command copy running-config bootflash:/current_config.txt
  action 4.0 cli command "no file prompt quiet"
  action 5.0 syslog priority critical msg "Configuration saved and copied to bootflash"

○ action 1.0 cli command copy running-config bootflash:/current_config.txt
  action 2.0 syslog priority critical msg"Configuration saved and copied to bootflash"
```

A. Option A
B. Option B

C. Option C
D. Option D

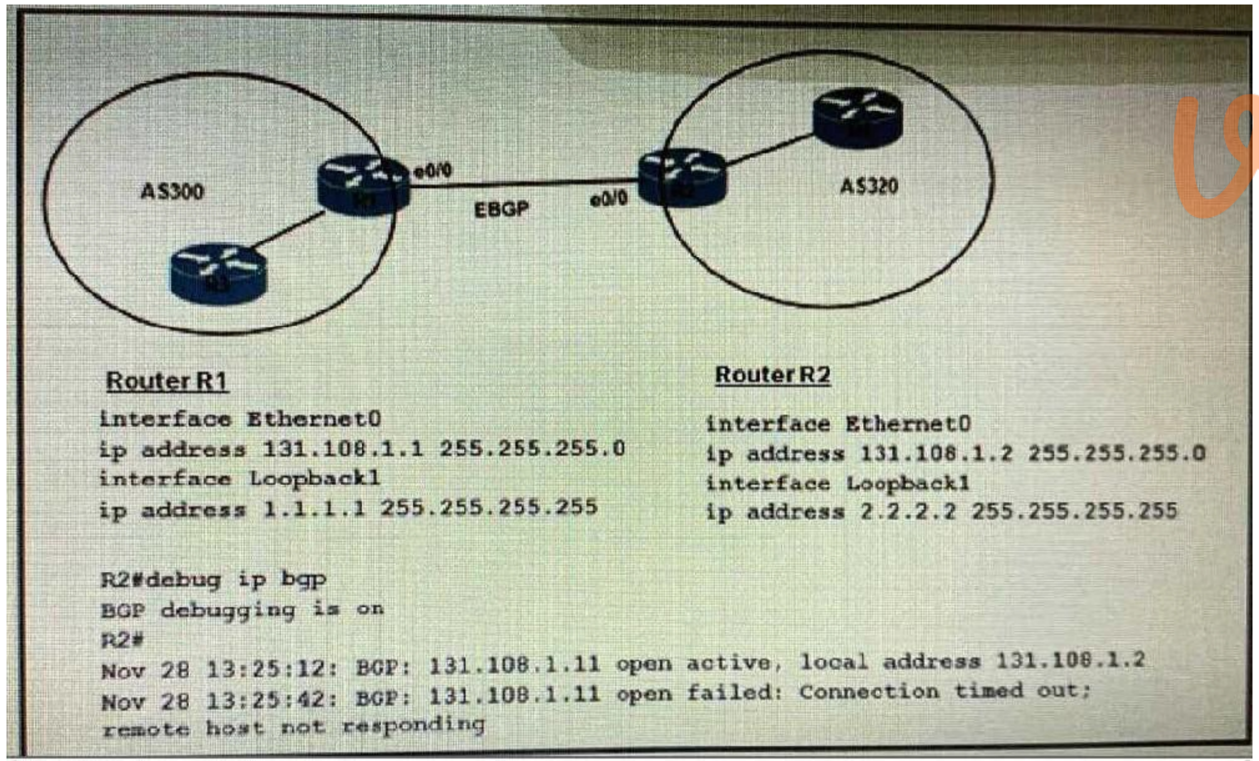
Correct Answer: B
Section:

QUESTION 366
Which two Cisco SD-WAN components exchange OMP information?

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

Correct Answer: B, C
Section:

QUESTION 367
Refer to the exhibit.



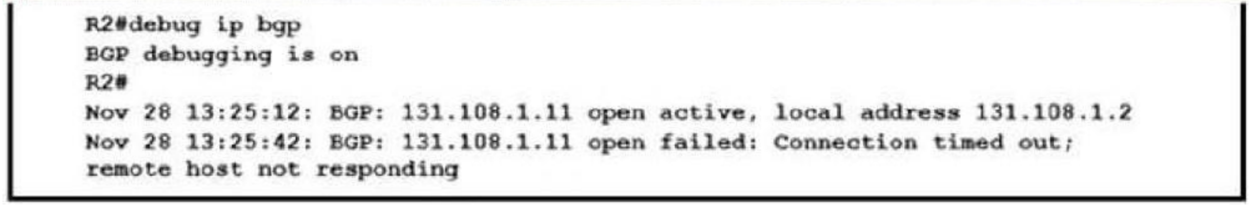
Router R1

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

Router R2

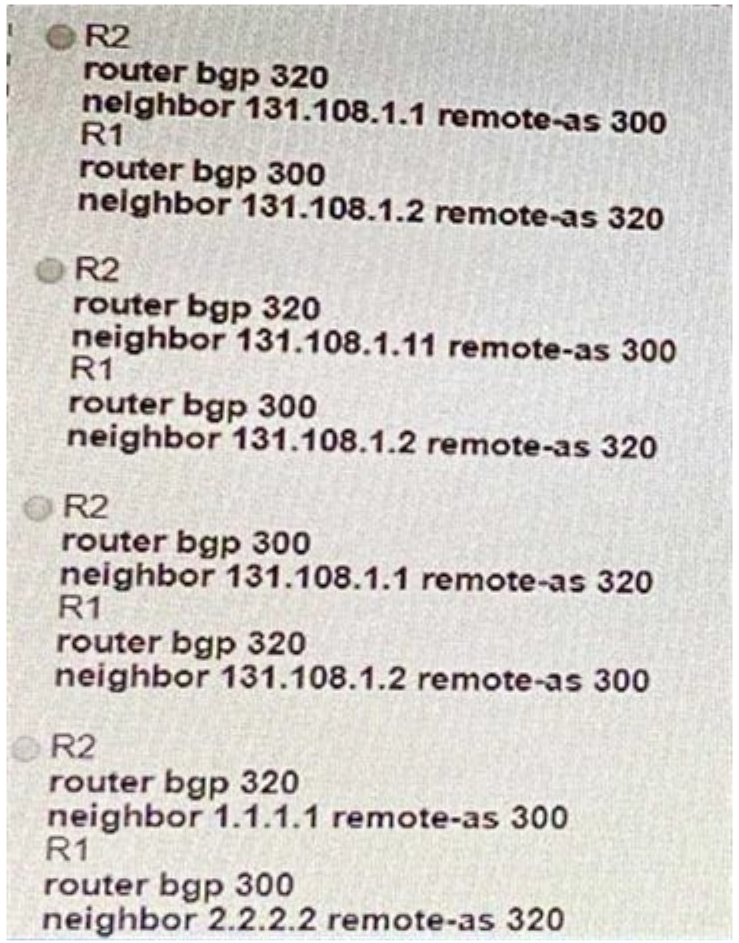
```
interface Ethernet0
ip address 131.108.1.2 255.255.255.0
interface Loopback1
ip address 2.2.2.2 255.255.255.255
```

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



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

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



○ 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
```

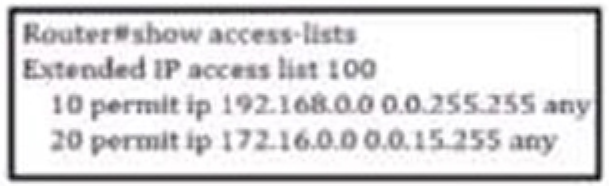
○ R2
```
router bgp 300
neighbor 131.108.1.1 remote-as 320
R1
router bgp 320
neighbor 131.108.1.2 remote-as 300
```

○ 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

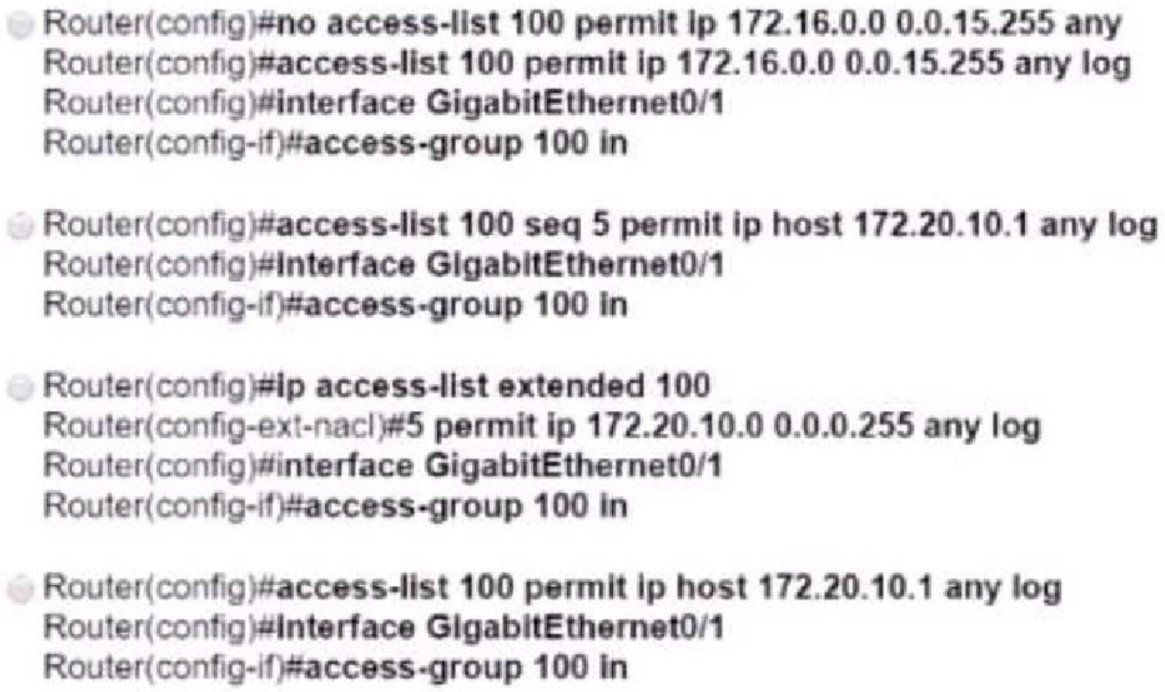
Correct Answer: A
Section:

QUESTION 368
Refer to the exhibit.



```
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
```

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

Correct Answer: B
Section:

QUESTION 369
Which option must be used to support a WLC with an IPv6 management address and 100 Cisco Aironet 2800 Series access points that will use DHCP to register?

A. 43
B. 52
C. 60
D. 82

Correct Answer: B
Section:

QUESTION 370
An engineer is configuring Local WebAuth on a Cisco Wireless LAN Controller. According to RFC 5737, WHICH VIRTUAL IP address must be used in this configuration?

A. 192.0.2.1
B. 172.20.10.1
C. 1.1.1.1
D. 192.168.0.1

Correct Answer: A

Section:

QUESTION 371
By default, which virtual MAC address does HSRP group 32 use?

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

Correct Answer: D
Section:

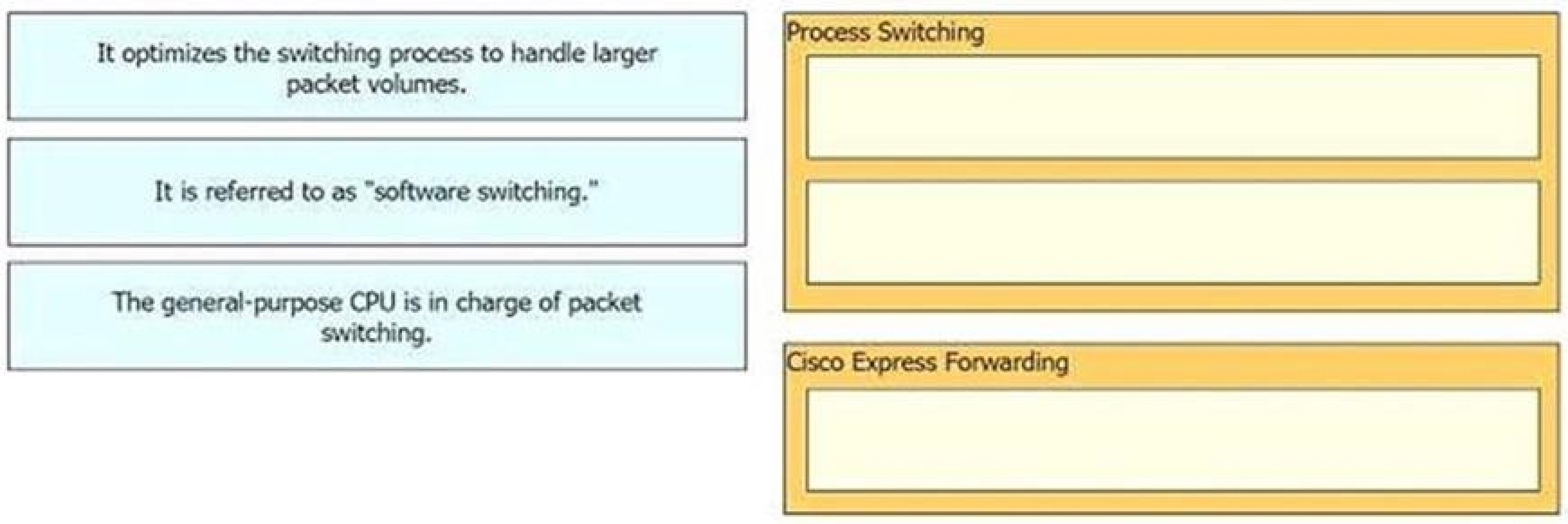
QUESTION 372
What does the number in an NTP stratum level represent?

A. The number of hops it takes to reach the master time server.
B. The number of hops it takes to reach the authoritative time source.
C. The amount of offset between the device clock and true time.
D. The amount of drift between the device clock and true time.

Correct Answer: B
Section:

QUESTION 373
DRAG DROP
Drag and drop the characteristics from the left onto the switching architectures on the right.

Select and Place:

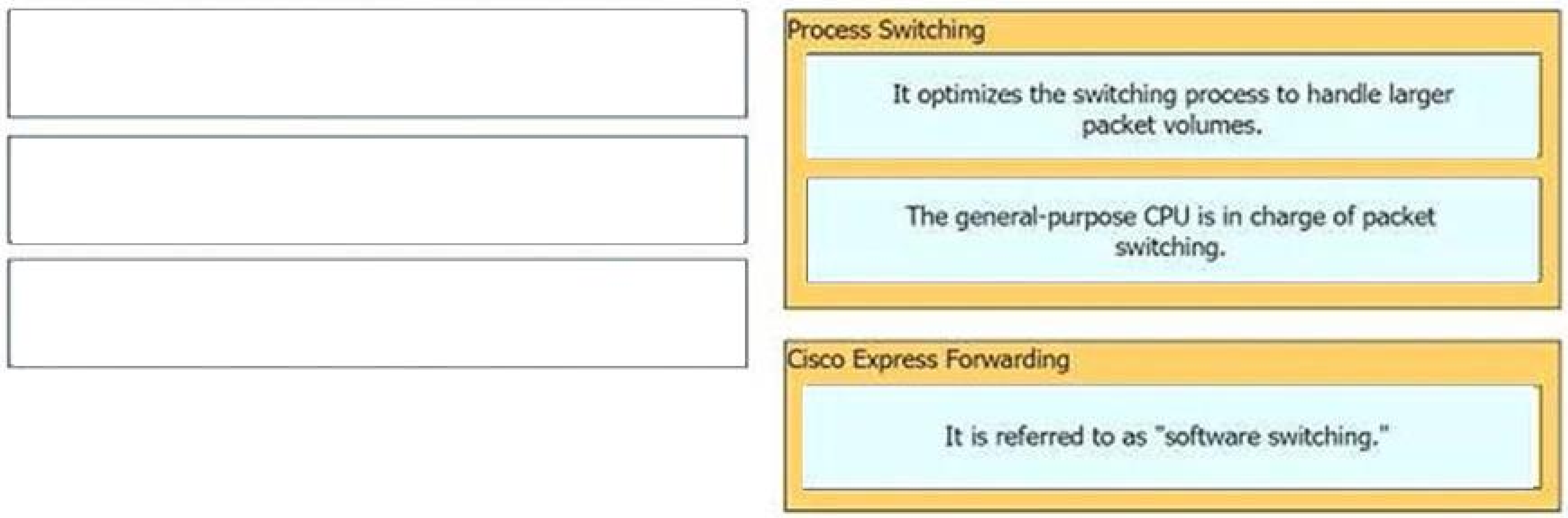


It optimizes the switching process to handle larger packet volumes.

It is referred to as "software switching."

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

Correct Answer:



Process Switching

It optimizes the switching process to handle larger packet volumes.

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

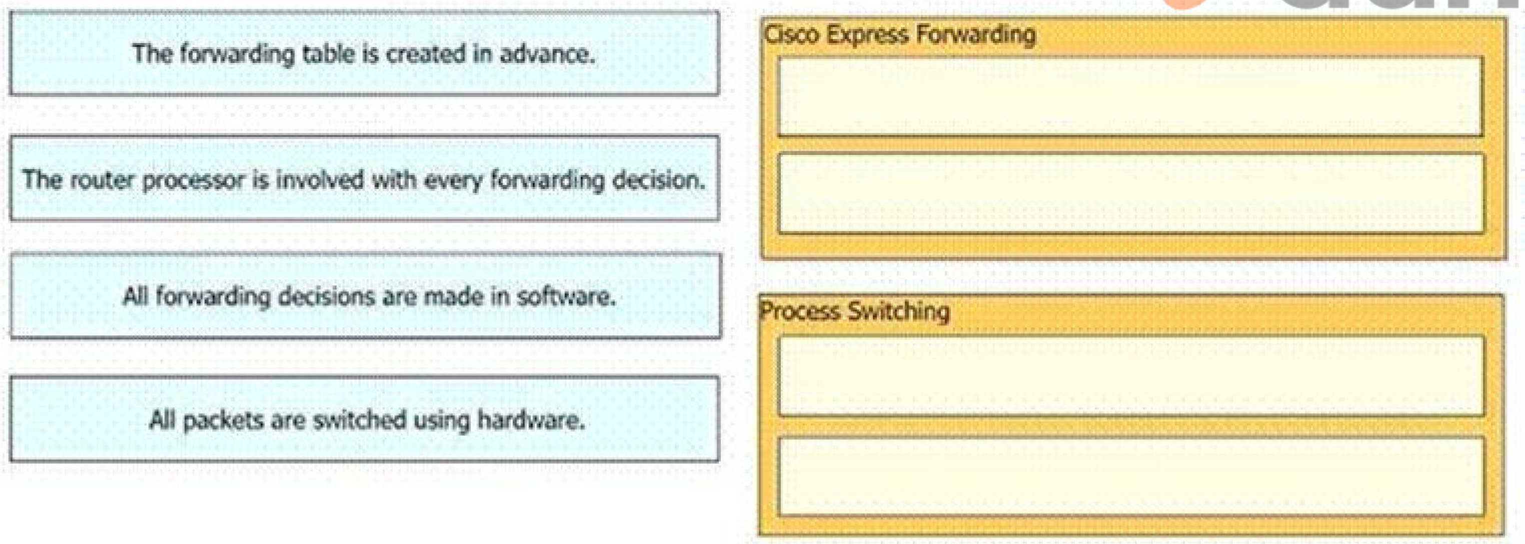
Cisco Express Forwarding

It is referred to as "software switching."

Section:
Explanation:

QUESTION 374
DRAG DROP
Drag and drop the characteristics from the left onto the switching mechanisms they describe on the right.

Select and Place:



The forwarding table is created in advance.

The router processor is involved with every forwarding decision.

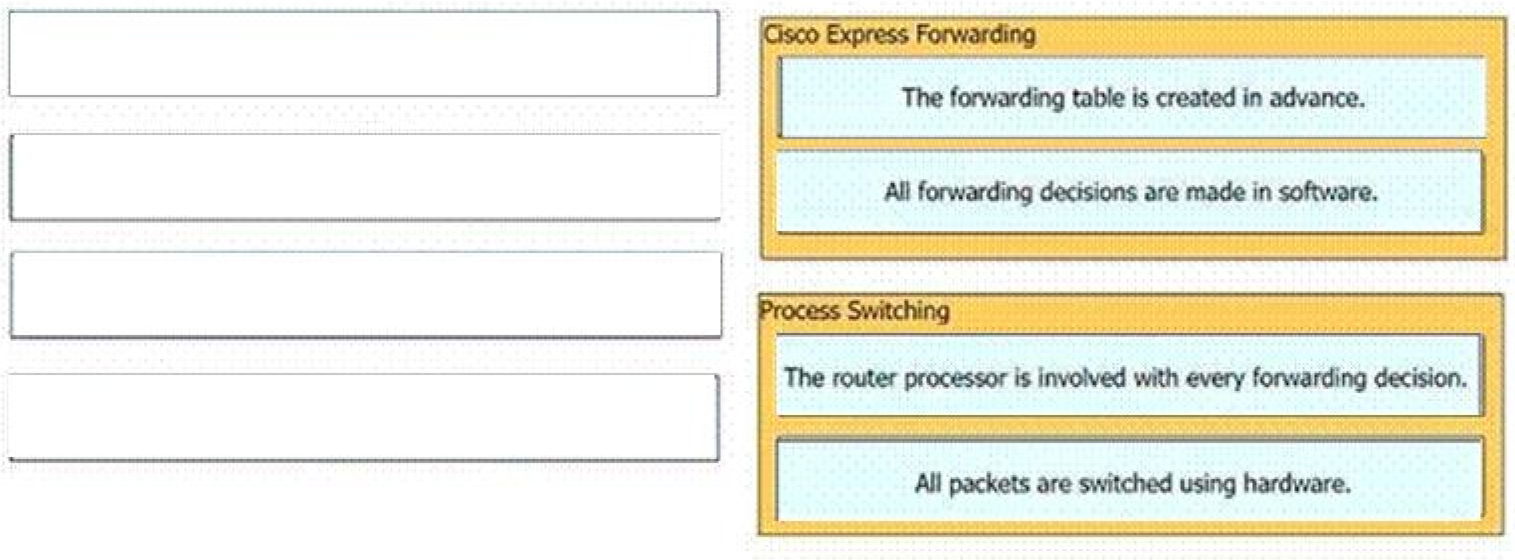
All forwarding decisions are made in software.

All packets are switched using hardware.

Cisco Express Forwarding

Process Switching

Correct Answer:



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.

Section:
Explanation:

QUESTION 375

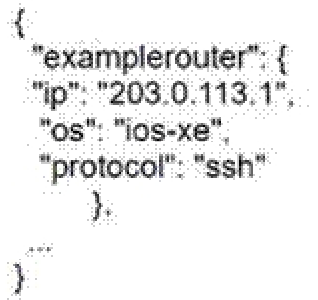
DRAG DROP

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

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

After being interrupted, the script displays the entered entries and adds them to the JSON-formatted file, replacing existing entries whose hostname matches.

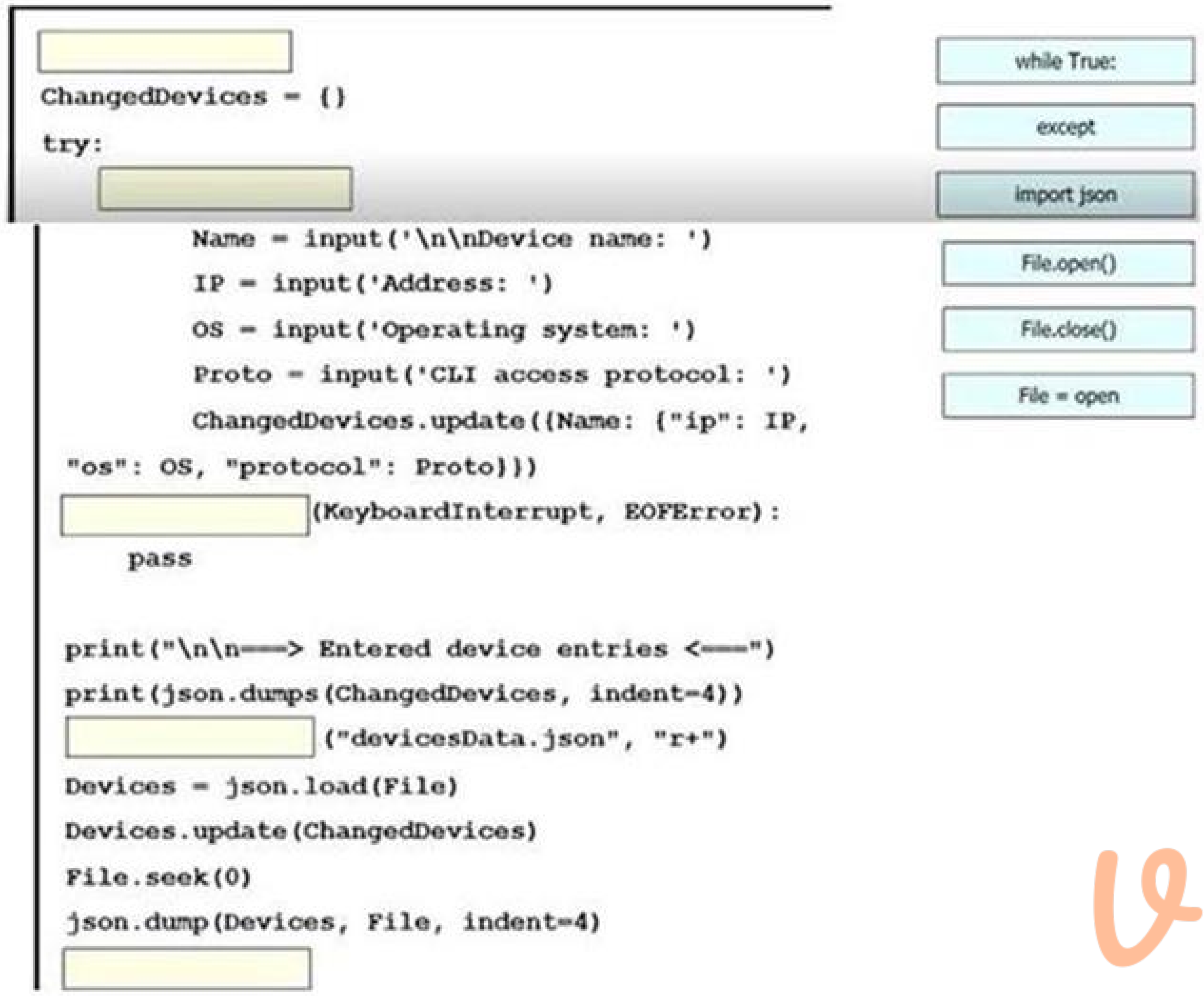
The contents of the JSON-formatted file are as follows:



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

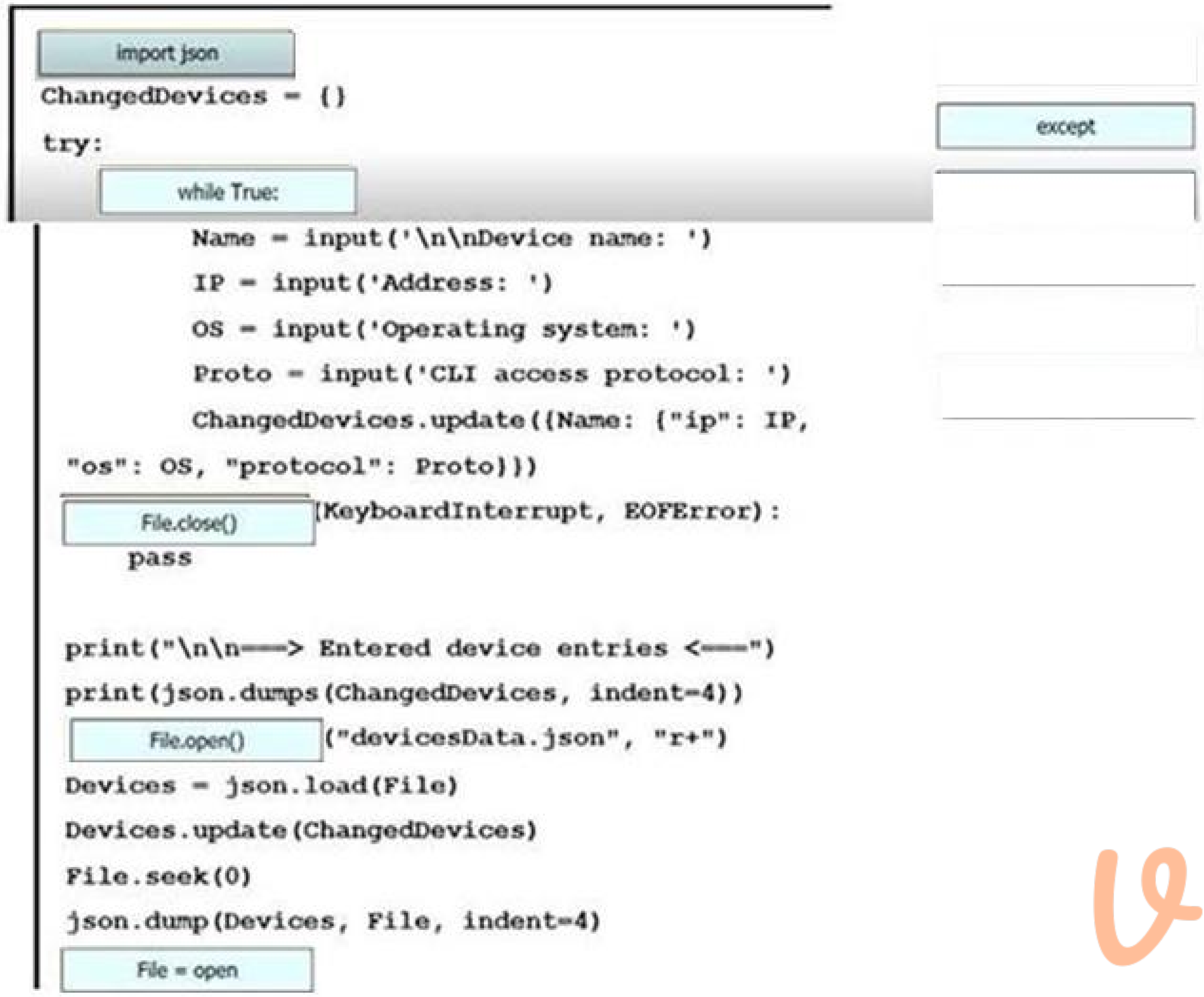
Drag and drop the statements onto the blanks within the code to complete the script. Not all options are used.

Select and Place:



```

ChangedDevices = {}
try:

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

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

```

Correct Answer:

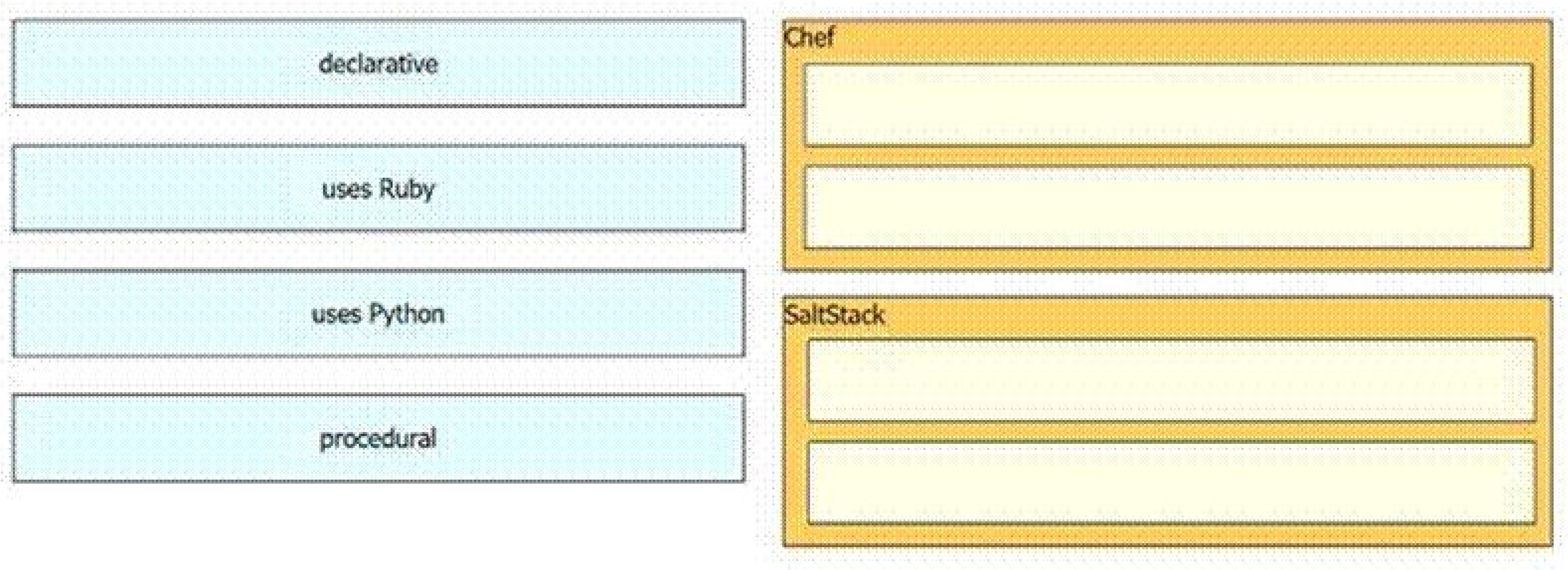


```
import json
ChangedDevices = {}
try:
    while True:
        Name = input('\n\nDevice name: ')
        IP = input('Address: ')
        OS = input('Operating system: ')
        Proto = input('CLI access protocol: ')
        ChangedDevices.update({Name: {"ip": IP,
"os": OS, "protocol": Proto}})
File.close()(KeyboardInterrupt,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

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

Section:
Explanation:

QUESTION 376
DRAG DROP
Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right

Select and Place:



declarative

uses Ruby

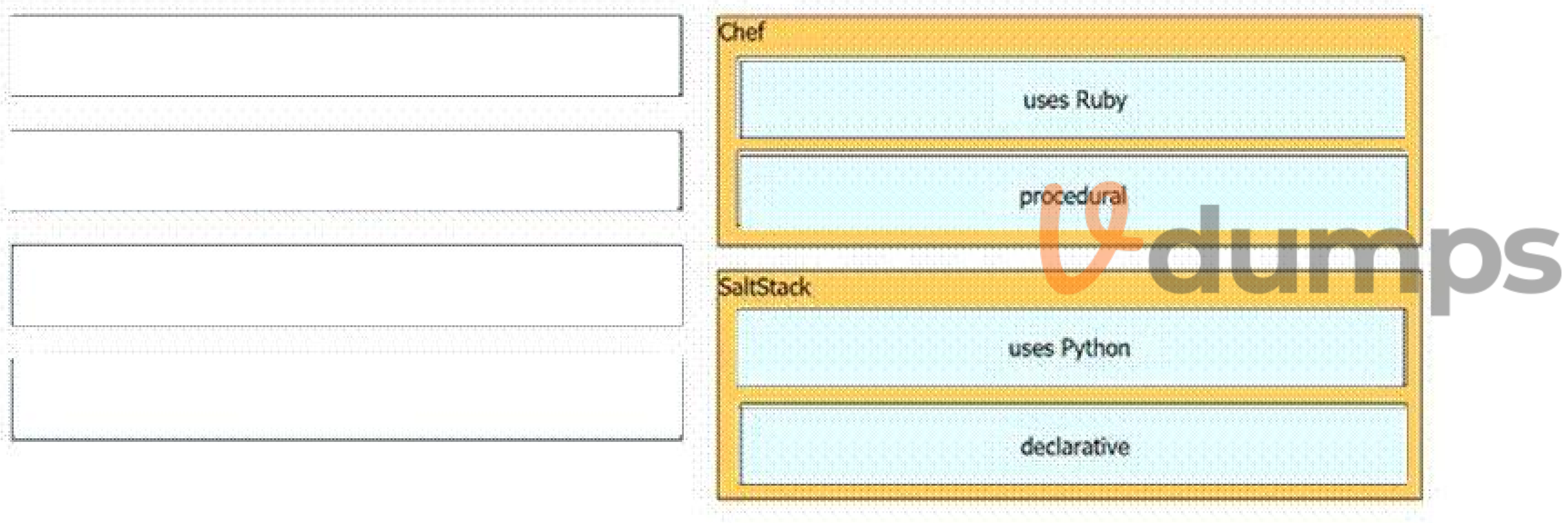
uses Python

procedural

Chef

SaltStack

Correct Answer:



Chef

uses Ruby

procedural

SaltStack

uses Python

declarative

Section:
Explanation:

QUESTION 377
A customer deploys a new wireless network to perform location-based services using Cisco DNA Spaces The customer has a single WLC located on-premises in a secure data center. The security team does not want to expose the WLC to the public Internet. Which solution allows the customer to securely send RSSI updates to Cisco DNA Spaces?

A. Implement Cisco Mobility Services Engine
B. Replace the WLC with a cloud-based controller.
C. Perform tethering with Cisco DNA Center.
D. Deploy a Cisco DNA Spaces connector as a VM.

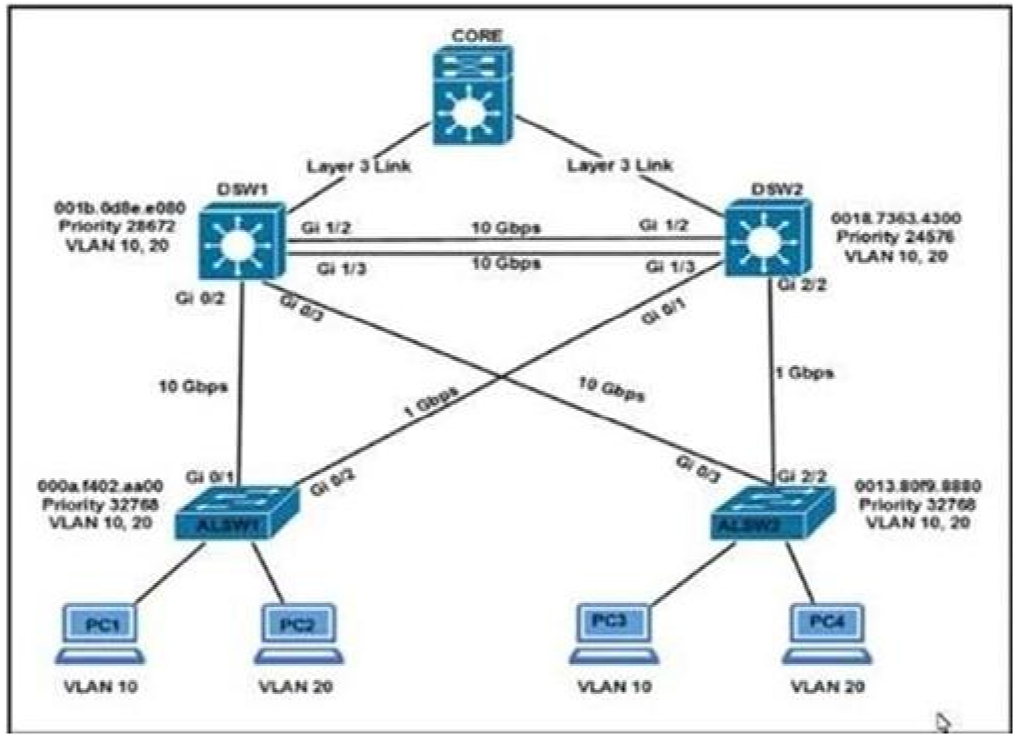
Correct Answer: D
Section:

QUESTION 378
What does a YANG model provide?

A. standardized data structure independent of the transport protocols
B. creation of transport protocols and their interaction with the OS
C. user access to interact directly with the CLI of the device to receive or modify network configurations
D. standardized data structure that can be used only with NETCONF or RESTCONF transport protocols

Correct Answer: D
Section:

QUESTION 379
Refer to the exhibit.

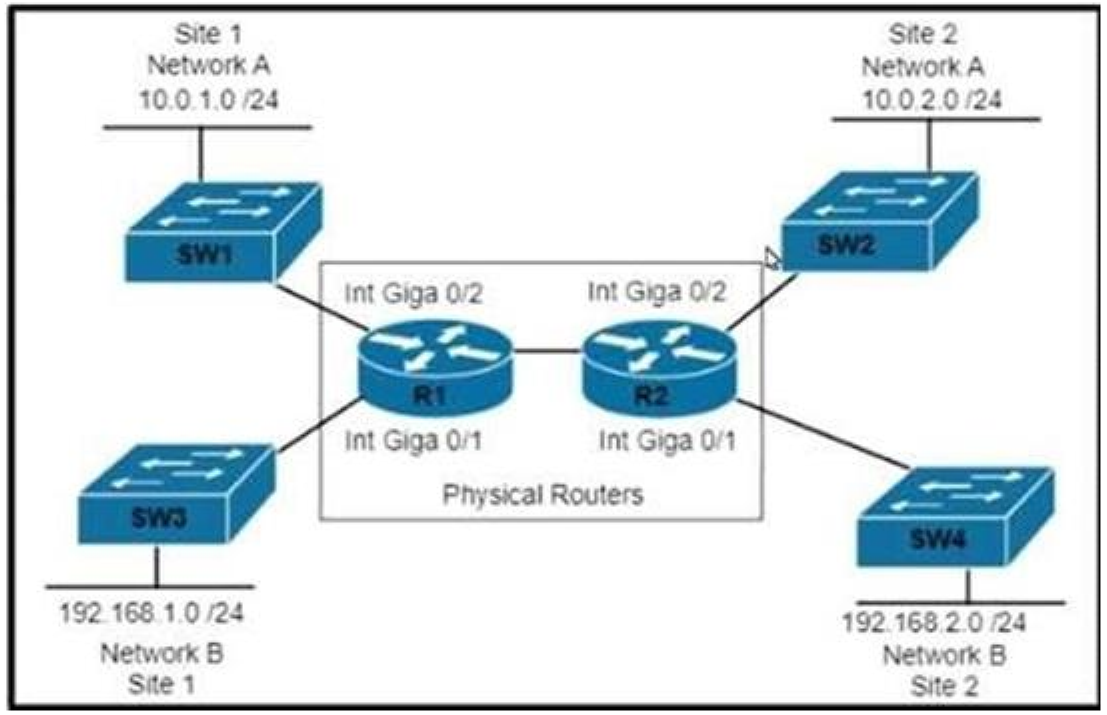


Assuming all links are functional, which path does PC1 take to reach DSW1?

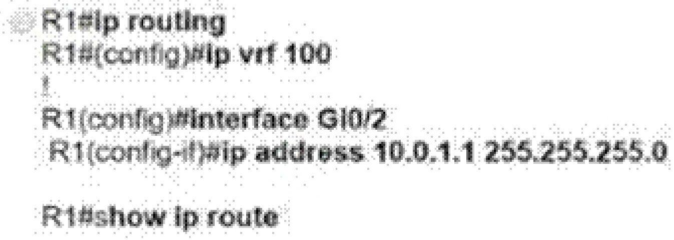
A. PC1 goes from ALSW1 to DSW2 to CORE to DSW1.
B. PC1 goes from ALSW1 to DSW2 to DSW1.
C. PC1 goes from ALSW1 to DSW1.
D. PC1 goes from ALSW1 to DSW2 to ALSW2 to DSW1.

Correct Answer: B
Section:
Explanation:

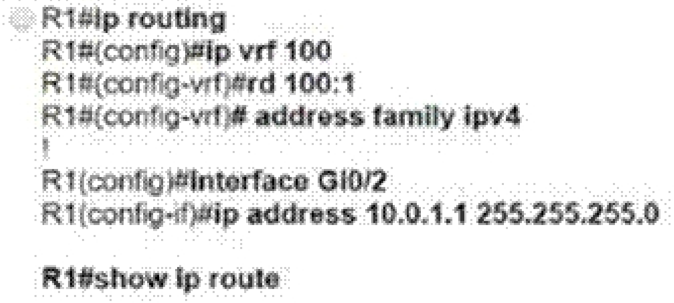
QUESTION 380
Refer to the exhibit.



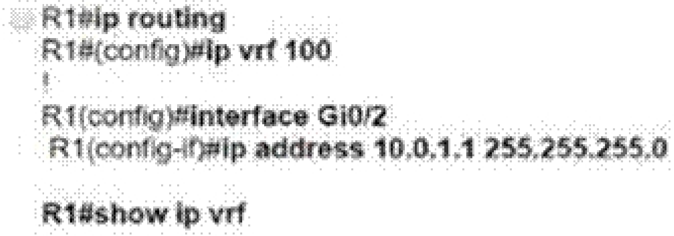
Refer to the exhibit. Which set of commands is required to configure and verify the VRF for Site 1 Network A on router R1?



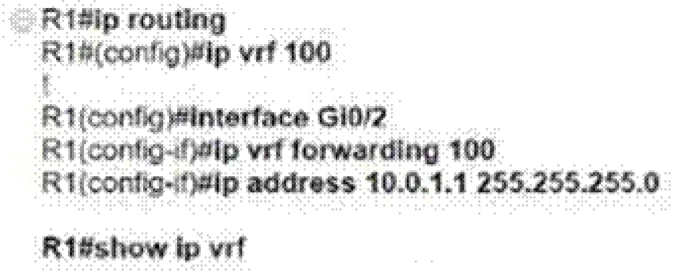
```
R1#ip routing
R1#(config)#ip vrf 100
!
R1(config)#interface Gi0/2
 R1(config-if)#ip address 10.0.1.1 255.255.255.0

R1#show ip route
```



```
R1#ip routing
R1#(config)#ip vrf 100
R1#(config-vrf)#rd 100:1
R1#(config-vrf)# address family ipv4
!
R1(config)#interface Gi0/2
R1(config-if)#ip address 10.0.1.1 255.255.255.0

R1#show ip route
```



```
R1#ip routing
R1#(config)#ip vrf 100
!
R1(config)#interface Gi0/2
 R1(config-if)#ip address 10.0.1.1 255.255.255.0

R1#show ip vrf
```



```
R1#ip routing
R1#(config)#ip vrf 100
!
R1(config)#interface Gi0/2
R1(config-if)#ip vrf forwarding 100
R1(config-if)#ip address 10.0.1.1 255.255.255.0

R1#show ip vrf
```

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

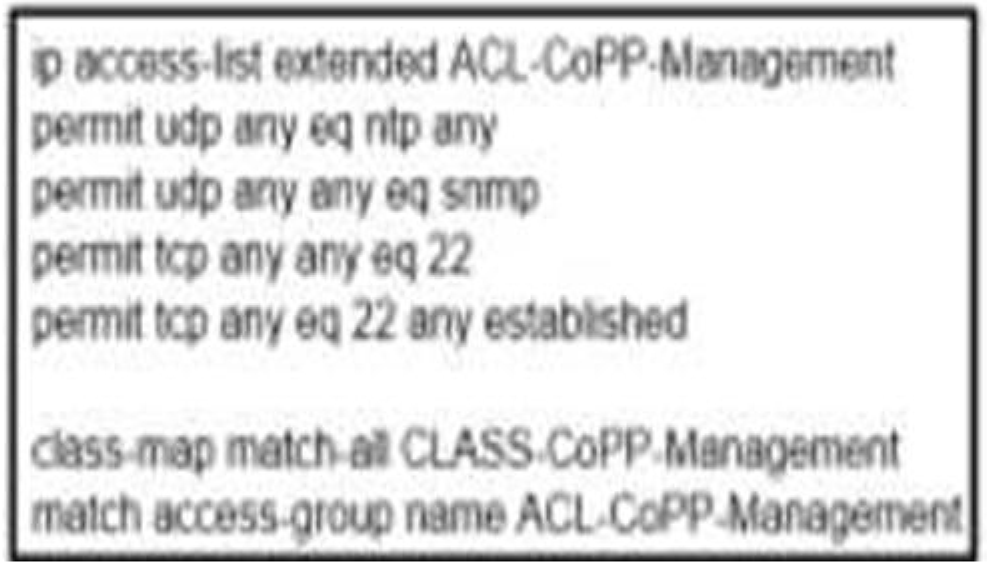
Correct Answer: D
Section:

QUESTION 381
By default, which virtual MAC address does HSRP group 22 use?

A. c0:42:01:67:05:16
B. c0:07:0c:ac:00:22
C. 00:00:0c:07:ac:16
D. 00:00:0c:07:ac:22

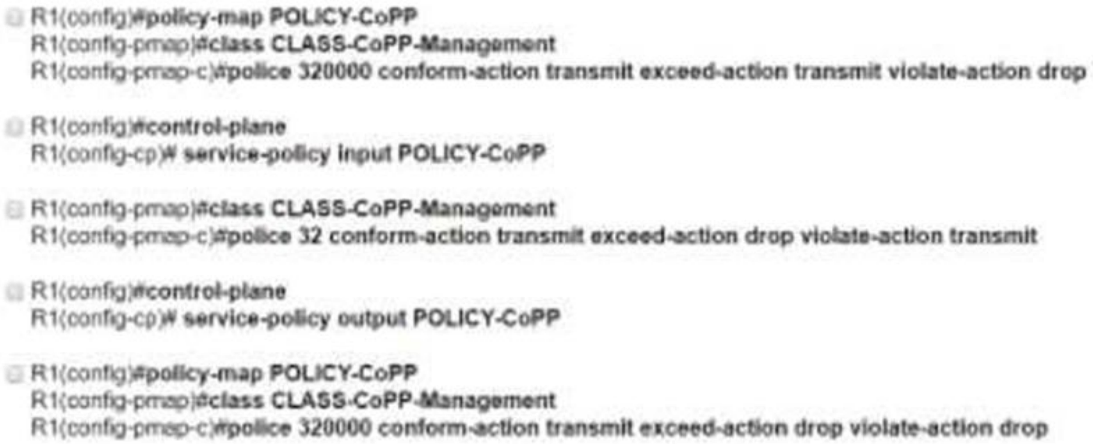
Correct Answer: D
Section:

QUESTION 382
Refer to the exhibit.



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

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

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

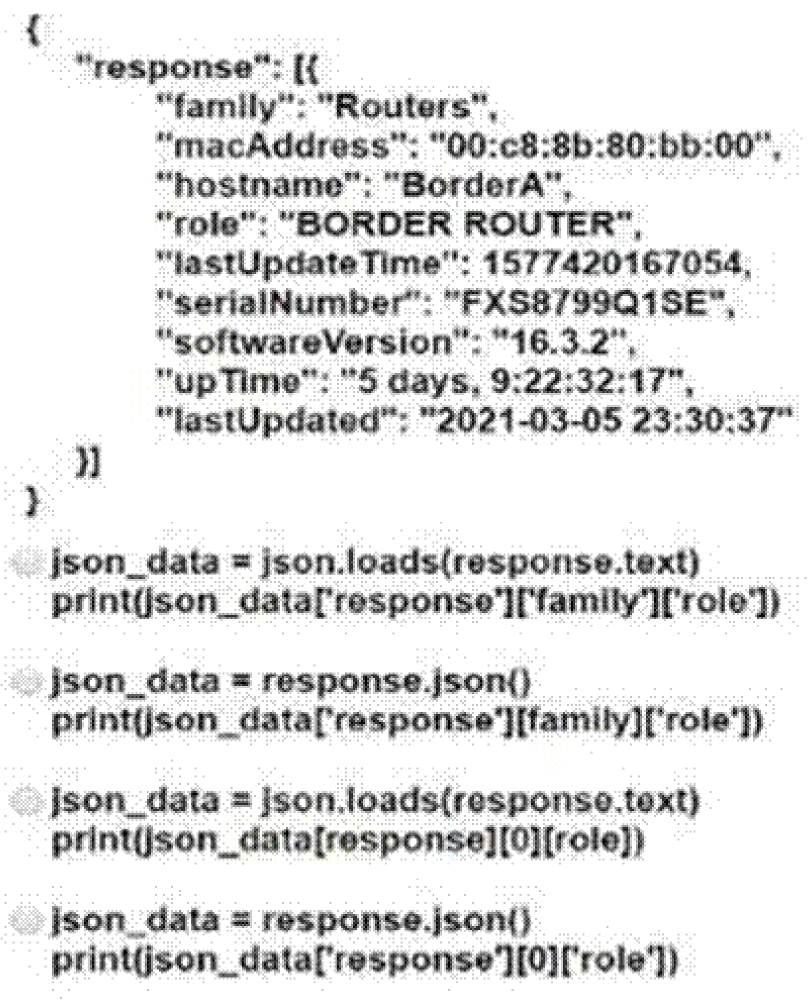


```
□ R1(config)#policy-map POLICY-CoPP
  R1(config-pmap)#class CLASS-CoPP-Management
  R1(config-pmap-c)#police 320000 conform-action transmit exceed-action transmit violate-action drop

□ R1(config)#control-plane
  R1(config-cp)# service-policy input POLICY-CoPP

□ R1(config-pmap)#class CLASS-CoPP-Management
  R1(config-pmap-c)#police 32 conform-action transmit exceed-action drop violate-action transmit

□ R1(config)#control-plane
  R1(config-cp)# service-policy output POLICY-CoPP

□ R1(config)#policy-map POLICY-CoPP
  R1(config-pmap)#class CLASS-CoPP-Management
  R1(config-pmap-c)#police 320000 conform-action transmit exceed-action drop violate-action drop
```

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

Correct Answer: B, E
Section:

QUESTION 383
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

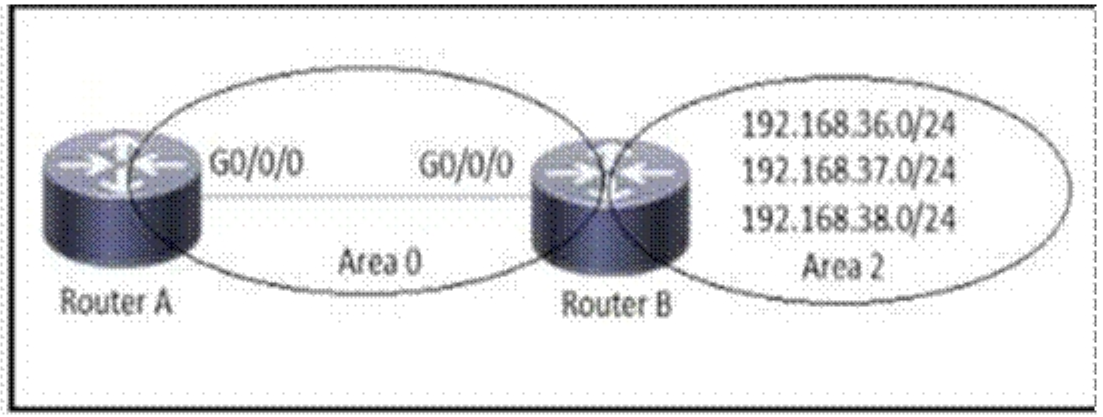
B. Option B

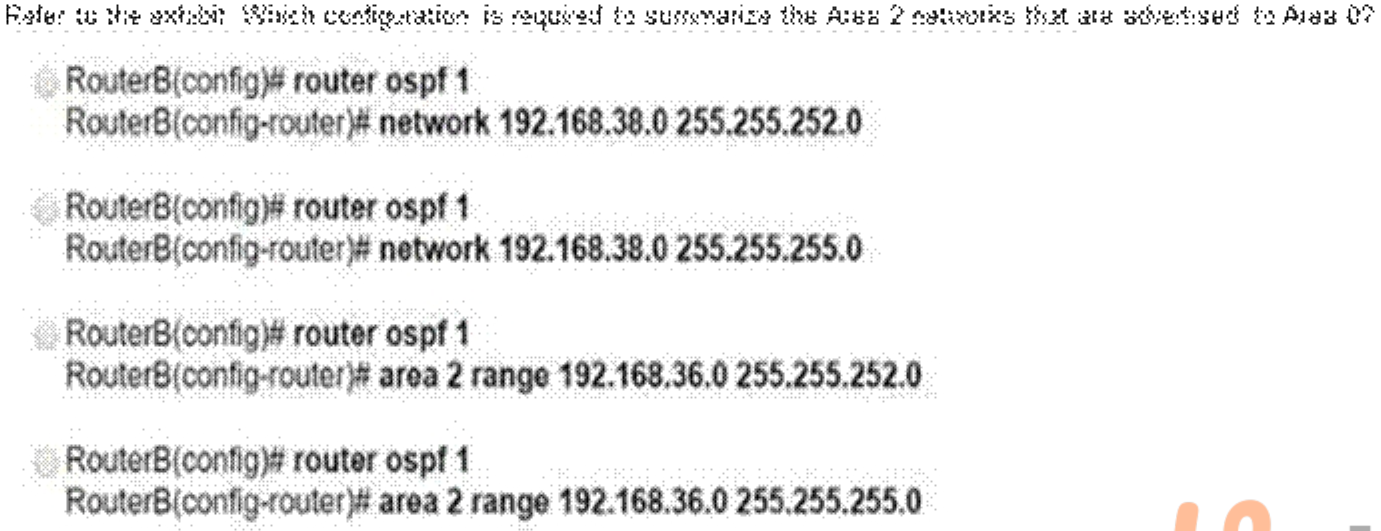
C. Option C

D. Option D

Correct Answer: C
Section:

QUESTION 384
Refer to the exhibit.





Refer to the exhibit. Which configuration is required to summarize the Area 2 networks that are advertised to Area 0?

```
○ RouterB(config)# router ospf 1
  RouterB(config-router)# network 192.168.38.0 255.255.252.0

○ RouterB(config)# router ospf 1
  RouterB(config-router)# network 192.168.38.0 255.255.255.0

○ RouterB(config)# router ospf 1
  RouterB(config-router)# area 2 range 192.168.36.0 255.255.252.0

○ RouterB(config)# router ospf 1
  RouterB(config-router)# area 2 range 192.168.36.0 255.255.255.0
```

Refer to the exhibit. Which configuration is required to summarize the Area 2 networks that are advertised to Area 0?

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

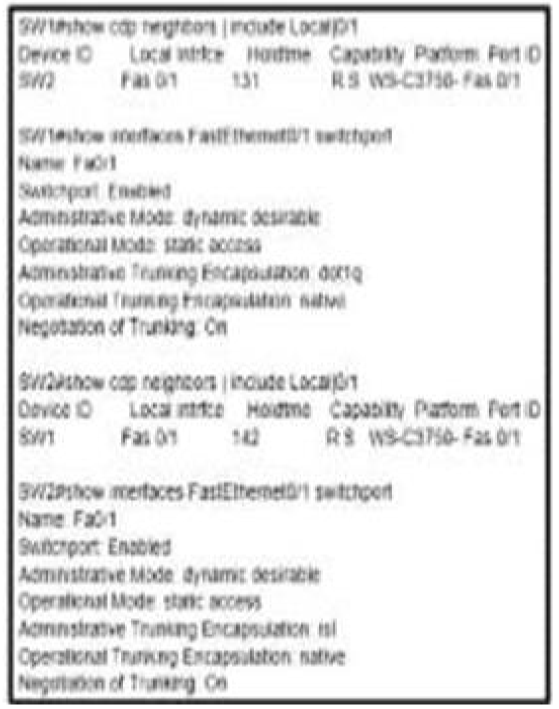
Correct Answer: C
Section:

QUESTION 385
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

Correct Answer: B
Section:

QUESTION 386
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          151         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.

Correct Answer: C
Section:

QUESTION 387
In a Cisco SD-Access wireless environment, which device is responsible for hosting the anycast gateway?

A. fusion router
B. control plane node
C. fabric border node
D. fabric edge node

Correct Answer: D
Section:

QUESTION 388
How does Protocol Independent Multicast function?

A. In sparse mode, it establishes neighbor adjacencies and sends hello messages at 5-second intervals.
B. It uses the multicast routing table to perform the multicast forwarding function.
C. It uses unicast routing information to perform the multicast forwarding function.
D. It uses broadcast routing information to perform the multicast forwarding function.

Correct Answer: C

Section:

QUESTION 389

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

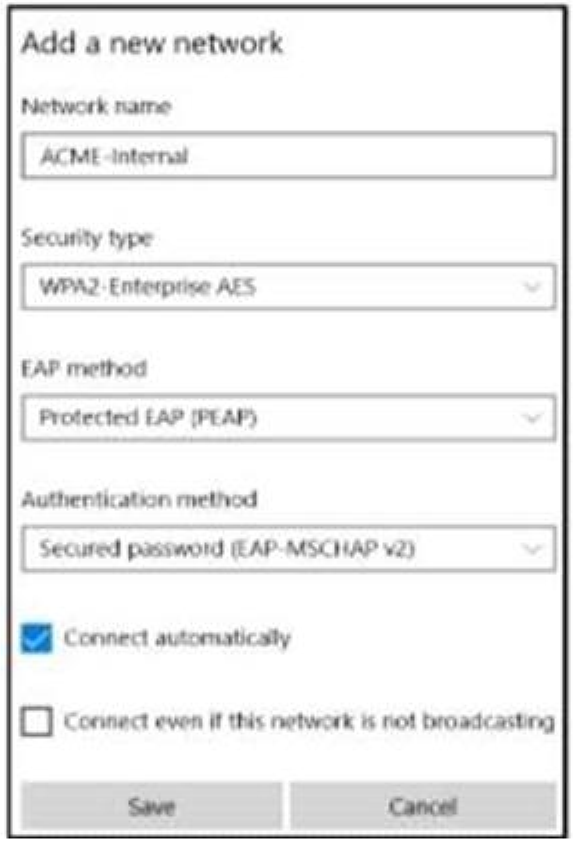
D. Runtime Dashboard

Correct Answer: A

Section:

QUESTION 390

Refer to the exhibit.



Add a new network

Network name: ACME-Internal

Security type: WPA2-Enterprise AES

EAP method: Protected EAP (PEAP)

Authentication method: Secured password (EAP-MSCHAP v2)

☑ Connect automatically

□ Connect even if this network is not broadcasting

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

A. Ensure that the "Connect even if this network is not broadcasting" option is selected.

B. Limit the enabled wireless channels on the laptop to the maximum channel range that is supported by the access points.

C. Change the security type to WPA2-Personal AES.

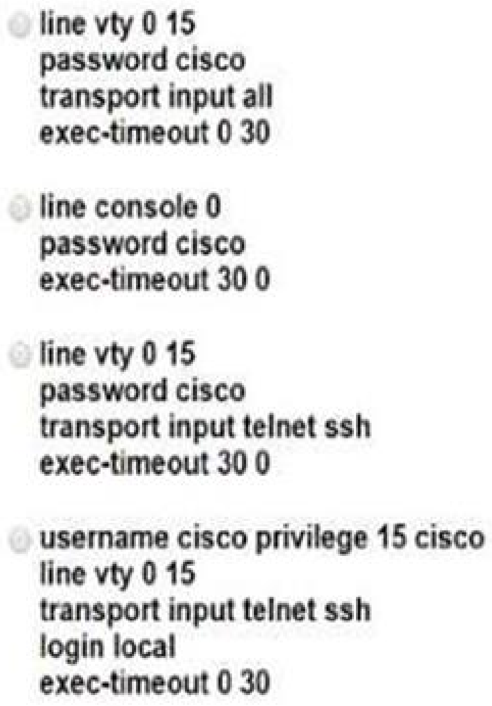
D. Use the empty string as the hidden SSID network name.

Correct Answer: A

Section:

QUESTION 391

A network engineer must configure a switch to allow remote access for all feasible protocols. Only a password must be requested for device authentication and all idle sessions must be terminated in 30 minutes. Which configuration must be applied?



○
```
line vty 0 15
password cisco
transport input all
exec-timeout 0 30
```

○
```
line console 0
password cisco
exec-timeout 30 0
```

○
```
line vty 0 15
password cisco
transport input telnet ssh
exec-timeout 30 0
```

○
```
username cisco privilege 15 cisco
line vty 0 15
transport input telnet ssh
login local
exec-timeout 0 30
```

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

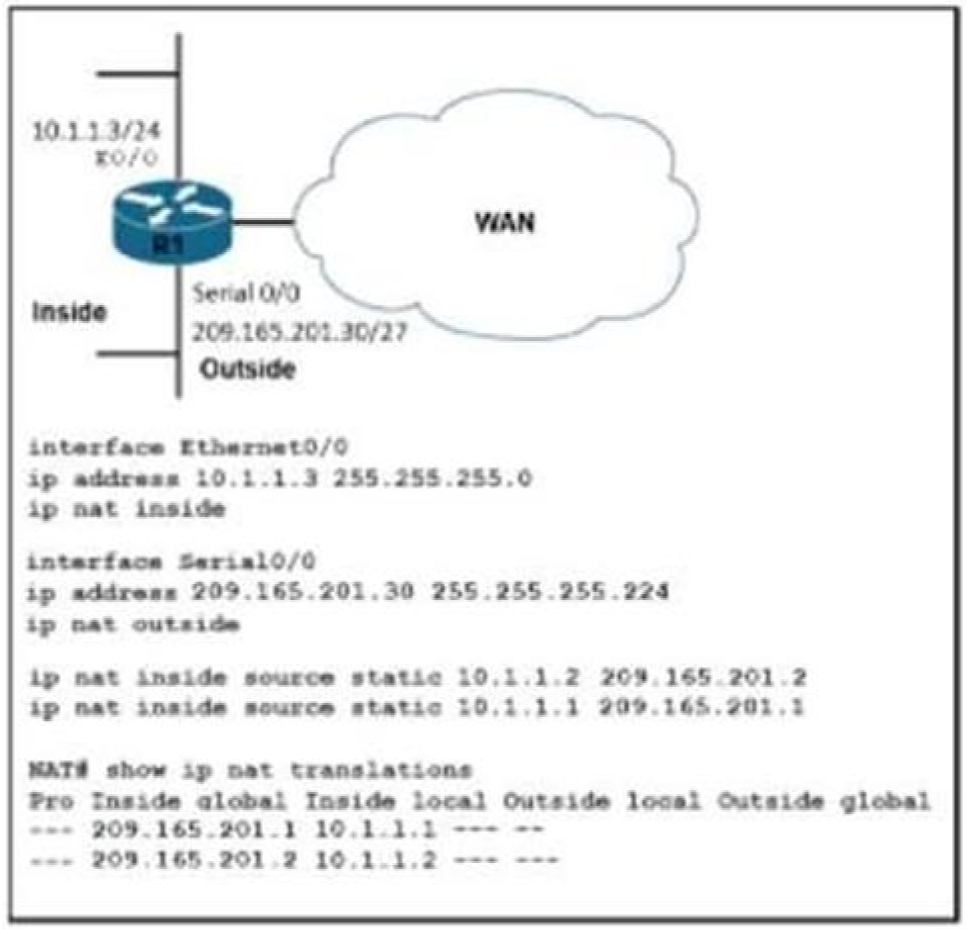
Correct Answer: C
Section:

QUESTION 392
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

Correct Answer: C
Section:

QUESTION 393
Refer to the exhibit. What are two results of the NAT configuration? (Choose two.)



```
interface Ethernet0/0
ip address 10.1.1.3 255.255.255.0
ip nat inside

interface Serial0/0
ip address 209.165.201.30 255.255.255.224
ip nat outside

ip nat inside source static 10.1.1.2 209.165.201.2
ip nat inside source static 10.1.1.1 209.165.201.1

NAT# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.201.1 10.1.1.1 --- --
--- 209.165.201.2 10.1.1.2 --- ---
```

A. Packets with a destination of 200.1.1.1 are translated to 10.1.1.1 or .2. respectively.

B. A packet that is sent to 200.1.1.1 from 10.1.1.1 is translated to 209.165.201.1 on R1.

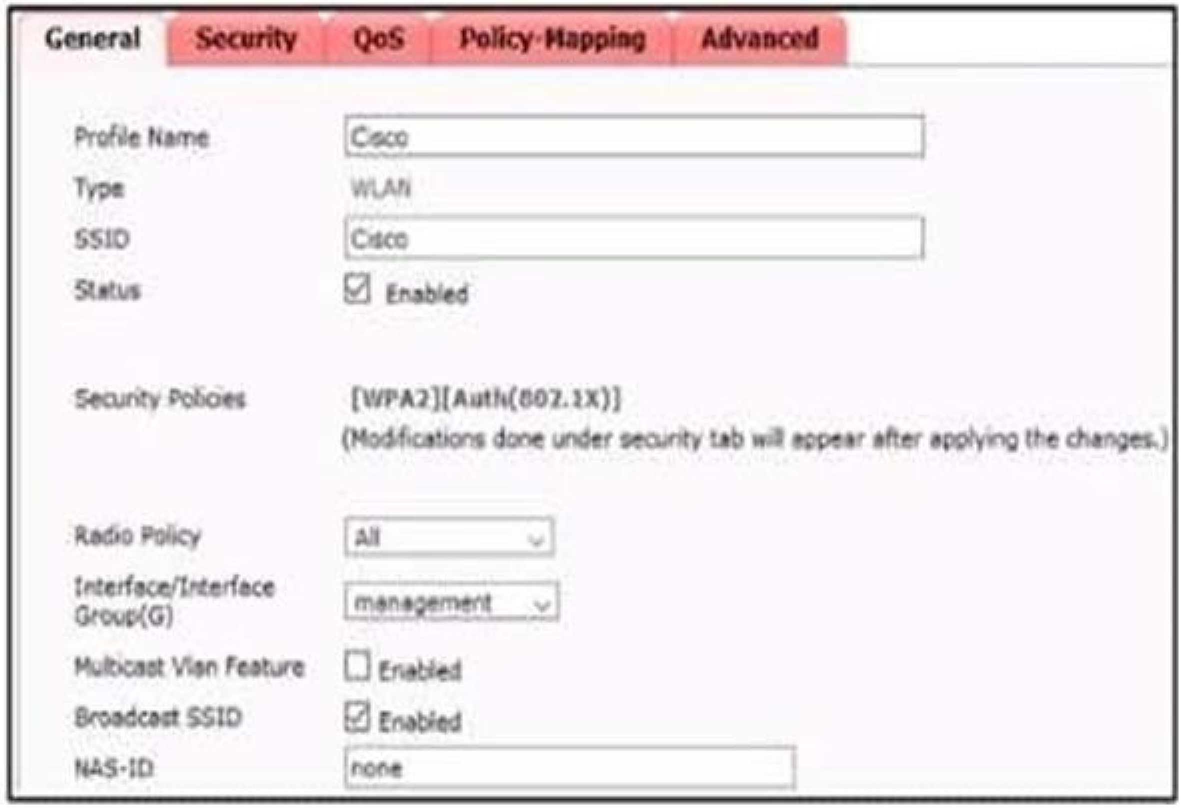
C. R1 looks at the destination IP address of packets entering S0/0 and destined for inside hosts.

D. R1 processes packets entering E0/0 and S0/0 by examining the source IP address.

E. R1 is performing NAT for inside addresses and outside address.

Correct Answer: B, C
Section:

QUESTION 394
Refer to the exhibit.



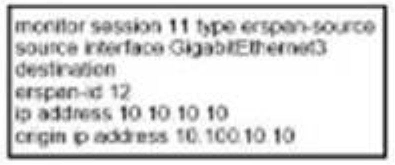
Profile Name	Cisco
Type	WLAN
SSID	Cisco
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	none

Clients report that they cannot connect to this SSID using the provided PSK.
Which action will resolve this issue?

A. Apply the correct interface to this WLAN.
B. Apply the changes this SSID.
C. Select the PSK under authentication key management.
D. Define the correct Radio Policy.

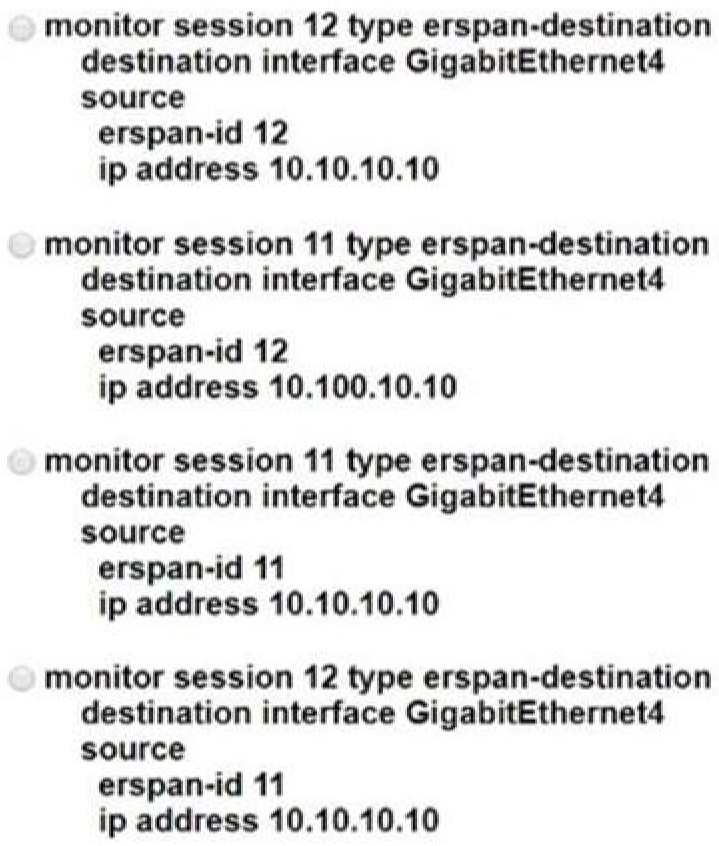
Correct Answer: A
Section:

QUESTION 395
Refer to the exhibit.



```
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

Correct Answer: A

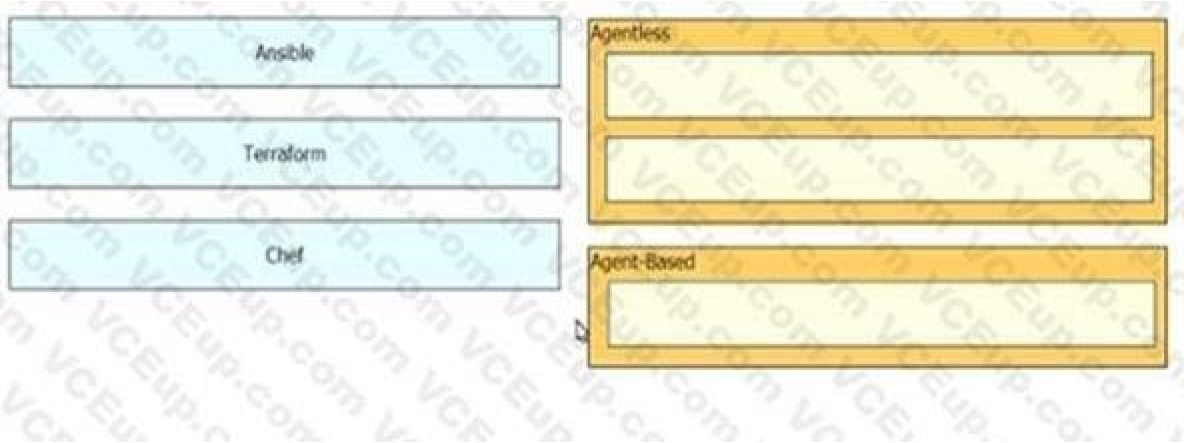
Section:

QUESTION 396

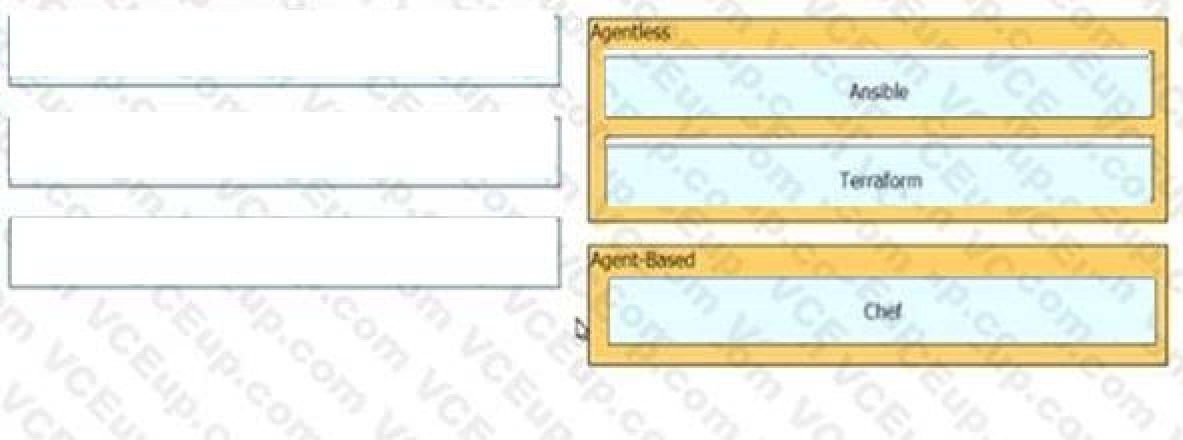
DRAG DROP

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

Select and Place:



Correct Answer:



Agentless

Ansible

Terraform

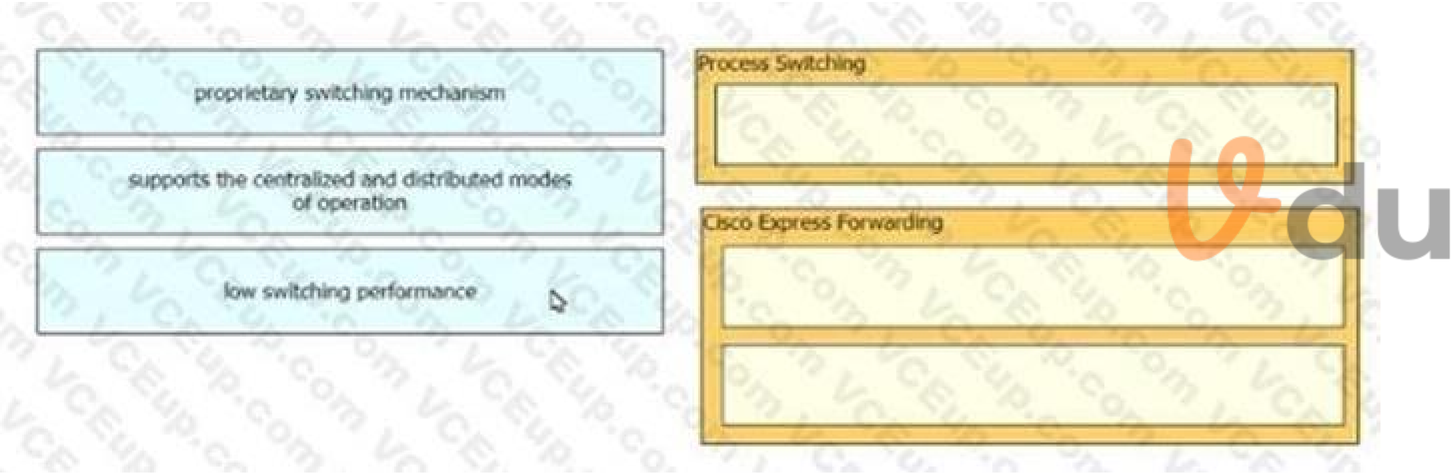
Agent-Based

Chef

Section:
Explanation:

QUESTION 397
DRAG DROP
Drag and drop the characteristics from the left onto the switching architectures on the right.

Select and Place:



proprietary switching mechanism

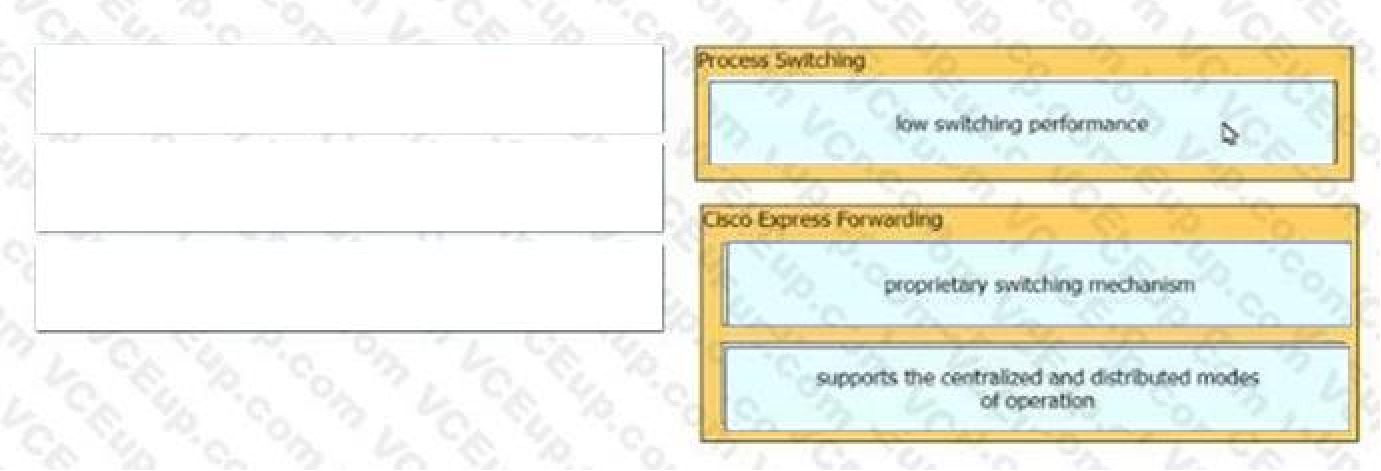
supports the centralized and distributed modes of operation

low switching performance

Process Switching

Cisco Express Forwarding

Correct Answer:



Process Switching

low switching performance

Cisco Express Forwarding

proprietary switching mechanism

supports the centralized and distributed modes of operation

Section:
Explanation:

QUESTION 398

How do the RIB and the FIB differ?

A. FIB contains routes learned through a dynamic routing protocol, and the RIB contains routes that are static or directly connected.
B. RIB contains the interface for a destination, and the FIB contains the next hop information.
C. FIB is derived from the control plane, and the RIB is derived from the data plane.
D. RIB is derived from the control plane, and the FIB is derived from the RIB.

Correct Answer: D
Section:

QUESTION 399
In a Cisco StackWise Virtual environment, which planes are virtually combined in the common logical switch?

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

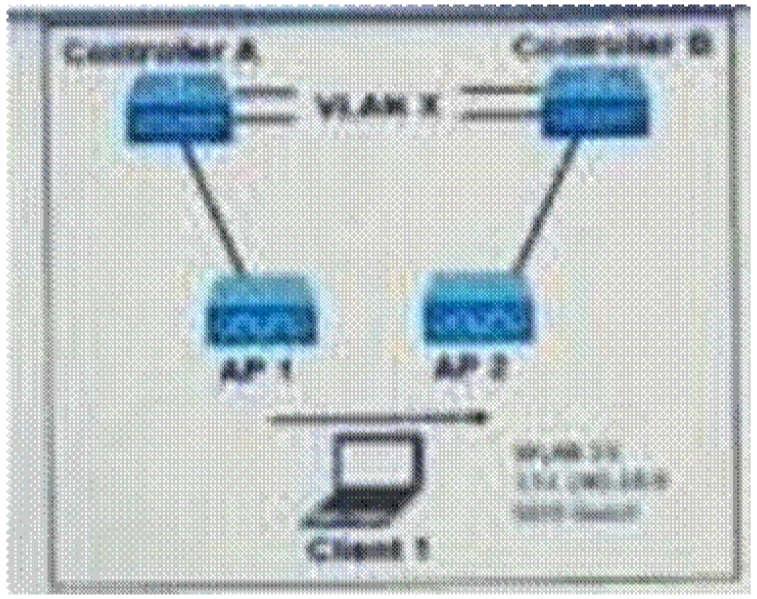
Correct Answer: C
Section:

QUESTION 400
How do stratum levels relate to the distance from a time source?

A. Stratum 1 devices are connected directly to an authoritative time source.
B. Stratum 15 devices are connected directly to an authoritative time source
C. Stratum 0 devices are connected directly to an authoritative time source.
D. Stratum 15 devices are an authoritative time source.

Correct Answer: C
Section:

QUESTION 401
Refer to the exhibit.



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

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

Correct Answer: D
Section:

QUESTION 402
the following system log message is presented after a network administrator configures a GRE tunnel:
%TUN-5-RECURDOWN Interface Tunnel 0 temporarily disabled due to recursive routing.
Why is tunnel 0 disabled?

A. Because dynamic routing is not enabled
B. Because the tunnel cannot reach its tunnel destination
C. Because the best path to the tunnel destination is through the tunnel itself
D. Because the router cannot recursively identify its egress forwarding interface

Correct Answer: C
Section:

QUESTION 403
Which action is the vSmart controller responsible for in a Cisco SO-WAN deployment?

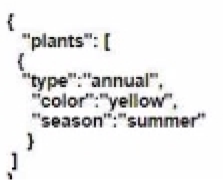
A. gather telemetry data from WAN Edge routes
B. manage, maintain, and gather configuration and status for nodes within me SD-WAN fabric
C. onboard WAN Edge nodes into the SD-WAN fabric
D. distribute security information for tunnel establishment between WAN Edge routers

Correct Answer: D
Section:

QUESTION 404

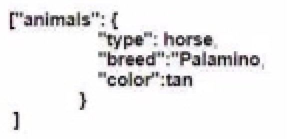
Which JSON script is properly formatted?

A)



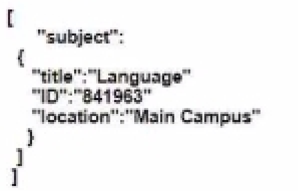
```
{
  "plants": [
 {
 "type":"annual",
   "color":"yellow",
   "season":"summer"
  }
 ]
,
```

B)



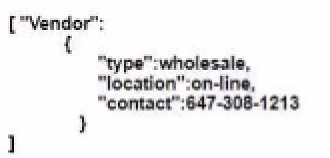
```
["animals": {
              "type": horse,
              "breed":"Palamino,
              "color":tan
          }
 ]
```

C)



```
[
   "subject":
 {
  "title":"Language"
  "ID":"841963"
  "location":"Main Campus"
 }
 ]
]
```

D)



```
[ "Vendor":
        {
              "type":wholesale,
              "location":on-line,
              "contact":647-308-1213
          }
]
```

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

Correct Answer: A
Section:

QUESTION 405

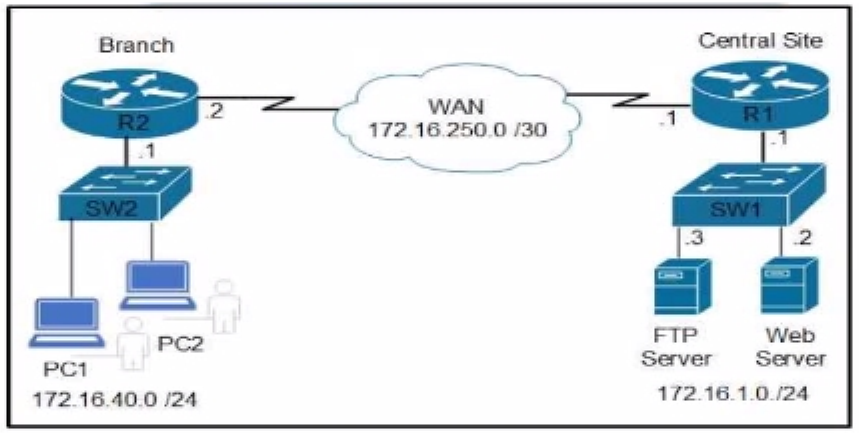
What does the Cisco WLC Layer 3 roaming feature allow clients to do?

A. maintain their IP address when roaming to an AP 01 controller with a different client VLAN assignment
B. maintain their connection between APs even when the AP management VLANs arc different
C. roam seamlessly between controllers even when the controller management VLANs are different
D. maintain their connection even if the client IP address changes when roaming

Correct Answer: A
Section:

QUESTION 406

Refer to the exhibit.



Which command required to validate that an IP SLA configuration matches the traffic between the branch office and the central site?

A. R1# show ip sla configuration
B. R1# show Ip sla group schedule
C. R1# show Ip route
D. R1# show ip sla statistics

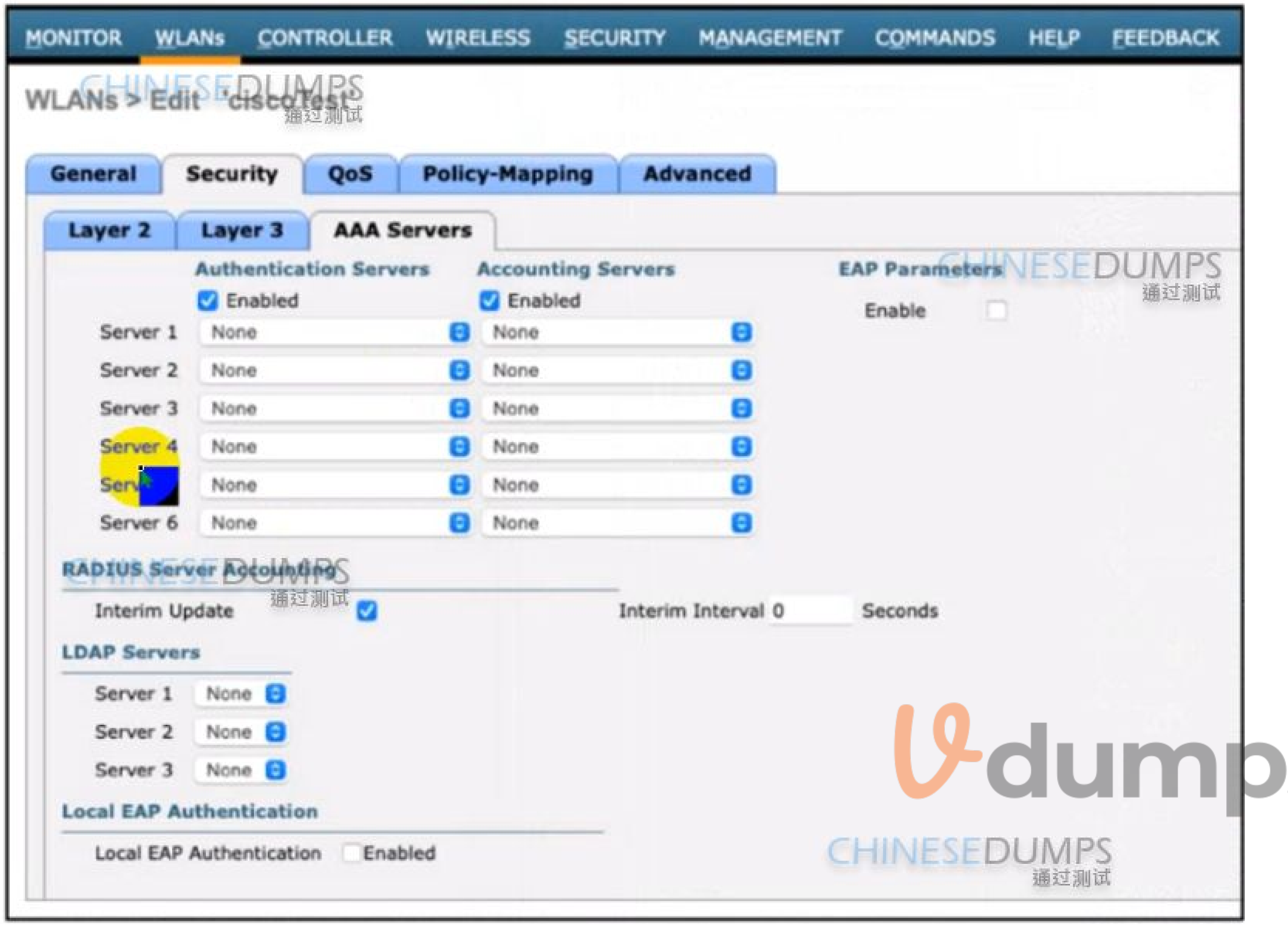
Correct Answer: D
Section:
Explanation:
To validate that an IP SLA configuration matches the traffic between the branch office and the central site, the commandR1# show ip sla statisticsis used. This command provides details on the IP SLA operations and their statistics, which include the latest return code and over thresholds occurrences, thus confirming whether the IP SLA operations are being executed as configured and if they match the expected traffic patterns.
References: The Cisco documentation on IP SLA commands provides information on how to use theshow ip sla statisticscommand to verify IP SLA operations. This is aligned with the Implementing and Operating Cisco Service Provider Network Core Technologies (SPCOR) curriculum, which covers the monitoring and verification of IP SLA configurations as part of ensuring network performance and reliability.

QUESTION 407
Which security option protects credentials train snifter attacks in a basic API authentication?

A. TLS of SSL for communication
B. next-generation firewall
C. VPN connection between client and server
D. AAA services to authenticate the API

Correct Answer: A
Section:

QUESTION 408
Refer to the Exhibit.



WLANs > Edit 'ciscoTest'

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	None	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Serv	None	None
Server 6	None	None

EAP Parameters

Enable □

RADIUS Server Accounting

Interim Update ☑ Interim Interval 0 Seconds

LDAP Servers

Server 1	None
Server 2	None
Server 3	None

Local EAP Authentication

Local EAP Authentication □ Enabled

Refer to the exhibit. An engineer must configure a Cisco WLC with WPA2 Enterprise mode and avoid global server lists. Which action is required?

A. Apply CISCO ISE default settings.
B. Disable the RADIUS server accounting interim update.
C. Select a RADIUS authentication server.
D. Enable EAP parameters.

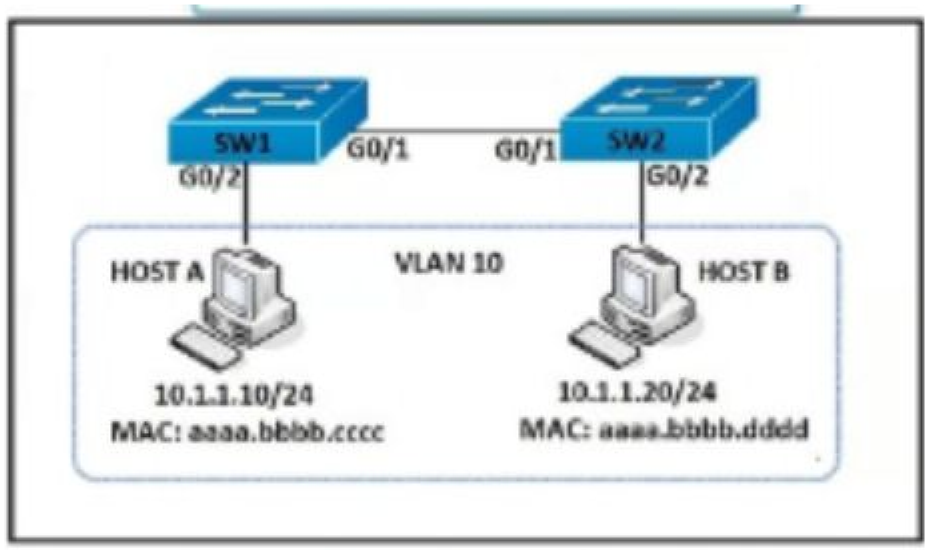
Correct Answer: C
Section:

QUESTION 409
Which two security mechanisms aie used by Cisco Threat Defense to gain visibility into the most dangerous cyber threats? (Choose two.)

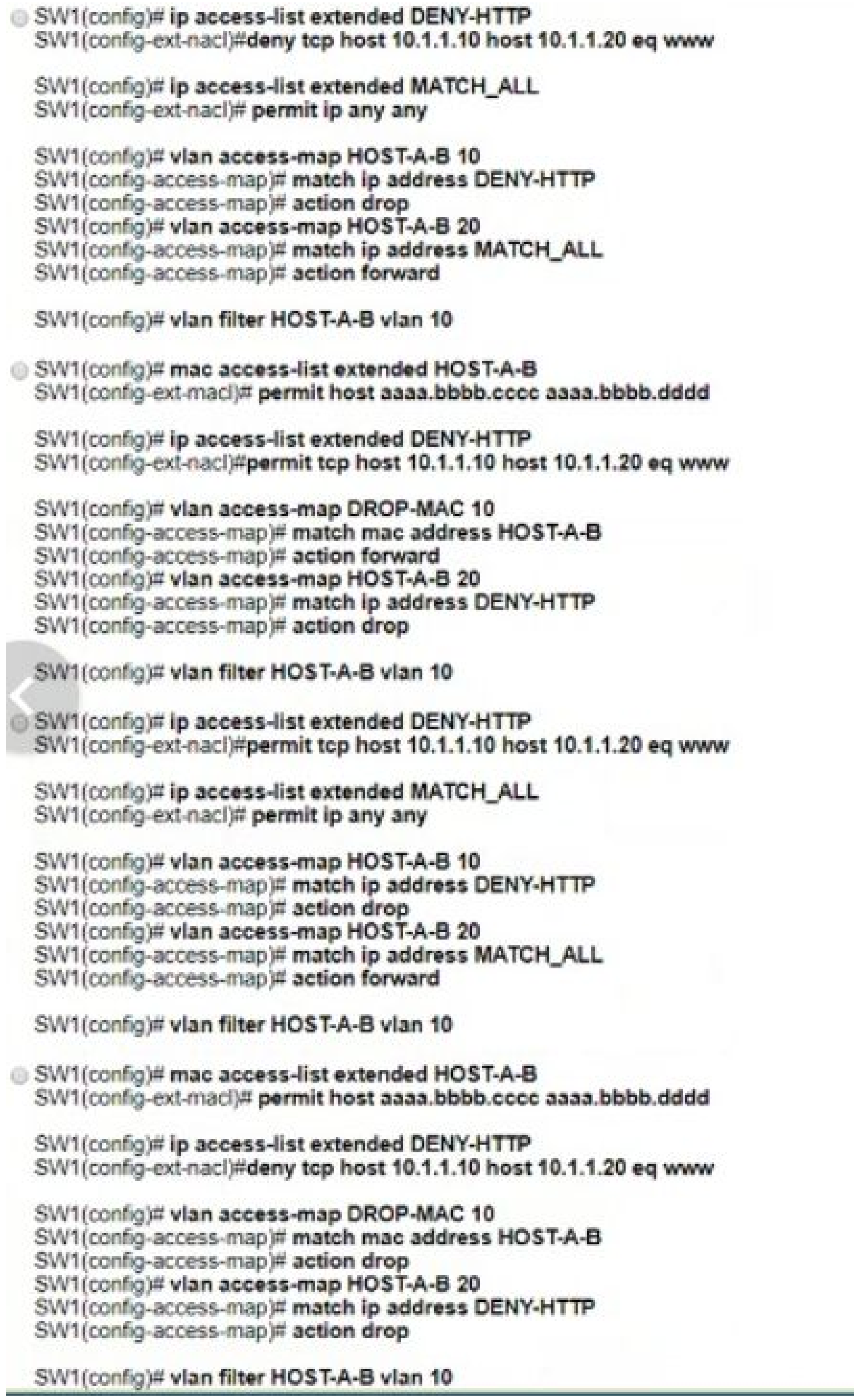
A. Traffic Telemetry
B. VLAN segmentation
C. virtual private networks
D. dynamic enforce policy
E. file reputation

Correct Answer: A, E
Section:

QUESTION 410
Refer to the Exhibit.



Refer to the exhibit. An engineer must deny HTTP traffic from host A to host B while allowing all other communication between the hosts. Which command set accomplishes this task?

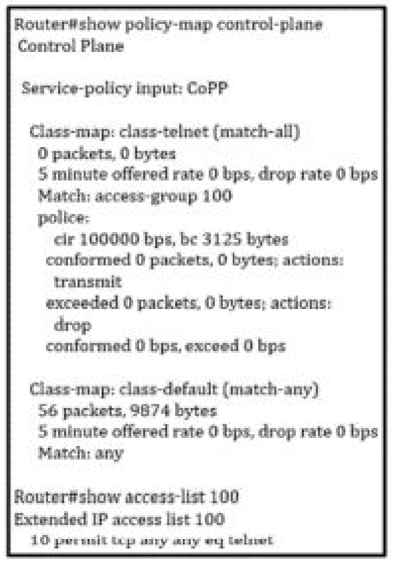


```
○ SW1(config)# ip access-list extended DENY-HTTP
  SW1(config-ext-nacl)#deny tcp host 10.1.1.10 host 10.1.1.20 eq www

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

  SW1(config)# vlan access-map HOST-A-B 10
  SW1(config-access-map)# match ip address DENY-HTTP
  SW1(config-access-map)# action drop
  SW1(config)# vlan access-map HOST-A-B 20
  SW1(config-access-map)# match ip address MATCH_ALL
  SW1(config-access-map)# action forward

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

○ SW1(config)# mac access-list extended HOST-A-B
  SW1(config-ext-macl)# permit host aaaa.bbbb.cccc aaaa.bbbb.dddd

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

  SW1(config)# vlan access-map DROP-MAC 10
  SW1(config-access-map)# match mac address HOST-A-B
  SW1(config-access-map)# action forward
  SW1(config)# vlan access-map HOST-A-B 20
  SW1(config-access-map)# match ip address DENY-HTTP
  SW1(config-access-map)# action drop

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

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

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

  SW1(config)# vlan access-map HOST-A-B 10
  SW1(config-access-map)# match ip address DENY-HTTP
  SW1(config-access-map)# action drop
  SW1(config)# vlan access-map HOST-A-B 20
  SW1(config-access-map)# match ip address MATCH_ALL
  SW1(config-access-map)# action forward

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

○ SW1(config)# mac access-list extended HOST-A-B
  SW1(config-ext-macl)# permit host aaaa.bbbb.cccc aaaa.bbbb.dddd

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

  SW1(config)# vlan access-map DROP-MAC 10
  SW1(config-access-map)# match mac address HOST-A-B
  SW1(config-access-map)# action drop
  SW1(config)# vlan access-map HOST-A-B 20
  SW1(config-access-map)# match ip address DENY-HTTP
  SW1(config-access-map)# action drop

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

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

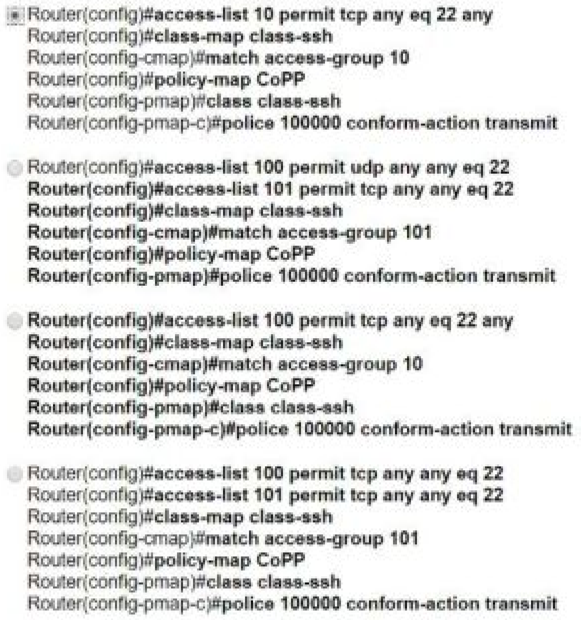
Correct Answer: A
Section:

QUESTION 411
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
```

Refer to the exhibit. Which commands are required to allow SSH connections to the router?

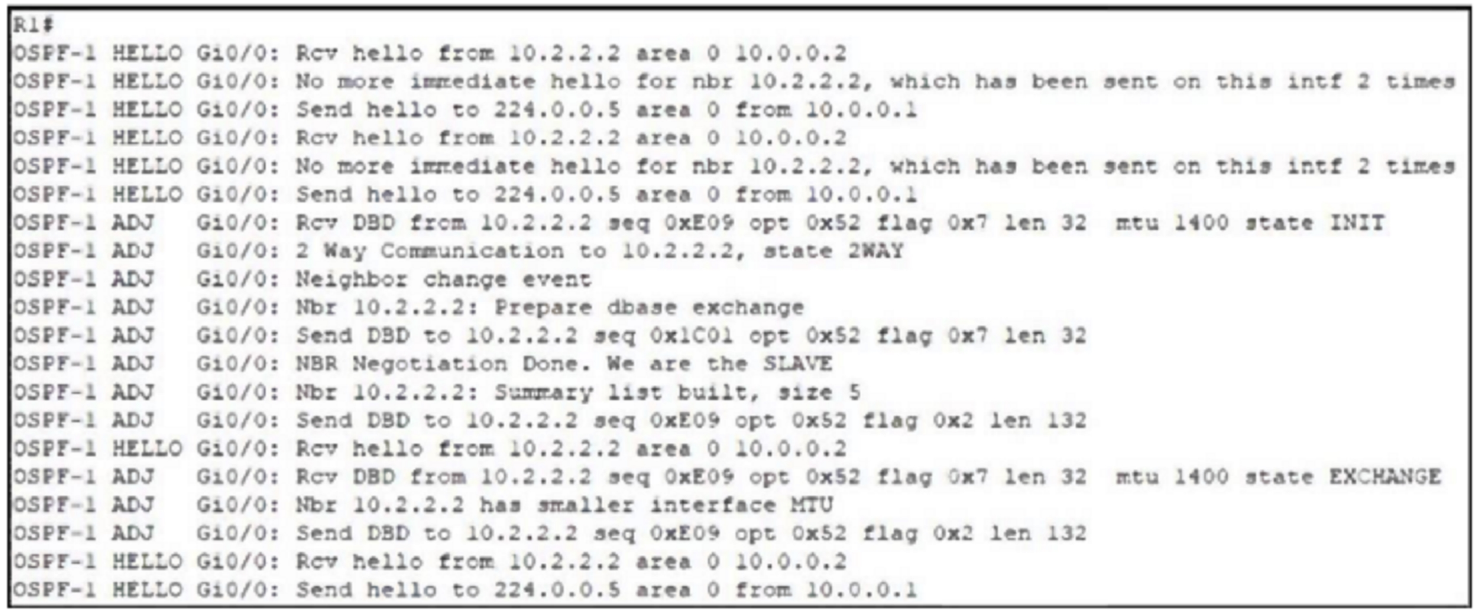


```
● Router(config)#access-list 10 permit tcp any eq 22 any
  Router(config)#class-map class-ssh
  Router(config-cmap)#match access-group 10
  Router(config)#policy-map CoPP
  Router(config-pmap)#class class-ssh
  Router(config-pmap-c)#police 100000 conform-action transmit

○ 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

○ 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

○ 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

Correct Answer: D
Section:

QUESTION 412
Two indirectly connected routers fail to form an OSPF neighborship. What is the cause of the issue?

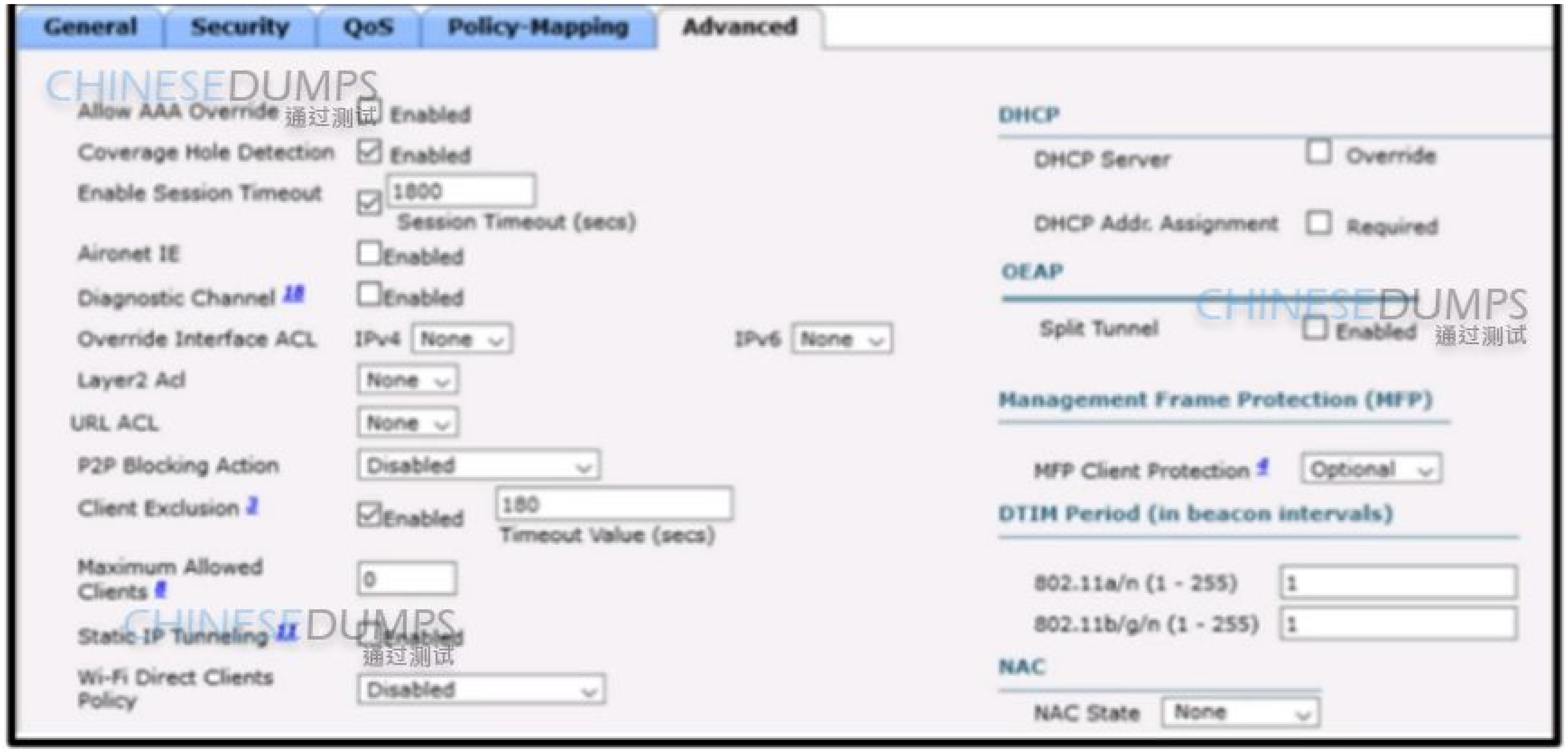


```
R1#
OSPF-1 HELLO Gi0/0: Rcv hello from 10.2.2.2 area 0 10.0.0.2
OSPF-1 HELLO Gi0/0: No more immediate hello for nbr 10.2.2.2, which has been sent on this intf 2 times
OSPF-1 HELLO Gi0/0: Send hello to 224.0.0.5 area 0 from 10.0.0.1
OSPF-1 HELLO Gi0/0: Rcv hello from 10.2.2.2 area 0 10.0.0.2
OSPF-1 HELLO Gi0/0: No more immediate hello for nbr 10.2.2.2, which has been sent on this intf 2 times
OSPF-1 HELLO Gi0/0: Send hello to 224.0.0.5 area 0 from 10.0.0.1
OSPF-1 ADJ   Gi0/0: Rcv DBD from 10.2.2.2 seq 0xE09 opt 0x52 flag 0x7 len 32  mtu 1400 state INIT
OSPF-1 ADJ   Gi0/0: 2 Way Communication to 10.2.2.2, state 2WAY
OSPF-1 ADJ   Gi0/0: Neighbor change event
OSPF-1 ADJ   Gi0/0: Nbr 10.2.2.2: Prepare dbase exchange
OSPF-1 ADJ   Gi0/0: Send DBD to 10.2.2.2 seq 0x1C01 opt 0x52 flag 0x7 len 32
OSPF-1 ADJ   Gi0/0: NBR Negotiation Done. We are the SLAVE
OSPF-1 ADJ   Gi0/0: Nbr 10.2.2.2: Summary list built, size 5
OSPF-1 ADJ   Gi0/0: Send DBD to 10.2.2.2 seq 0xE09 opt 0x52 flag 0x2 len 132
OSPF-1 HELLO Gi0/0: Rcv hello from 10.2.2.2 area 0 10.0.0.2
OSPF-1 ADJ   Gi0/0: Rcv DBD from 10.2.2.2 seq 0xE09 opt 0x52 flag 0x7 len 32  mtu 1400 state EXCHANGE
OSPF-1 ADJ   Gi0/0: Nbr 10.2.2.2 has smaller interface MTU
OSPF-1 ADJ   Gi0/0: Send DBD to 10.2.2.2 seq 0xE09 opt 0x52 flag 0x2 len 132
OSPF-1 HELLO Gi0/0: Rcv hello from 10.2.2.2 area 0 10.0.0.2
OSPF-1 HELLO Gi0/0: Send hello to 224.0.0.5 area 0 from 10.0.0.1
```

A. failing hello packets between the two routers
B. MTU mismatch
C. OSPF network type mismatch
D. DR/BDR selection dispute

Correct Answer: B
Section:

QUESTION 413
Refer to the Exhibit.



Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE □ Enabled
Diagnostic Channel □ Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
URL ACL None
P2P Blocking Action Disabled
Client Exclusion ☑ Enabled 180 Timeout Value (secs)
Maximum Allowed Clients 0
Static IP Tunneling □ Enabled
Wi-Fi Direct Clients Policy Disabled

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

OEAP
Split Tunnel □ Enabled

Management Frame Protection (MFP)
MFP Client Protection Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
NAC State None

Refer to the exhibit An engineer is troubleshooting an mDNS issue in an environment where Cisco ISE is used to dynamically assign mDNS roles to users The engineer has confirmed that ISE is sending the correct values, but name resolution is not functioning as expected Which WLC configuration change resolves the issue?

A. Enable AAA Override
B. Set MFP client protection to Required
C. Enable Aironet IE.
D. Change NAC state to ISE NAC

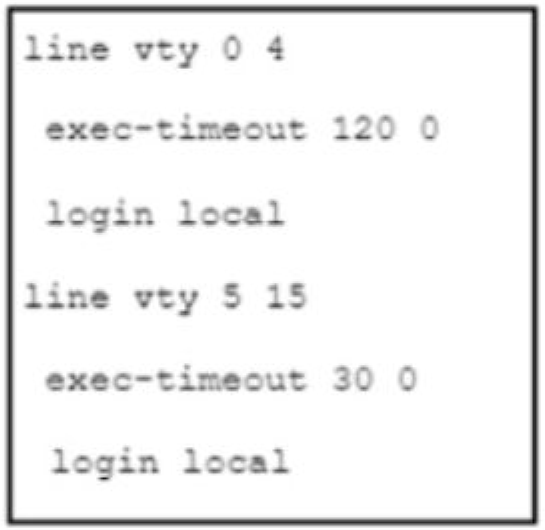
Correct Answer: A
Section:

QUESTION 414
How is OAuth framework used in REST API?

A. by providing the user credentials to the external application
B. by providing the external application a token that authorizes access to the account
C. as a framework to hash the security Information in the REST URL
D. as a framework to hide the security information in the REST URL

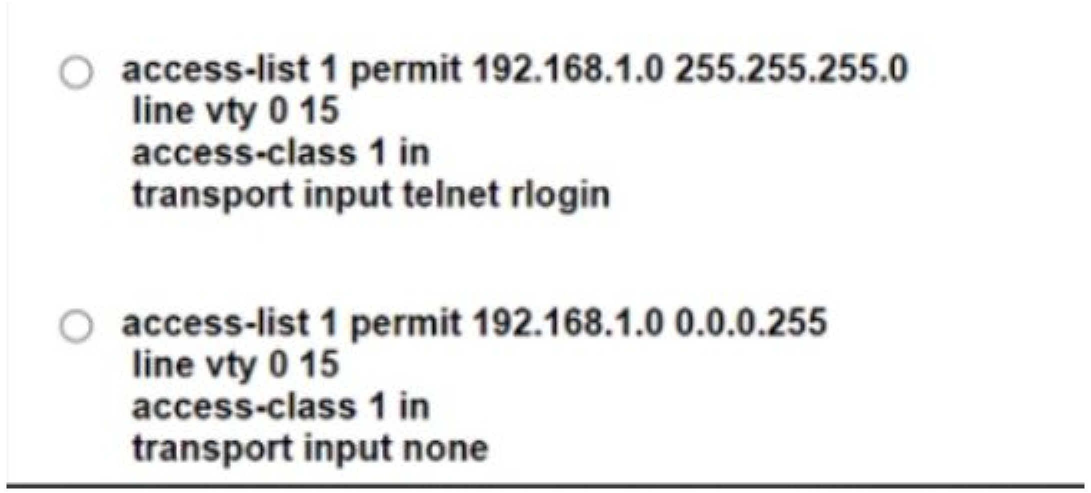
Correct Answer: B
Section:

QUESTION 415
Refer to the Exhibit.

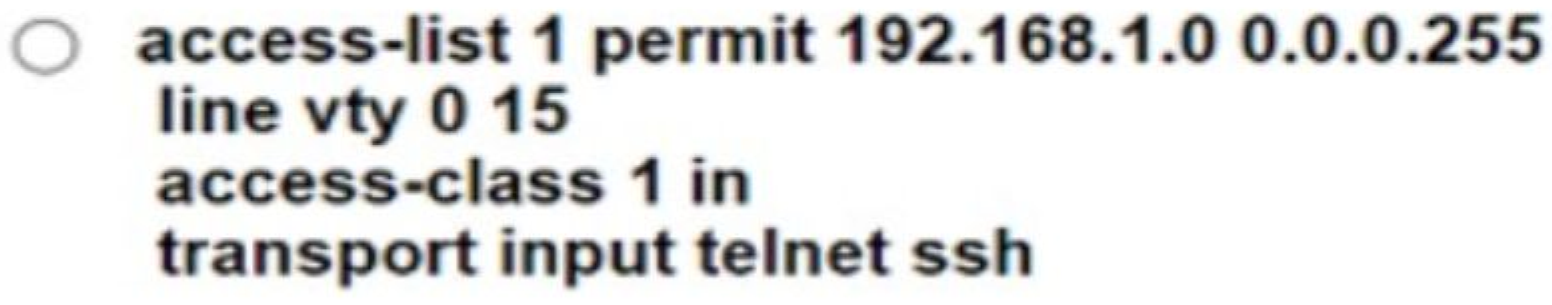


```
line vty 0 4
 exec-timeout 120 0
 login local
line vty 5 15
 exec-timeout 30 0
 login local
```

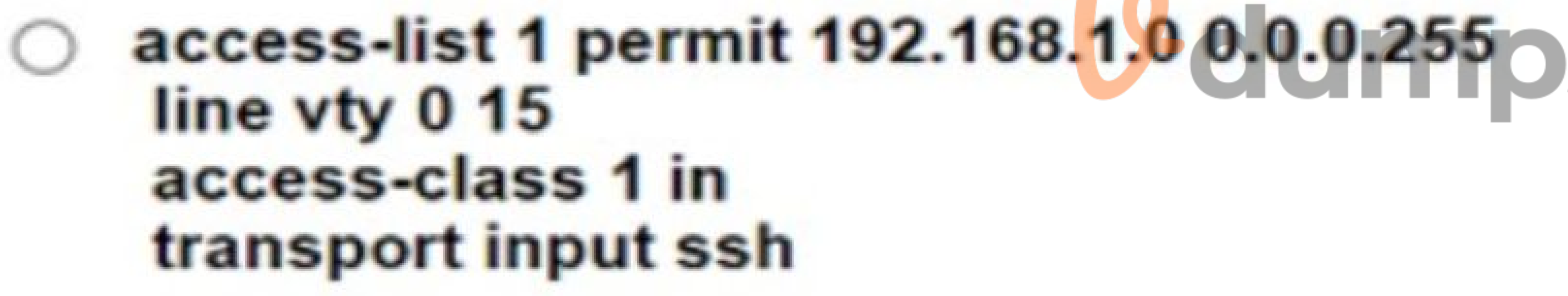
Refer to the exhibit. An engineer must update the existing configuration to achieve these results
Only administrators from the 192.168.1.0/24 subnet can access the vty lines.
Access to the vty lines using dear-text protocols is prohibited.
Which command set should be applied?



```
○ access-list 1 permit 192.168.1.0 255.255.255.0
  line vty 0 15
  access-class 1 in
  transport input telnet rlogin

○ access-list 1 permit 192.168.1.0 0.0.0.255
  line vty 0 15
  access-class 1 in
  transport input none
```



```
○ access-list 1 permit 192.168.1.0 0.0.0.255
  line vty 0 15
  access-class 1 in
  transport input telnet ssh
```



```
○ access-list 1 permit 192.168.1.0 0.0.0.255
  line vty 0 15
  access-class 1 in
  transport input ssh
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C
Section:

QUESTION 416
Which two features does the Cisco SD-Access architectures add to a traditional campus network?

A. private VLANs

B. Identity services

C. modular QoS

D. software-defined segmentation

E. SD-WAN

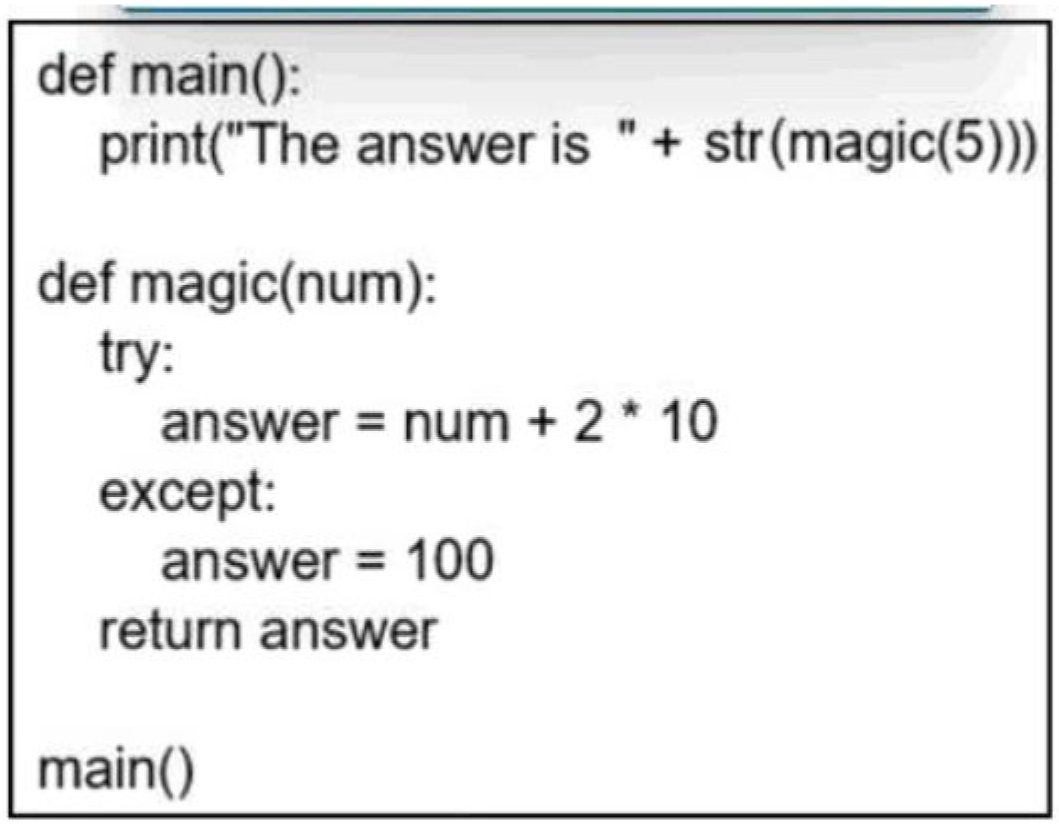
Correct Answer: B, D
Section:

QUESTION 417
Which two operational modes enables an AP to scan one or more wireless channels for rogue access points and at the same time provide wireless services to clients? (Choose two)

A. sniffer
B. FlexConnect
C. rogue detector
D. monitor
E. local

Correct Answer: B, E
Section:

QUESTION 418
Refer to the Exhibit.



```
def main():
    print("The answer is  " + str(magic(5)))

def magic(num):
    try:
        answer = num + 2 * 10
    except:
        answer = 100
    return answer

main()
```

Refer to the exhibit. What is displayed when the code is run?

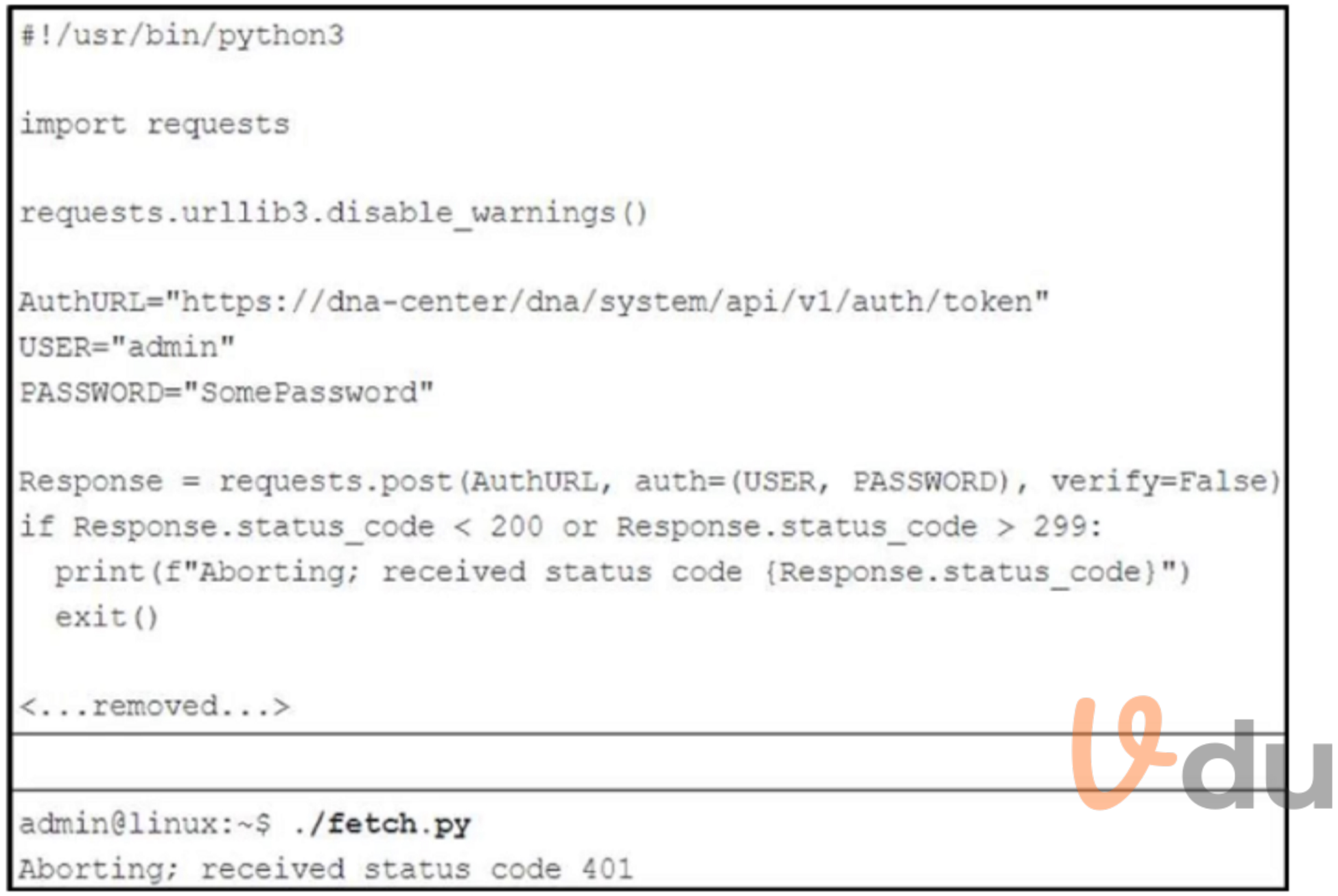
A. The answer is 100
B. The answer is 5
C. The answer is 25
D. The answer is 70

Correct Answer: C

Section:

QUESTION 419

Refer to the Exhibit.



```
#!/usr/bin/python3

import requests

requests.urllib3.disable_warnings()

AuthURL="https://dna-center/dna/system/api/v1/auth/token"
USER="admin"
PASSWORD="SomePassword"

Response = requests.post(AuthURL, auth=(USER, PASSWORD), verify=False)
if Response.status_code < 200 or Response.status_code > 299:
  print(f"Aborting; received status code {Response.status_code}")
  exit()

<...removed...>
```

```
admin@linux:~$ ./fetch.py
Aborting; received status code 401
```

Refer to the exhibit. An administrator writes a script to fetch the list of devices that are registered with Cisco DNA Center. Why does the execution abort?

A. The authentication URL is incorrect.

B. The 'dna-center' hostname cannot be resolved to an IP address.

C. The TLS certificate of DNA Center is invalid.

D. The username or the password is Incorrect.

Correct Answer: D

Section:

QUESTION 420

Which virtualization component creates VMs and performs hardware abstraction that allows multiple VMs to run at the same time?

A. rkt

B. Docker

C. container

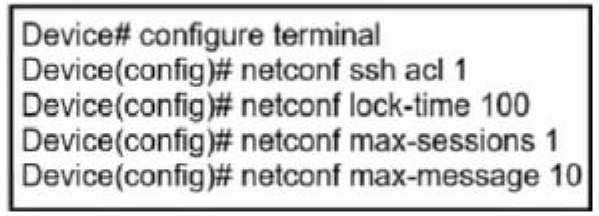
D. hypervisor

Correct Answer: D

Section:

QUESTION 421

Refer to the Exhibit.



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

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

A. Device(config)# netconf max-message 1000

B. Device(config)# netconf max-sessions 100

C. Device(config) netconf lock-time 500

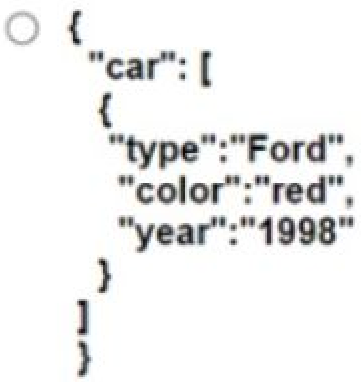
D. Device(config)# no netconf ssh aci 1

Correct Answer: D

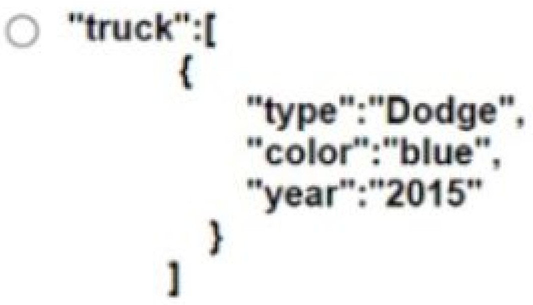
Section:

QUESTION 422

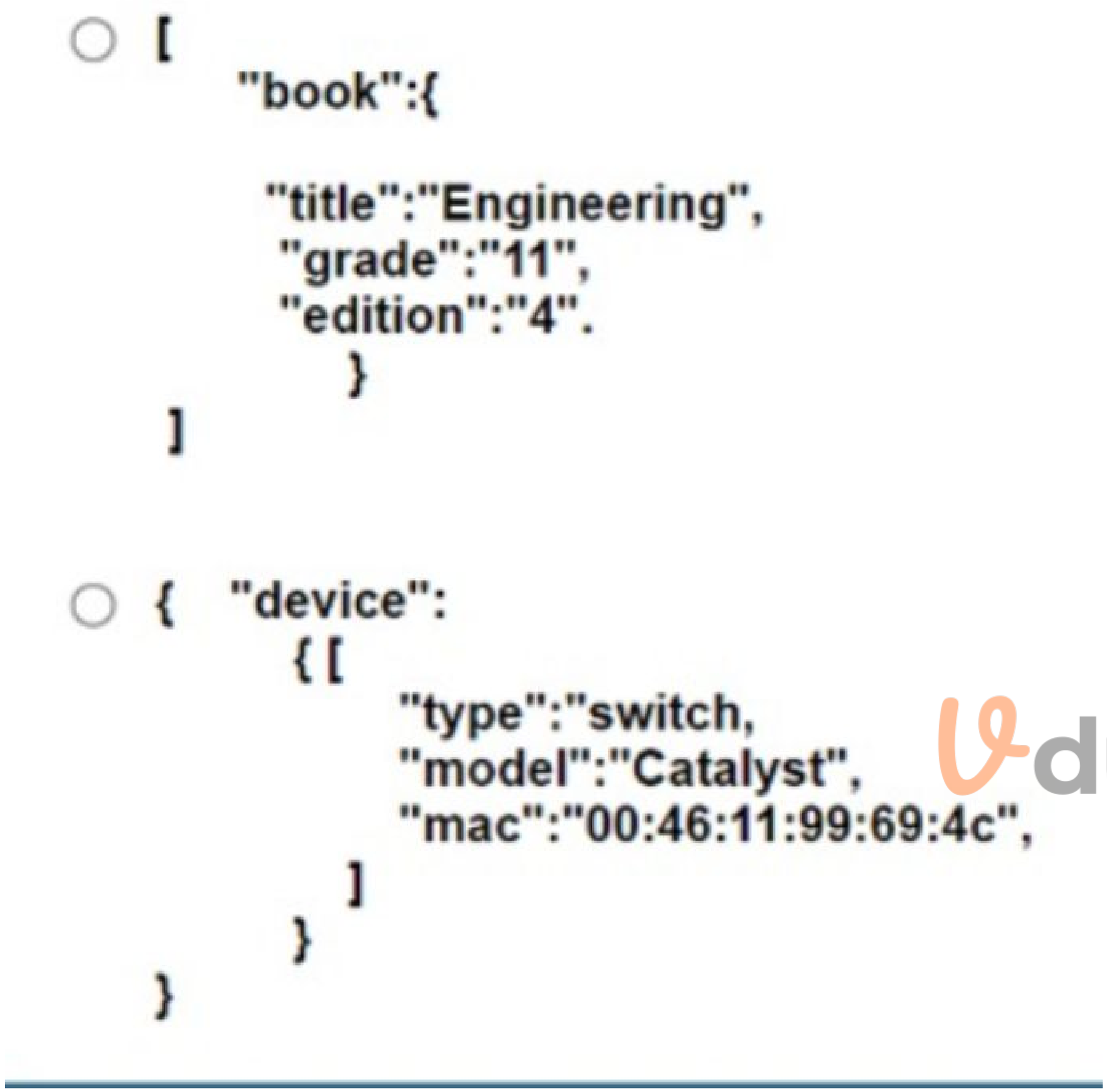
Which JSON script is properly formatted?



```
○ {
   "car": [
    {
     "type":"Ford",
      "color":"red",
      "year":"1998"
    }
   ]
  }
```



```
○ "truck":[
         {
               "type":"Dodge",
               "color":"blue",
               "year":"2015"
            }
        ]
```



```
○ [
      "book":{

        "title":"Engineering",
         "grade":"11",
         "edition":"4".
            }
   ]
```

```
○ {   "device":
        { [
              "type":"switch,
              "model":"Catalyst",
              "mac":"00:46:11:99:69:4c",
          ]
        }
  }
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A
Section:

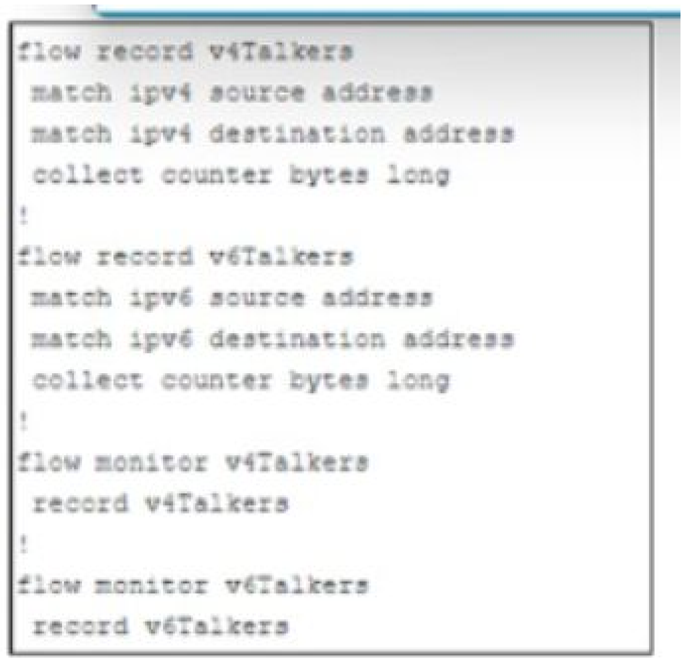
QUESTION 423
Which resource must a hypervisor make available to the virtual machines?

A. bandwidth

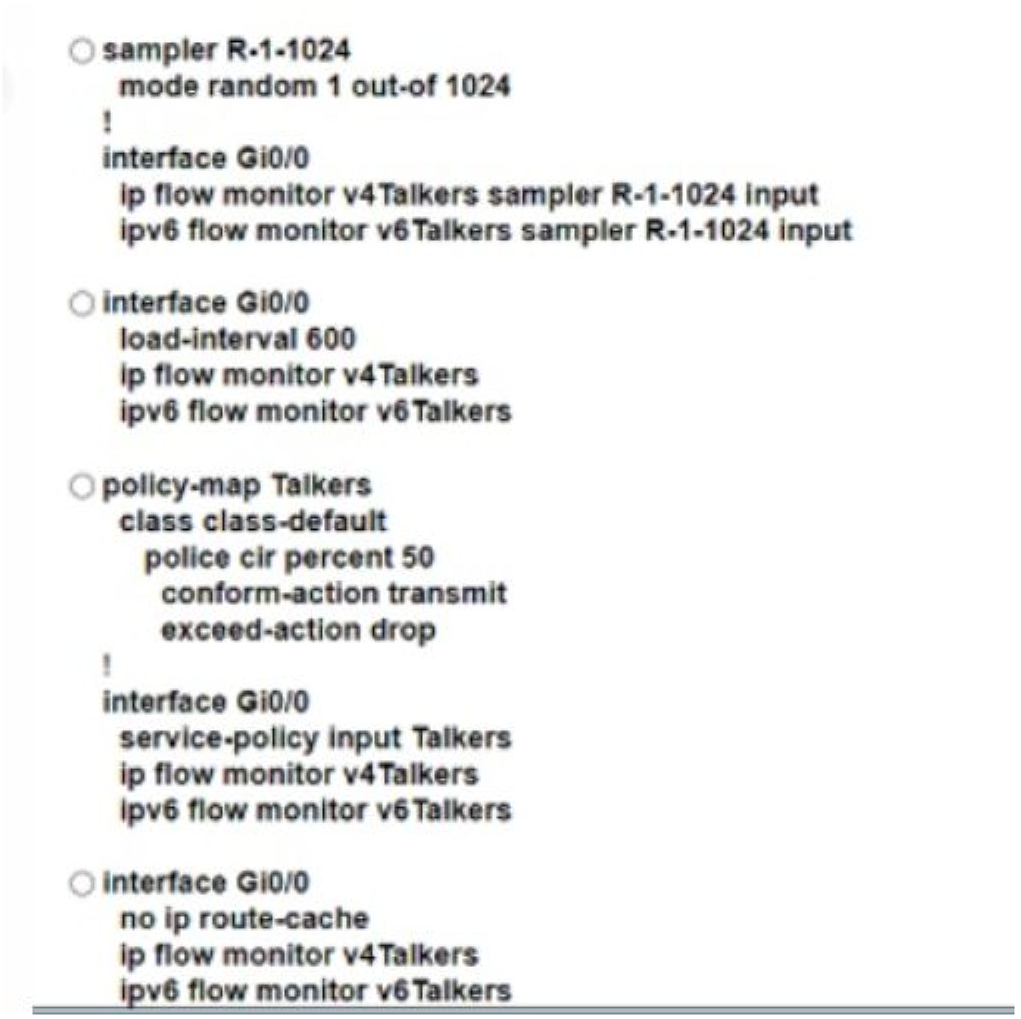
B. IP address
C. processor
D. secure access

Correct Answer: C
Section:

QUESTION 424
Refer to the exhibit.



```
flow record v4Talkers
 match ipv4 source address
 match ipv4 destination address
 collect counter bytes long
!
flow record v6Talkers
 match ipv6 source address
 match ipv6 destination address
 collect counter bytes long
!
flow monitor v4Talkers
 record v4Talkers
!
flow monitor v6Talkers
 record v6Talkers
```



```
○ sampler R-1-1024
    mode random 1 out-of 1024
  !
  interface Gi0/0
    ip flow monitor v4Talkers sampler R-1-1024 input
    ipv6 flow monitor v6Talkers sampler R-1-1024 input

○ interface Gi0/0
    load-interval 600
    ip flow monitor v4Talkers
    ipv6 flow monitor v6Talkers

○ policy-map Talkers
    class class-default
      police cir percent 50
        conform-action transmit
        exceed-action drop
  !
  interface Gi0/0
    service-policy input Talkers
    ip flow monitor v4Talkers
    ipv6 flow monitor v6Talkers

○ interface Gi0/0
    no ip route-cache
    ip flow monitor v4Talkers
    ipv6 flow monitor v6Talkers
```

A. Option A

B. Option B

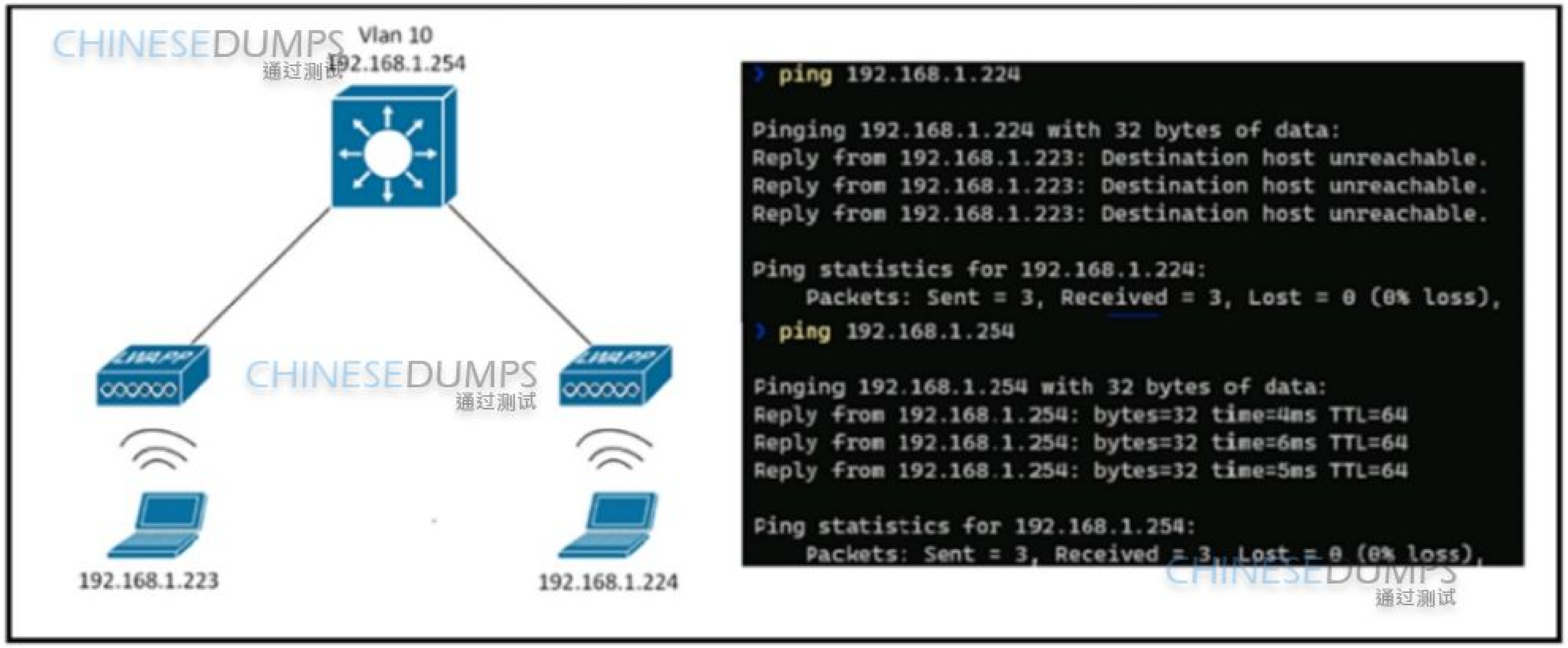
C. Option C

D. Option D

Correct Answer: A
Section:

QUESTION 425

Refer to the Exhibit.



```
> ping 192.168.1.224

Pinging 192.168.1.224 with 32 bytes of data:
Reply from 192.168.1.223: Destination host unreachable.
Reply from 192.168.1.223: Destination host unreachable.
Reply from 192.168.1.223: Destination host unreachable.

Ping statistics for 192.168.1.224:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
> ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time=4ms TTL=64
Reply from 192.168.1.254: bytes=32 time=6ms TTL=64
Reply from 192.168.1.254: bytes=32 time=5ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
```

Refer to the exhibit. An SSID is configured and both clients can reach their gateways on the Layer 3 switch, but they cannot communicate with each other. Which action resolves this issue?

A. Set the P2P Blocking Action to Forward-UpStream.
B. Set the WMM Policy to Allowed.
C. Set the P2P Blocking Action to Disabled.
D. Set the WMM Policy to Required

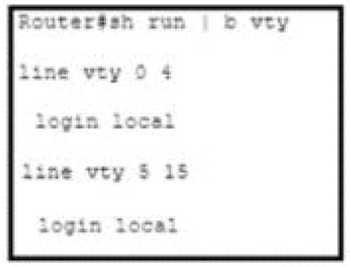
Correct Answer: C
Section:

QUESTION 426
A customer requires their wireless data traffic to egress at the switch port of the access point. Which access point mode supports this?

A. Bridge
B. Sniffer
C. FlexConnect
D. Monitor

Correct Answer: C
Section:

QUESTION 427
Refer to the Exhibit.



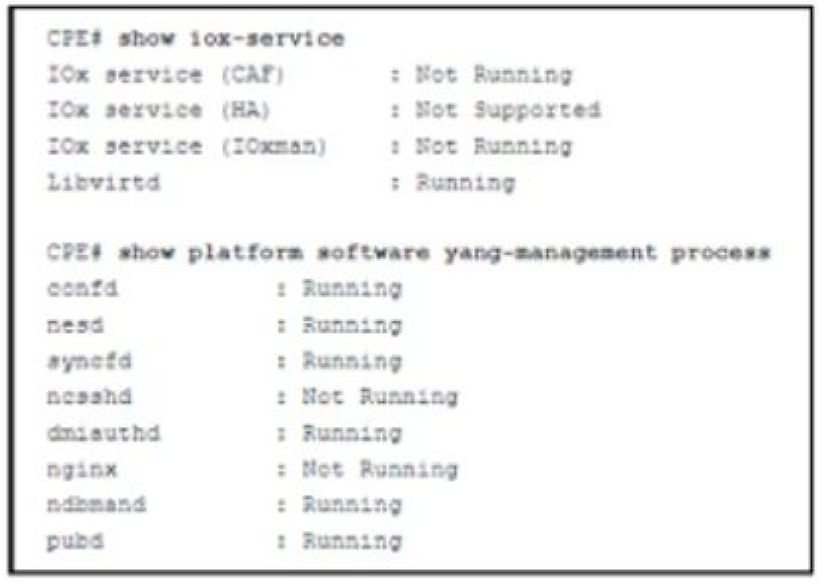
```
Router#sh run | b vty
line vty 0 4
 login local
line vty 5 15
 login local
```

Refer to the exhibit. The existing configuration must be updated to terminate EXEC sessions after 20 minutes of idle time. Which command set should be applied?

A. line vty 015 session-timeout 20
B. line vty 015 session-limit 20
C. line vty 015 exec-timeout 20
D. line vty 015 absolute-timeout 20

Correct Answer: C
Section:

QUESTION 428
Refer to the Exhibit.



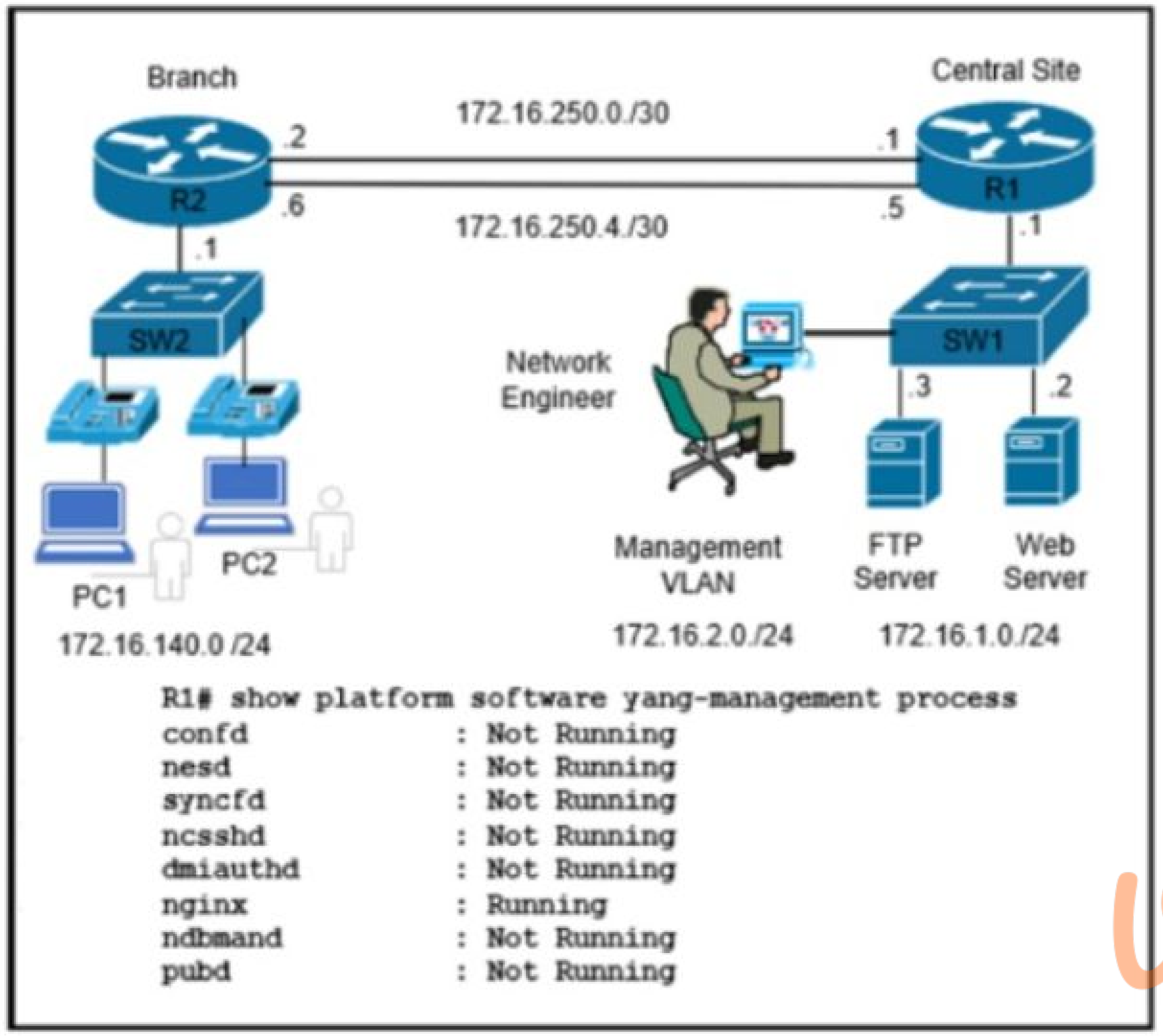
```
CPE# show iox-service
IOx service (CAF)         : Not Running
IOx service (HA)          : Not Supported
IOx service (IOxman)      : Not Running
Libvirtd                  : Running

CPE# show platform software yang-management process
confd               : Running
nesd                : Running
syncfd              : Running
ncsshd              : Not Running
dmiauthd            : Running
nginx               : Not Running
ndbmand             : Running
pubd                : Running
```

Refer to the exhibit. Which action must be performed to allow RESTCONF access to the device?

A. Enable the HTTPS service
B. Enable the SSH service.
C. Enable the NETCONF service
D. Enable the IOX service.

Correct Answer: A
Section:

QUESTION 429
Refer to the Exhibit.



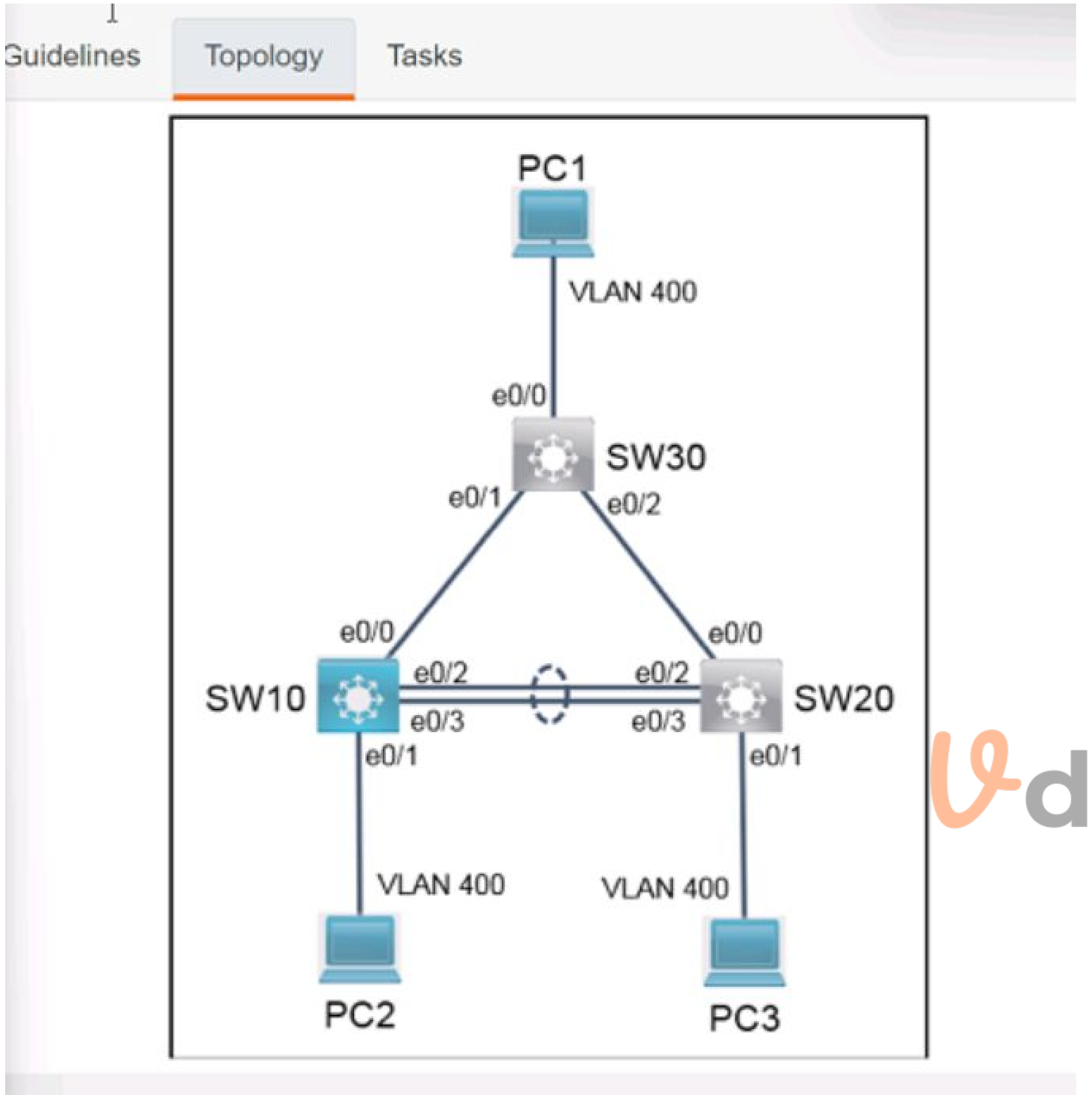
```
R1# show platform software yang-management process
confd                  : Not Running
nesd                   : Not Running
syncfd                 : Not Running
ncsshd                 : Not Running
dmiauthd               : Not Running
nginx                  : Running
ndbmand                : Not Running
pubd                   : Not Running
```

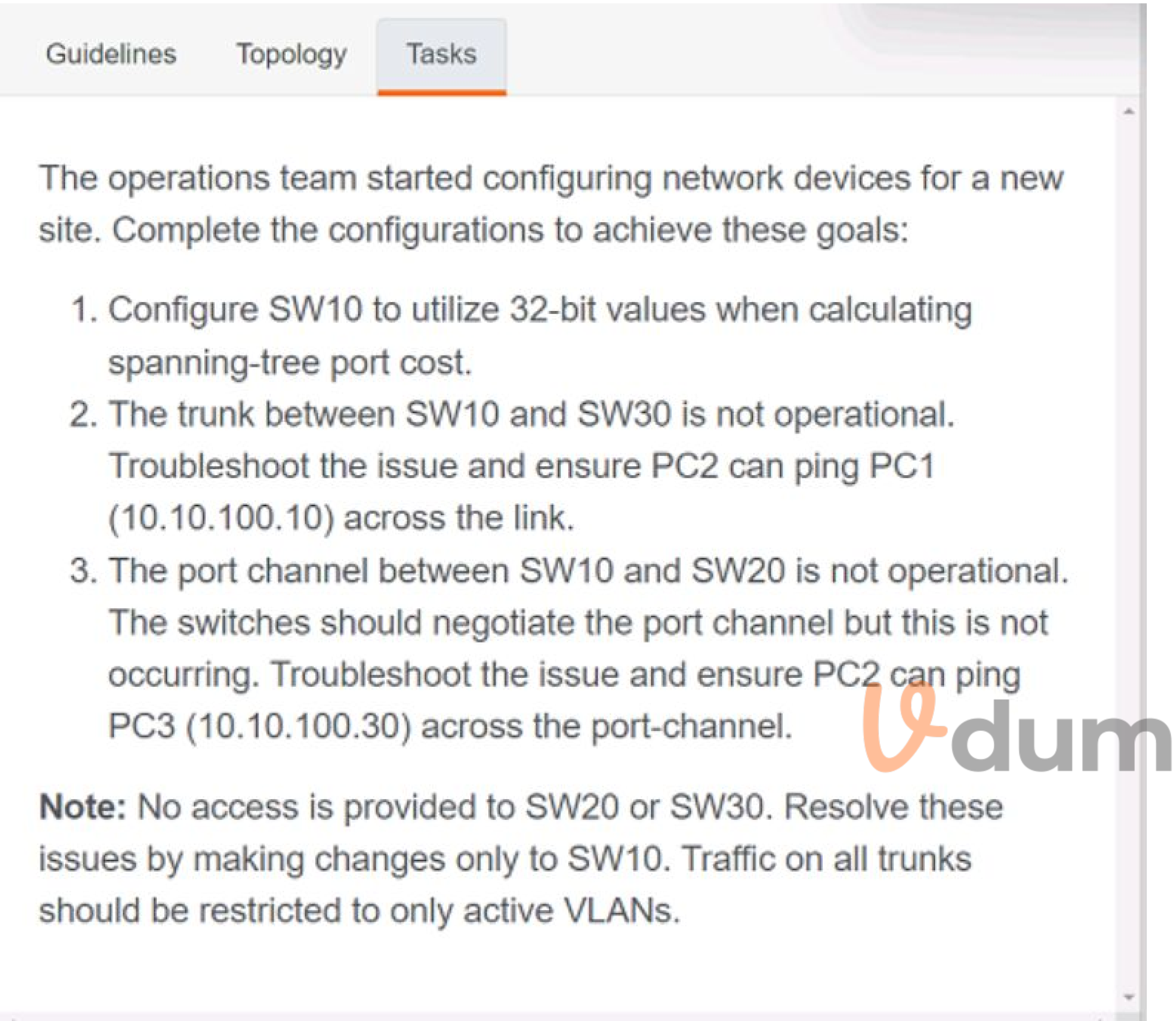
Refer to the exhibit. Which command is required on router R1 to start receiving RESTCONF requests?

A. R1(config)# ip http access-class 12
B. R1(config)# restconf
C. R1(config)# ip http server
D. R1(config) # ip http accounting commands 12 default

Correct Answer: B
Section:
Explanation:
Topic 6,
SIMULATIONS

QUESTION 430
SIMULATION

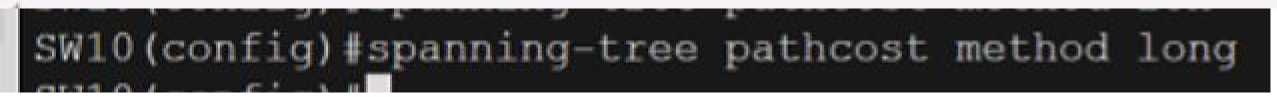

Guidelines
Topology
Tasks
PC1
VLAN 400
e0/0
SW30
e0/1
e0/2
e0/0
e0/0
SW10
e0/2
e0/3
e0/2
e0/3
SW20
e0/1
e0/1
VLAN 400
VLAN 400
PC2
PC3



The operations team started configuring network devices for a new site. Complete the configurations to achieve these goals:

1. Configure SW10 to utilize 32-bit values when calculating spanning-tree port cost.
2. The trunk between SW10 and SW30 is not operational. Troubleshoot the issue and ensure PC2 can ping PC1 (10.10.100.10) across the link.
3. The port channel between SW10 and SW20 is not operational. The switches should negotiate the port channel but this is not occurring. Troubleshoot the issue and ensure PC2 can ping PC3 (10.10.100.30) across the port-channel.

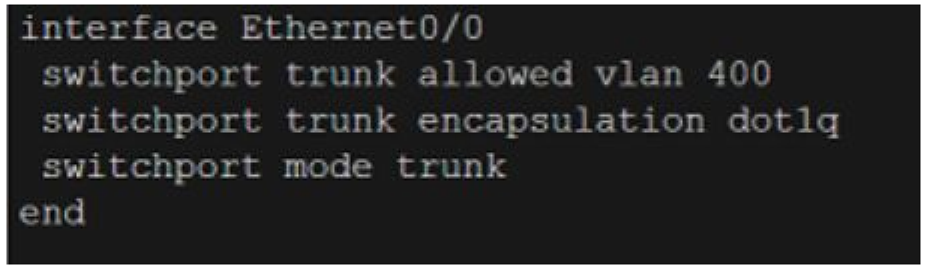
Note: No access is provided to SW20 or SW30. Resolve these issues by making changes only to SW10. Traffic on all trunks should be restricted to only active VLANs.



```
SW10(config)#spanning-tree pathcost method long
```

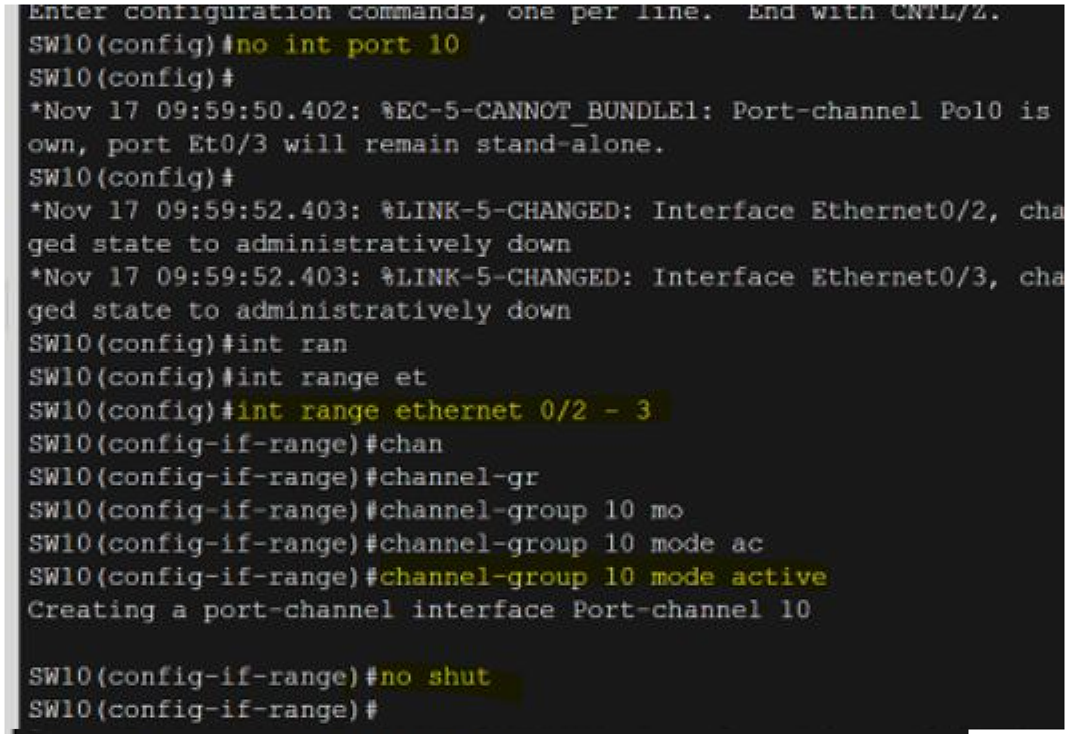
A. See the solution below in Explanation

Correct Answer: A
Section:
Explanation:
Solution:
SW10
Conf t
Default int e0/0
Int e0/0
No sh

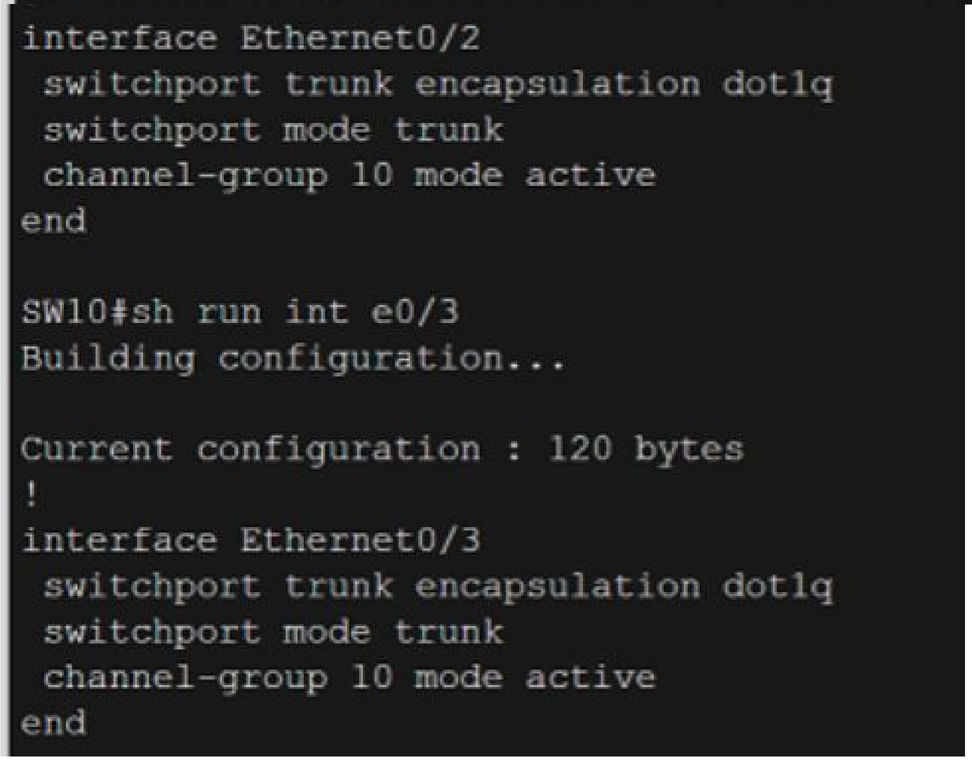


```
interface Ethernet0/0
 switchport trunk allowed vlan 400
 switchport trunk encapsulation dot1q
 switchport mode trunk
end
```

Conf t



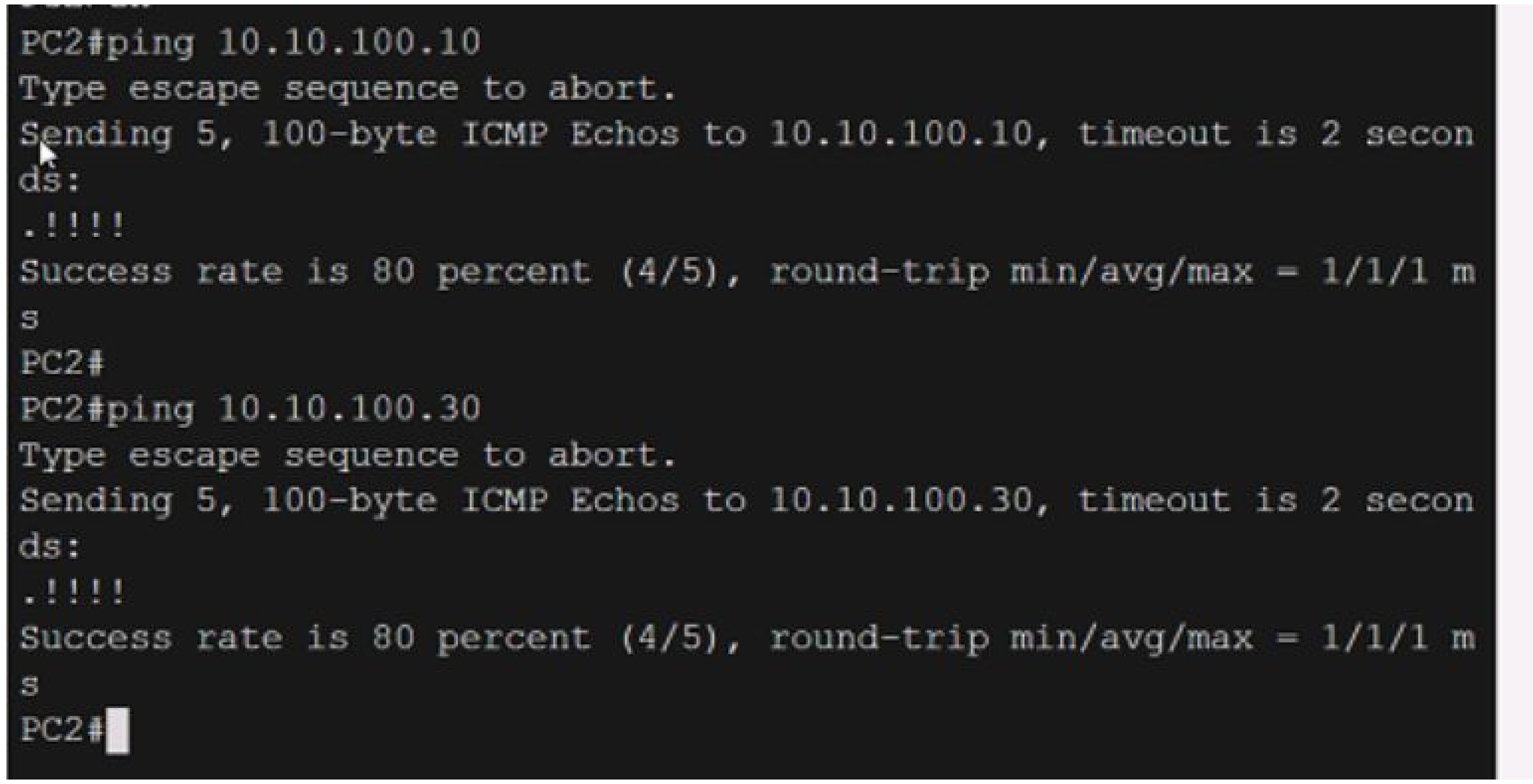
```
Enter configuration commands, one per line.  End with CNTL/Z.
SW10(config)#no int port 10
SW10(config)#
*Nov 17 09:59:50.402: %EC-5-CANNOT_BUNDLE1: Port-channel Po10 is
own, port Et0/3 will remain stand-alone.
SW10(config)#
*Nov 17 09:59:52.403: %LINK-5-CHANGED: Interface Ethernet0/2, cha
ged state to administratively down
*Nov 17 09:59:52.403: %LINK-5-CHANGED: Interface Ethernet0/3, cha
ged state to administratively down
SW10(config)#int ran
SW10(config)#int range et
SW10(config)#int range ethernet 0/2 - 3
SW10(config-if-range)#chan
SW10(config-if-range)#channel-gr
SW10(config-if-range)#channel-group 10 mo
SW10(config-if-range)#channel-group 10 mode ac
SW10(config-if-range)#channel-group 10 mode active
Creating a port-channel interface Port-channel 10

SW10(config-if-range)#no shut
SW10(config-if-range)#
```



```
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 10 mode active
end

SW10#sh run int e0/3
Building configuration...

Current configuration : 120 bytes
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 10 mode active
end
```

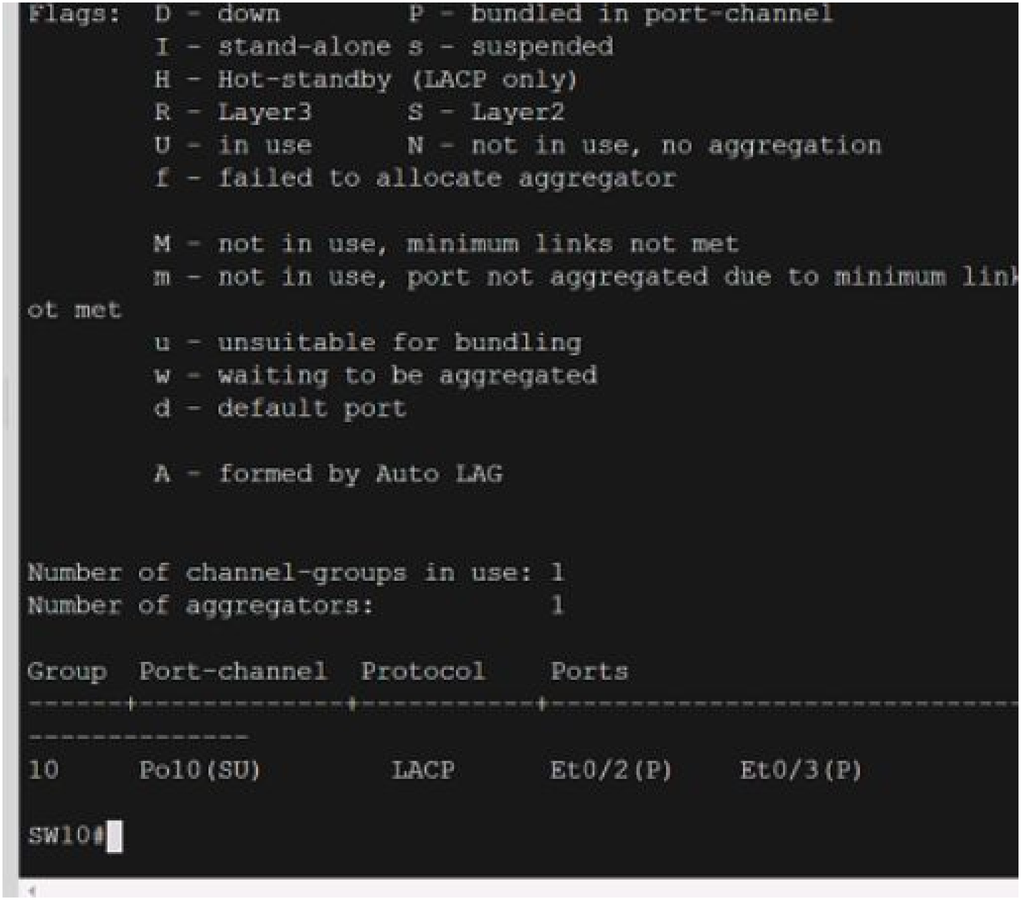
Copy run start

Verification from PC2



```
PC2#ping 10.10.100.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.100.10, timeout is 2 secon
ds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 m
s
PC2#
PC2#ping 10.10.100.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.100.30, timeout is 2 secon
ds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 m
s
PC2#
```

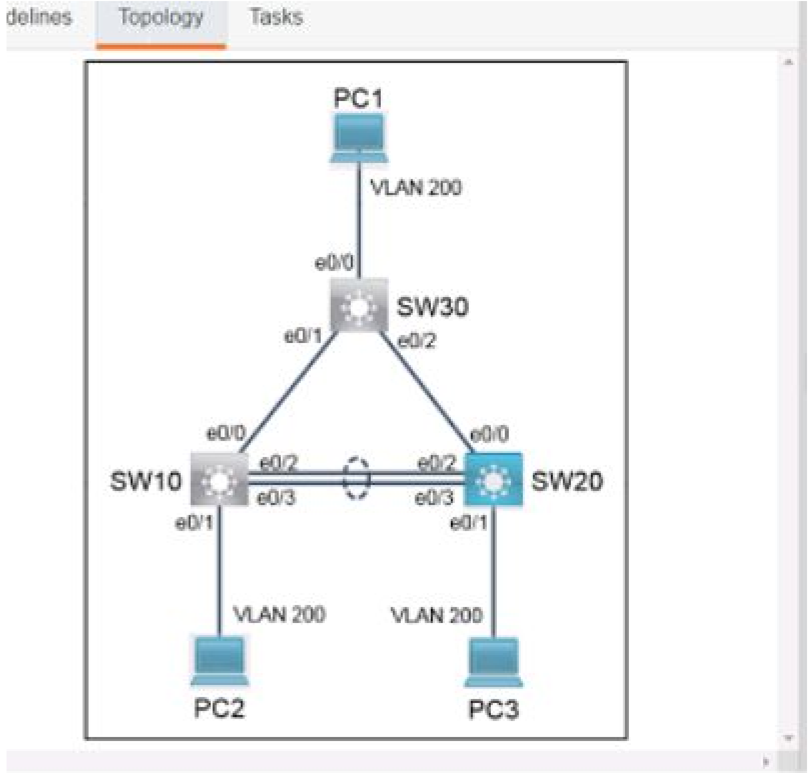
Show etherchannel summary

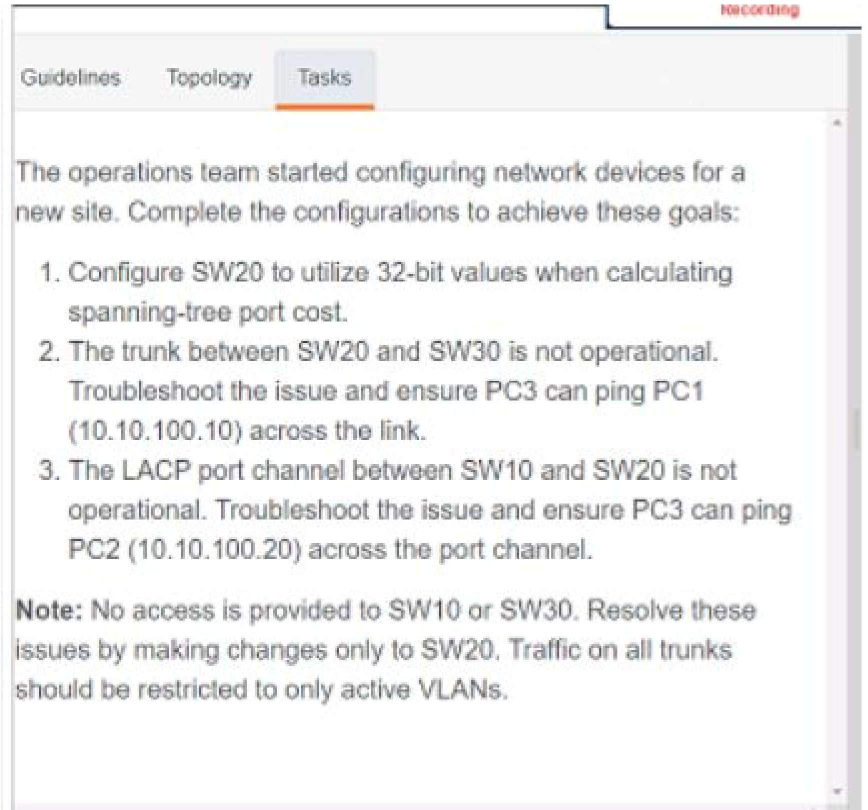


```
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum lin
ot met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------------------------
--------------
10     Po10(SU)        LACP      Et0/2(P)     Et0/3(P)

SW10#
```

QUESTION 431

SIMULATION





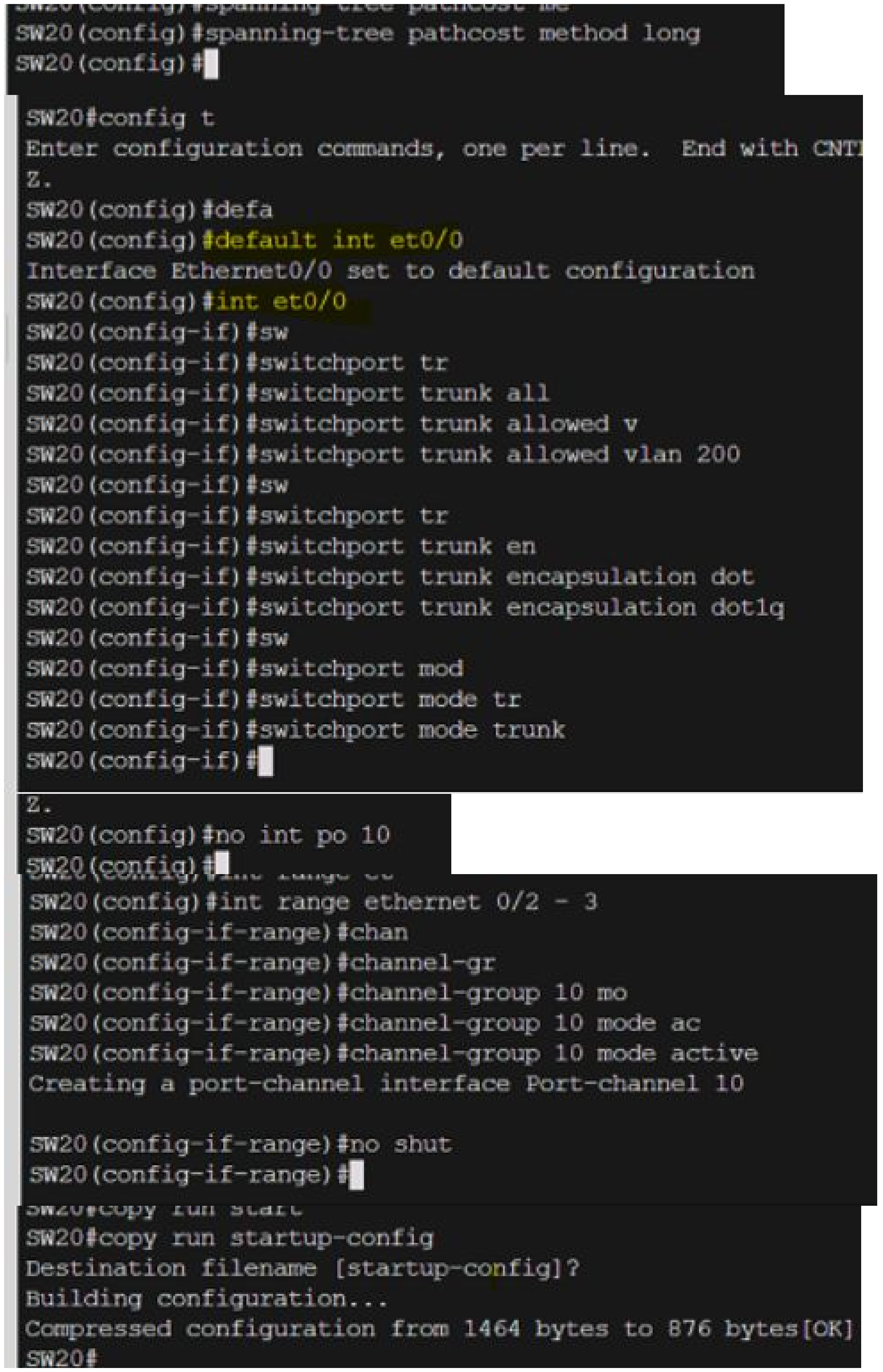
The operations team started configuring network devices for a new site. Complete the configurations to achieve these goals:

1. Configure SW20 to utilize 32-bit values when calculating spanning-tree port cost.
2. The trunk between SW20 and SW30 is not operational. Troubleshoot the issue and ensure PC3 can ping PC1 (10.10.100.10) across the link.
3. The LACP port channel between SW10 and SW20 is not operational. Troubleshoot the issue and ensure PC3 can ping PC2 (10.10.100.20) across the port channel.

Note: No access is provided to SW10 or SW30. Resolve these issues by making changes only to SW20. Traffic on all trunks should be restricted to only active VLANs.

A. See the solution below in Explanation

Correct Answer: A
Section:
Explanation:
SOLUTION: -



```
SW20(config)#spanning-tree pathcost me
SW20(config)#spanning-tree pathcost method long
SW20(config)#
```

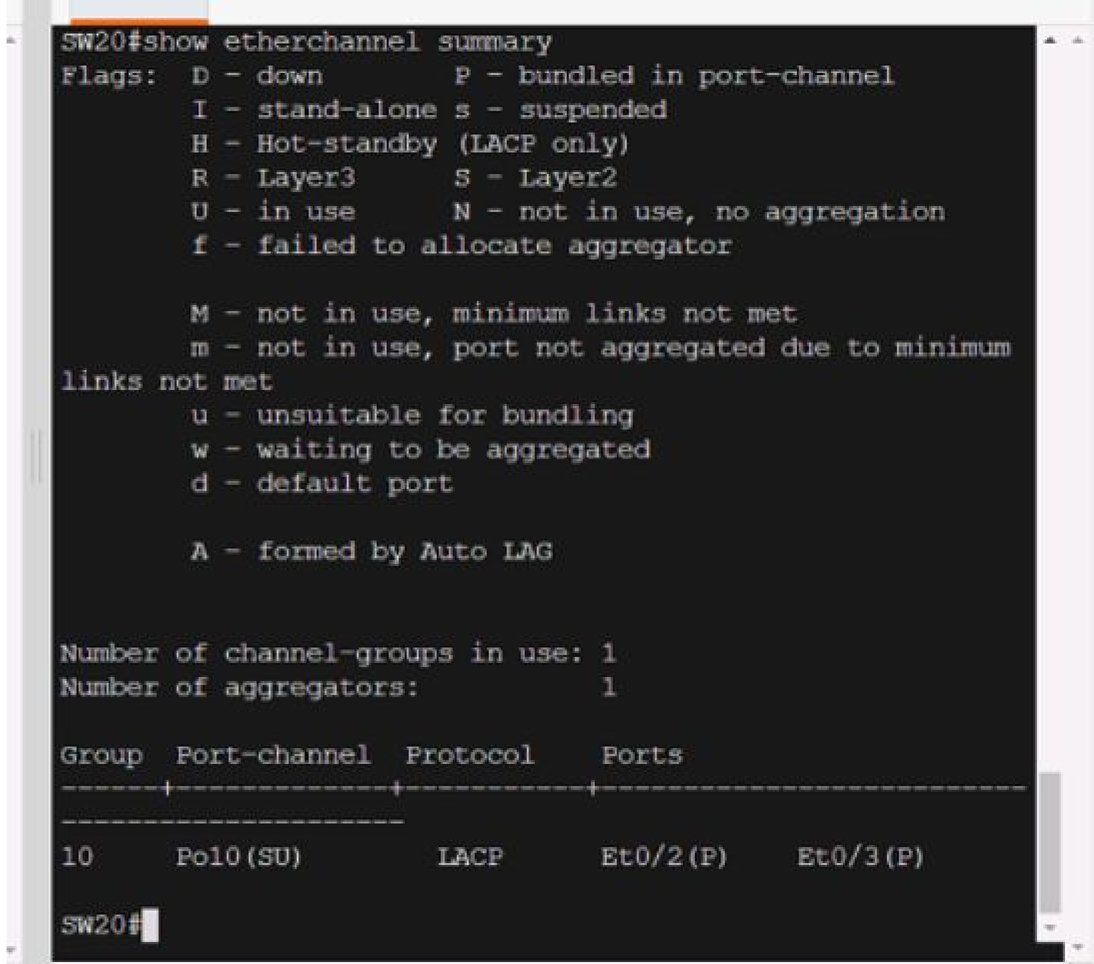
```
SW20#config t
Enter configuration commands, one per line.  End with CNTL/
Z.
SW20(config)#defa
SW20(config)#default int et0/0
Interface Ethernet0/0 set to default configuration
SW20(config)#int et0/0
SW20(config-if)#sw
SW20(config-if)#switchport tr
SW20(config-if)#switchport trunk all
SW20(config-if)#switchport trunk allowed v
SW20(config-if)#switchport trunk allowed vlan 200
SW20(config-if)#sw
SW20(config-if)#switchport tr
SW20(config-if)#switchport trunk en
SW20(config-if)#switchport trunk encapsulation dot
SW20(config-if)#switchport trunk encapsulation dot1q
SW20(config-if)#sw
SW20(config-if)#switchport mod
SW20(config-if)#switchport mode tr
SW20(config-if)#switchport mode trunk
SW20(config-if)#
```

```
Z.
SW20(config)#no int po 10
SW20(config)#
```

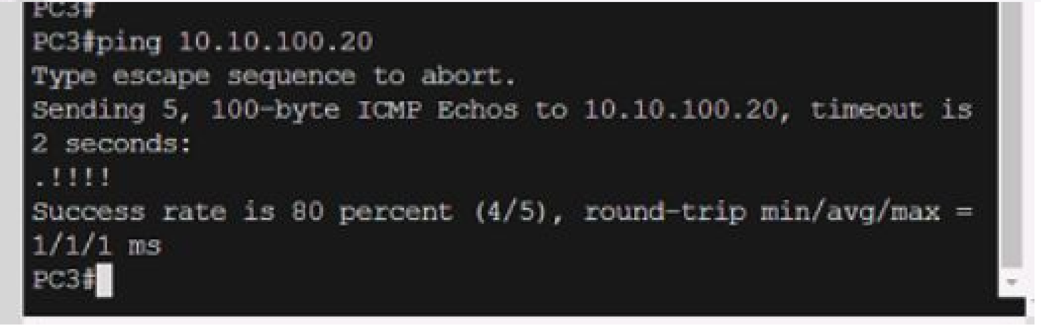
```
SW20(config)#int range et
SW20(config)#int range ethernet 0/2 - 3
SW20(config-if-range)#chan
SW20(config-if-range)#channel-gr
SW20(config-if-range)#channel-group 10 mo
SW20(config-if-range)#channel-group 10 mode ac
SW20(config-if-range)#channel-group 10 mode active
Creating a port-channel interface Port-channel 10

SW20(config-if-range)#no shut
SW20(config-if-range)#
```

```
SW20#copy run start
SW20#copy run startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 1464 bytes to 876 bytes[OK]
SW20#
```

VERIFICATION: -



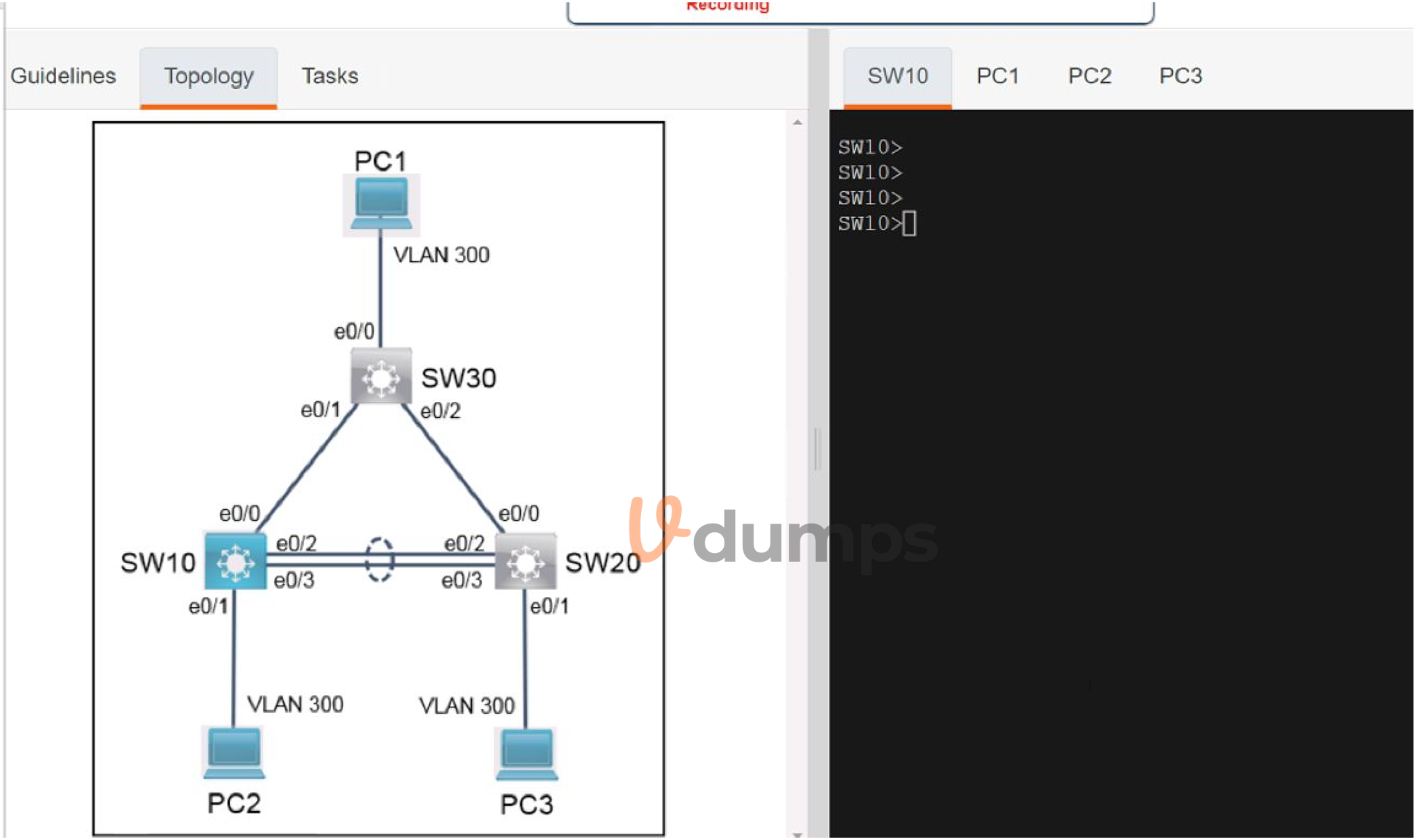
```
SW20#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum
links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+---------------------------
---------------------
10     Po10(SU)         LACP      Et0/2(P)    Et0/3(P)

SW20#
```



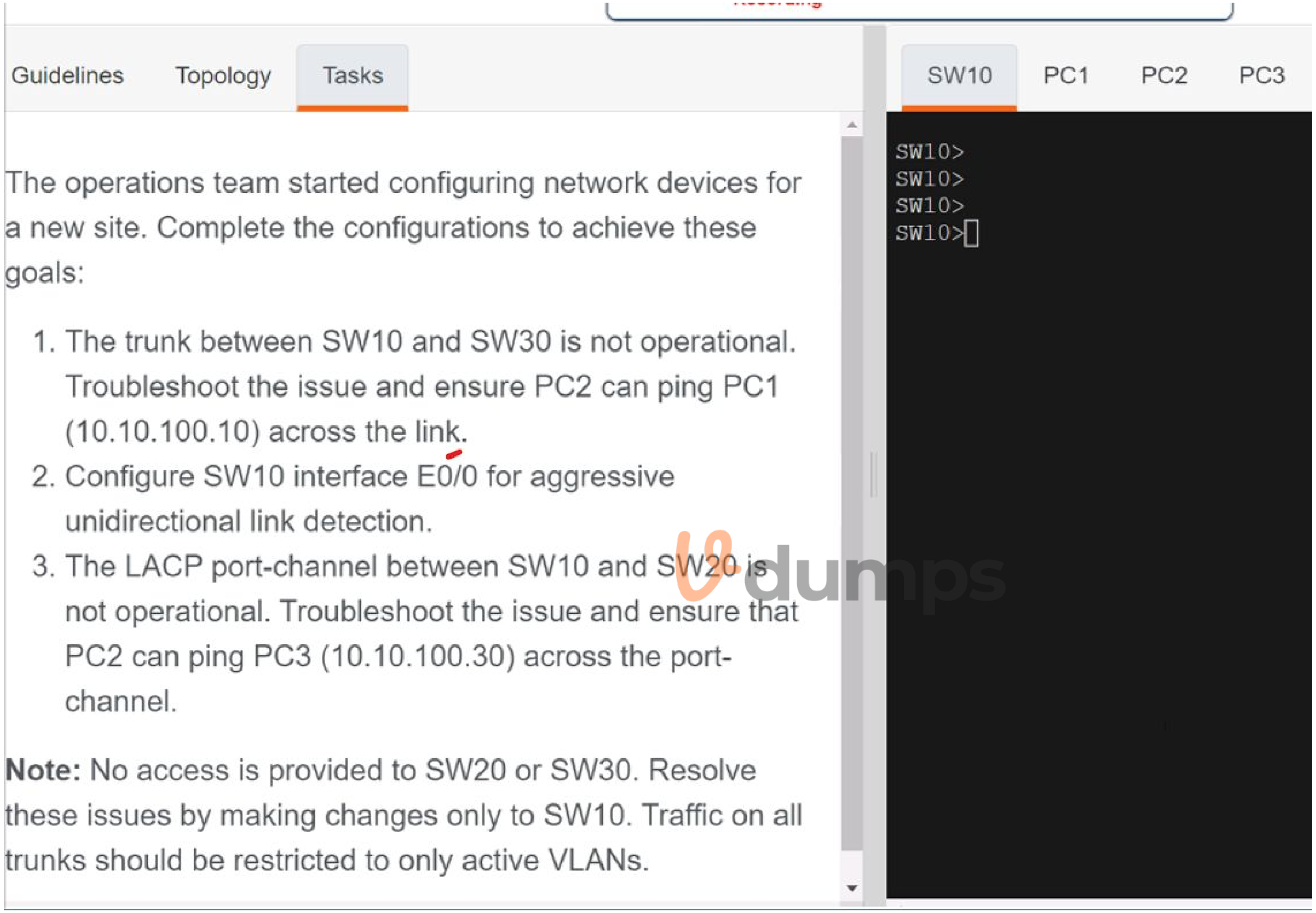
```
PC3#
PC3#ping 10.10.100.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.100.20, timeout is
2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max =
1/1/1 ms
PC3#
```

QUESTION 432

SIMULATION



```
SW10>
SW10>
SW10>
SW10>
```



The operations team started configuring network devices for a new site. Complete the configurations to achieve these goals:

1. The trunk between SW10 and SW30 is not operational. Troubleshoot the issue and ensure PC2 can ping PC1 (10.10.100.10) across the link.
2. Configure SW10 interface E0/0 for aggressive unidirectional link detection.
3. The LACP port-channel between SW10 and SW20 is not operational. Troubleshoot the issue and ensure that PC2 can ping PC3 (10.10.100.30) across the port-channel.

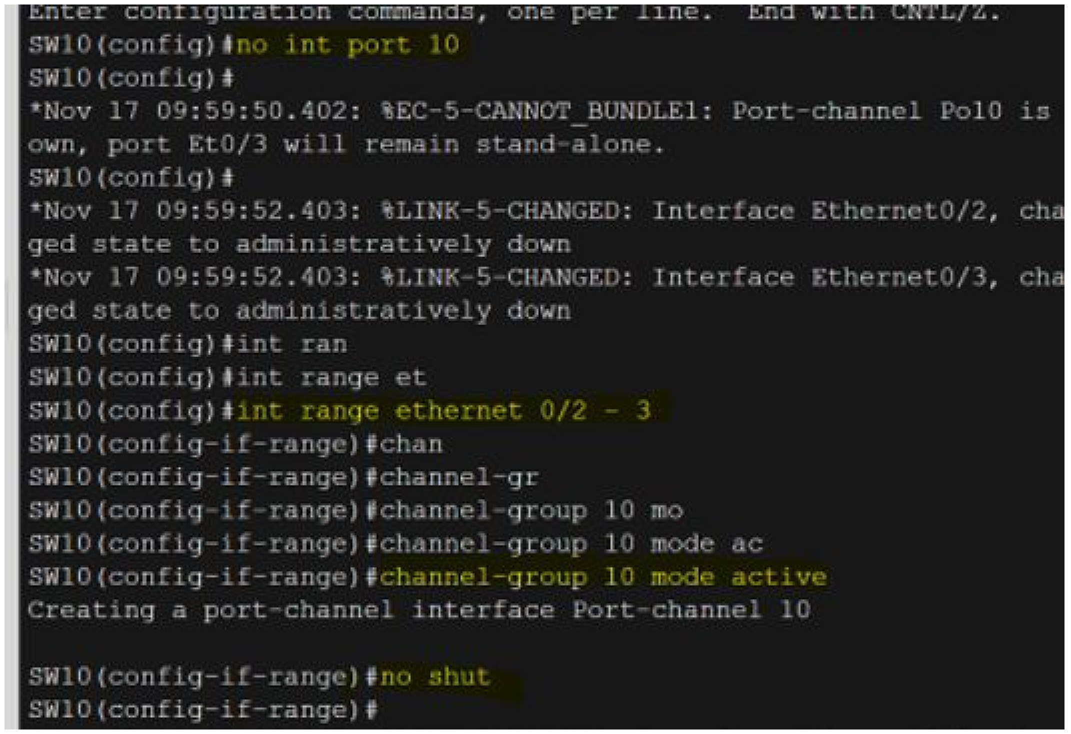
Note: No access is provided to SW20 or SW30. Resolve these issues by making changes only to SW10. Traffic on all trunks should be restricted to only active VLANs.

```
SW10>
SW10>
SW10>
SW10>
```

A. See the solution below in Explanation

Correct Answer: A
Section:
Explanation:
Conf t
Default int e0/0
Int e0/0
No sh

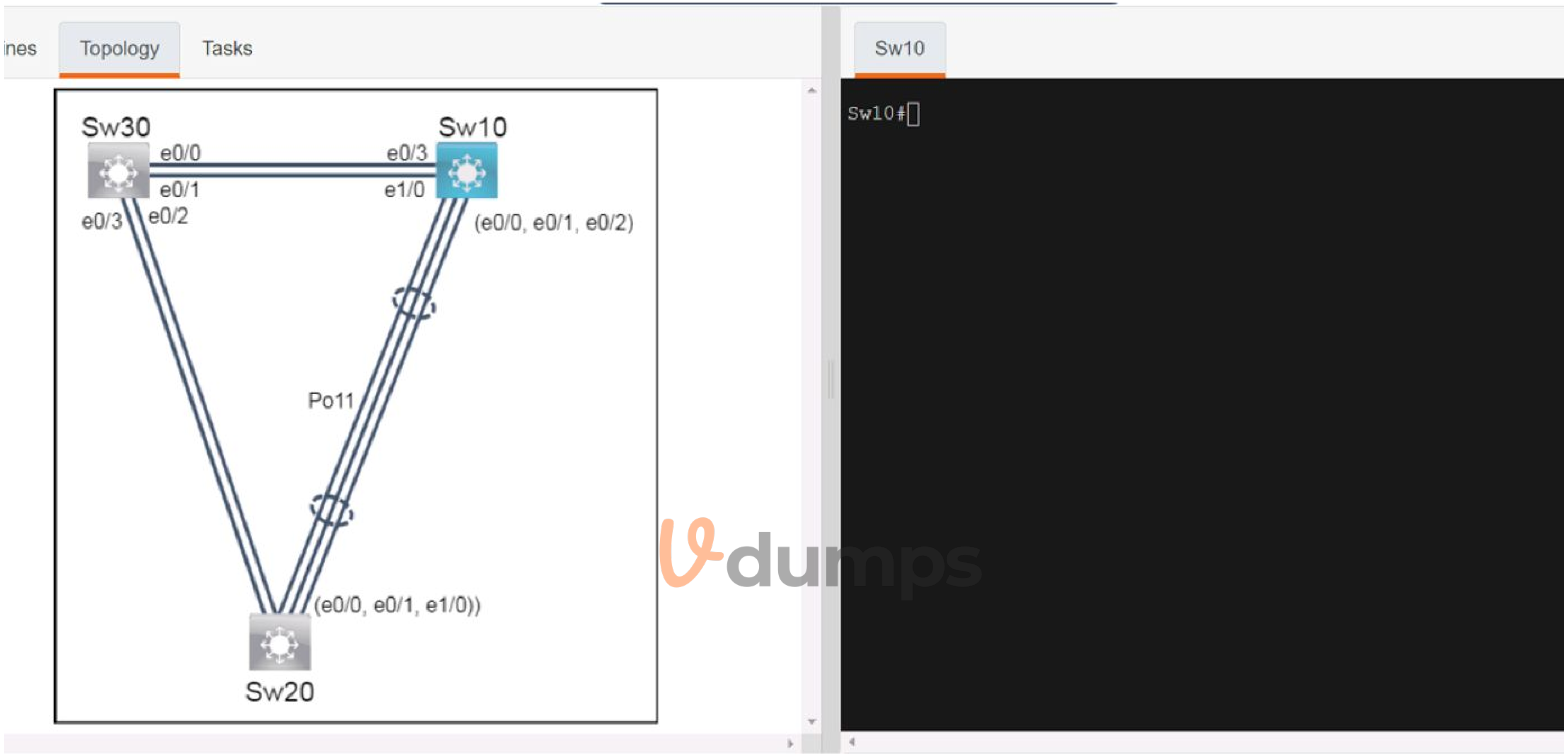
Switchport trunk encap dot1q
Switchport mode trunk
Udld port aggressive
Switchport trunk allowed vlan add 300
No sh
Ex



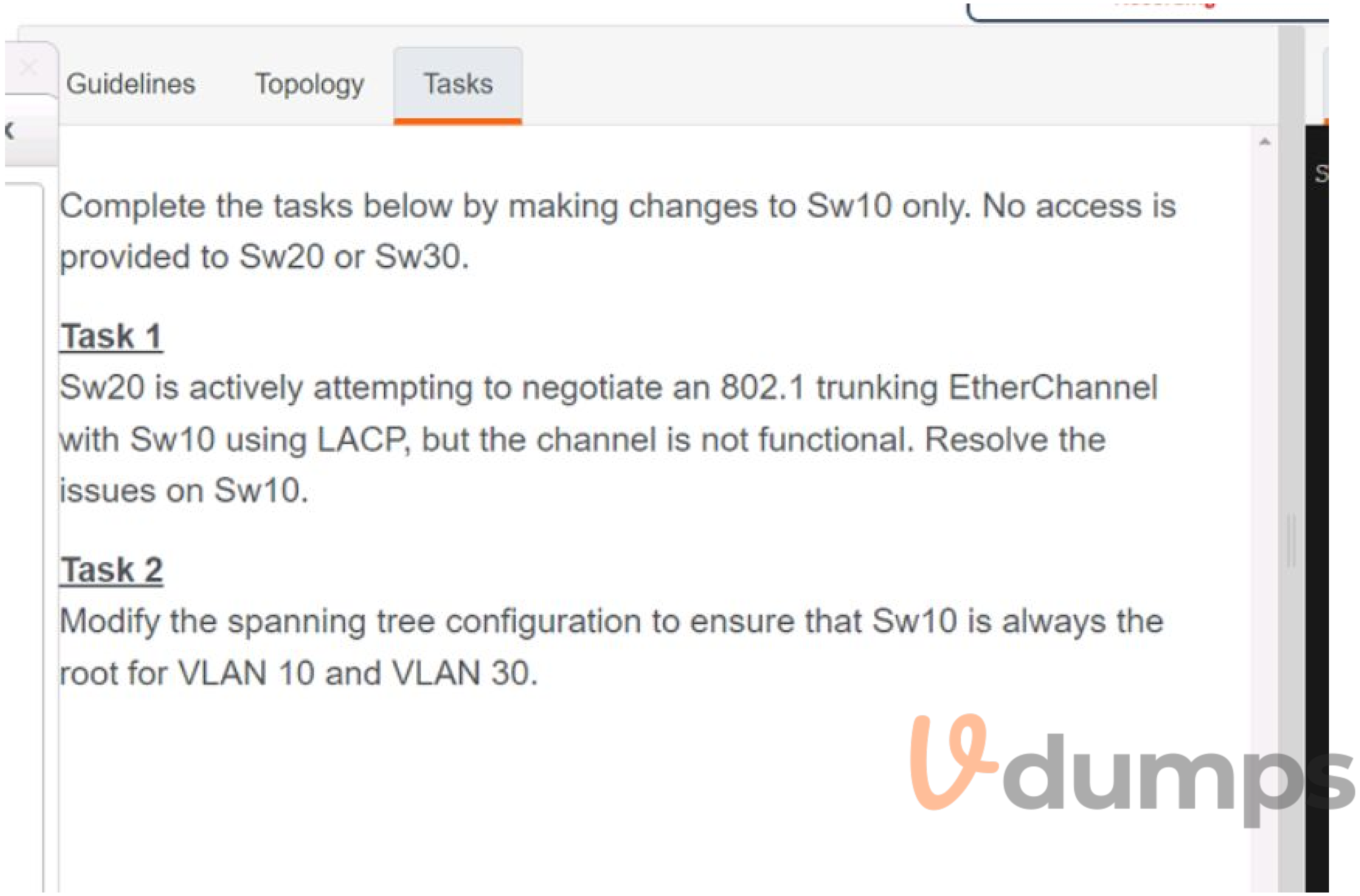
```
Enter configuration commands, one per line.  End with CNTL/Z.
SW10(config)#no int port 10
SW10(config)#
*Nov 17 09:59:50.402: %EC-5-CANNOT_BUNDLE1: Port-channel Po10 is
own, port Et0/3 will remain stand-alone.
SW10(config)#
*Nov 17 09:59:52.403: %LINK-5-CHANGED: Interface Ethernet0/2, cha
ged state to administratively down
*Nov 17 09:59:52.403: %LINK-5-CHANGED: Interface Ethernet0/3, cha
ged state to administratively down
SW10(config)#int ran
SW10(config)#int range et
SW10(config)#int range ethernet 0/2 - 3
SW10(config-if-range)#chan
SW10(config-if-range)#channel-gr
SW10(config-if-range)#channel-group 10 mo
SW10(config-if-range)#channel-group 10 mode ac
SW10(config-if-range)#channel-group 10 mode active
Creating a port-channel interface Port-channel 10

SW10(config-if-range)#no shut
SW10(config-if-range)#
```

OR

QUESTION 433
SIMULATION


ines
Topology
Tasks
Sw30
Sw10
e0/0
e0/3
e0/1
e1/0
e0/3
e0/2
(e0/0, e0/1, e0/2)
Po11
(e0/0, e0/1, e1/0))
Sw20
Sw10

```
Sw10#
```



Complete the tasks below by making changes to Sw10 only. No access is provided to Sw20 or Sw30.

Task 1

Sw20 is actively attempting to negotiate an 802.1 trunking EtherChannel with Sw10 using LACP, but the channel is not functional. Resolve the issues on Sw10.

Task 2

Modify the spanning tree configuration to ensure that Sw10 is always the root for VLAN 10 and VLAN 30.

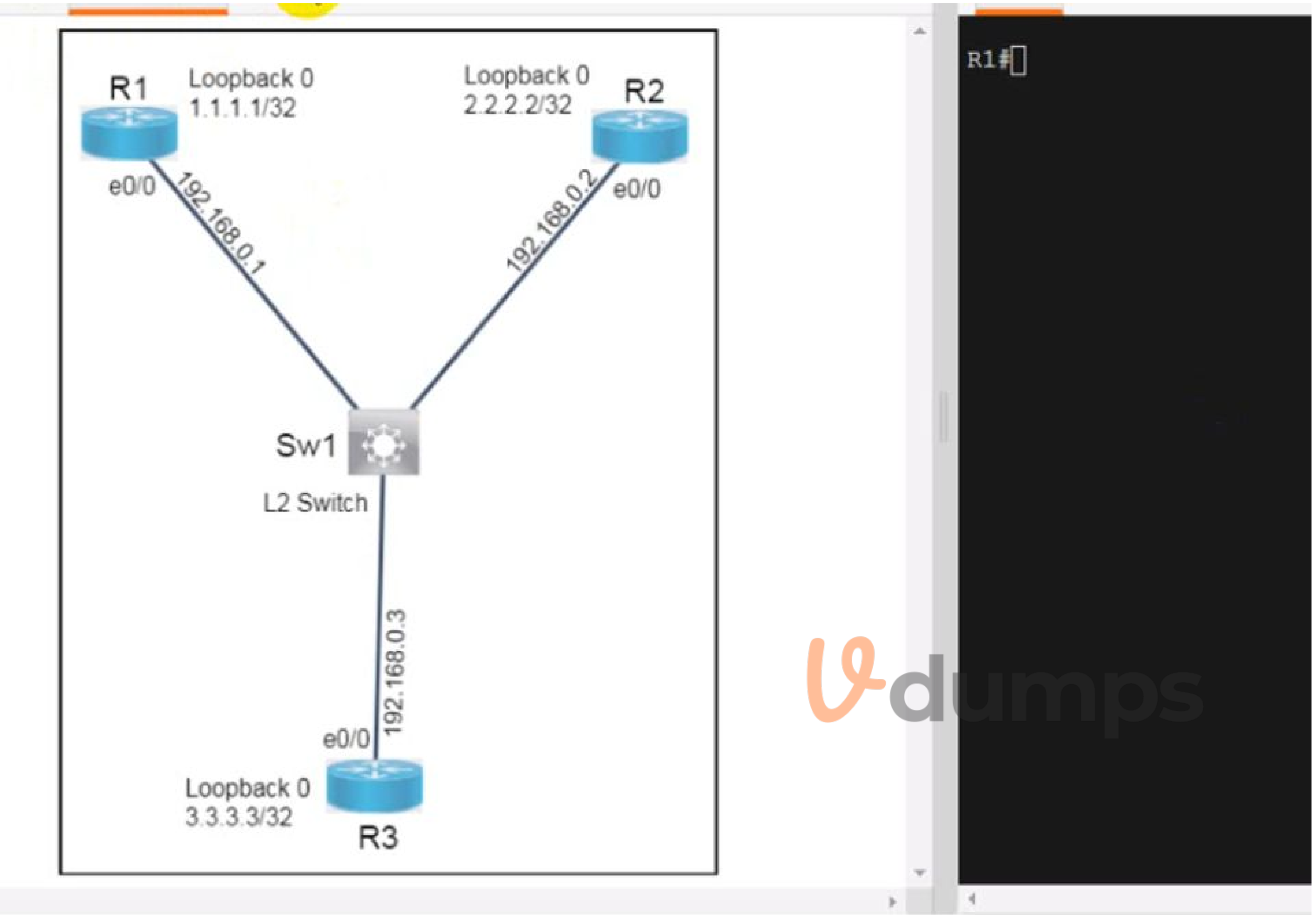
A. See the solution below in Explanation

Correct Answer: A
Section:
Explanation:

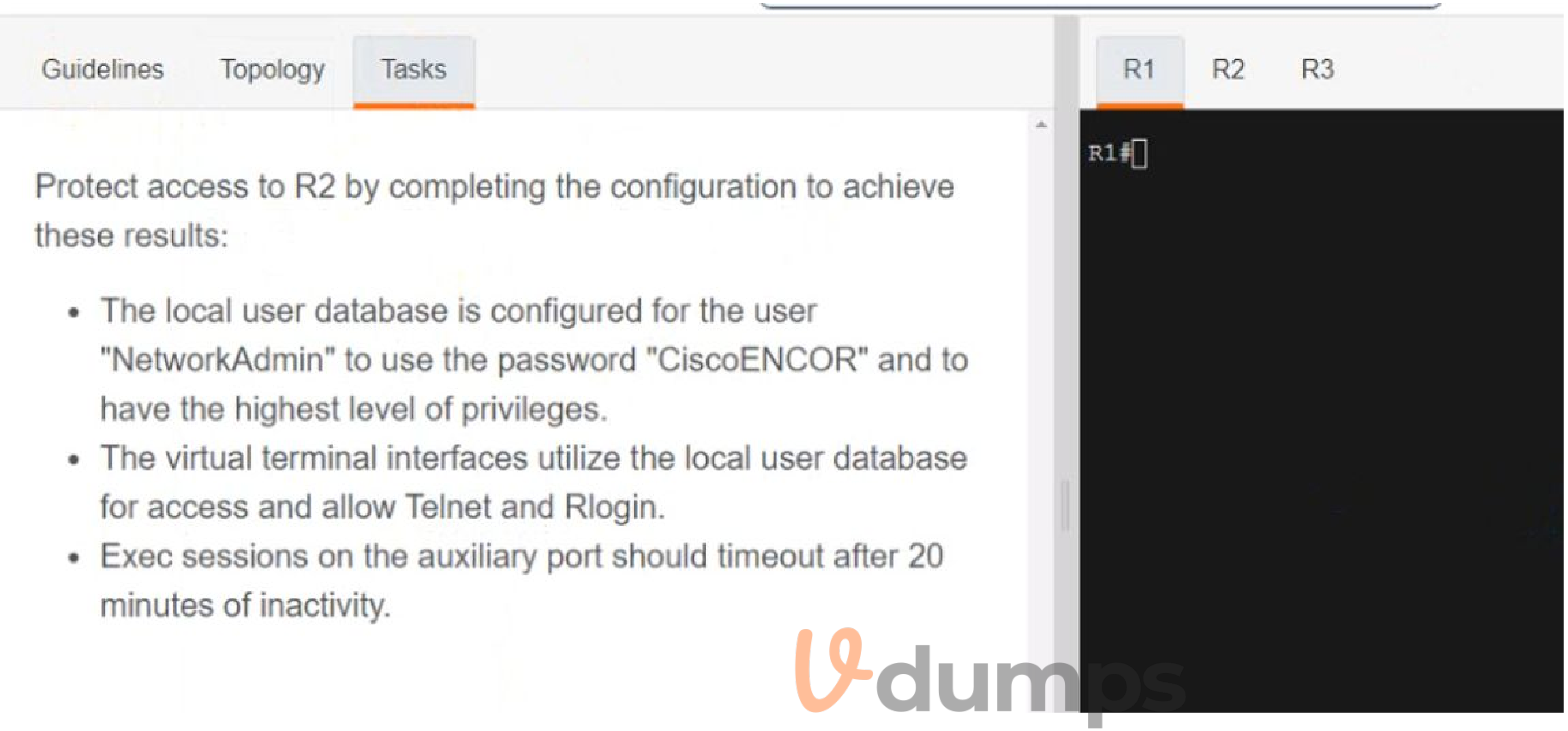
Solution:-
Default int range et0/0-1
Int range e0/0 -- 1
Sw trunk encap dot1
Switch mode trunk
Channel-group 2 mode passive
No shut
Spanning-tree vlan 10 priority 0
Spanning-tree vlan 30 priority 0

QUESTION 434

SIMULATION


R1
Loopback 0
1.1.1.1/32
Loopback 0
2.2.2.2/32
R2
e0/0
192.168.0.1
192.168.0.2
e0/0
Sw1
L2 Switch
192.168.0.3
e0/0
Loopback 0
3.3.3.3/32
R3

```
R1#
```



Protect access to R2 by completing the configuration to achieve these results:

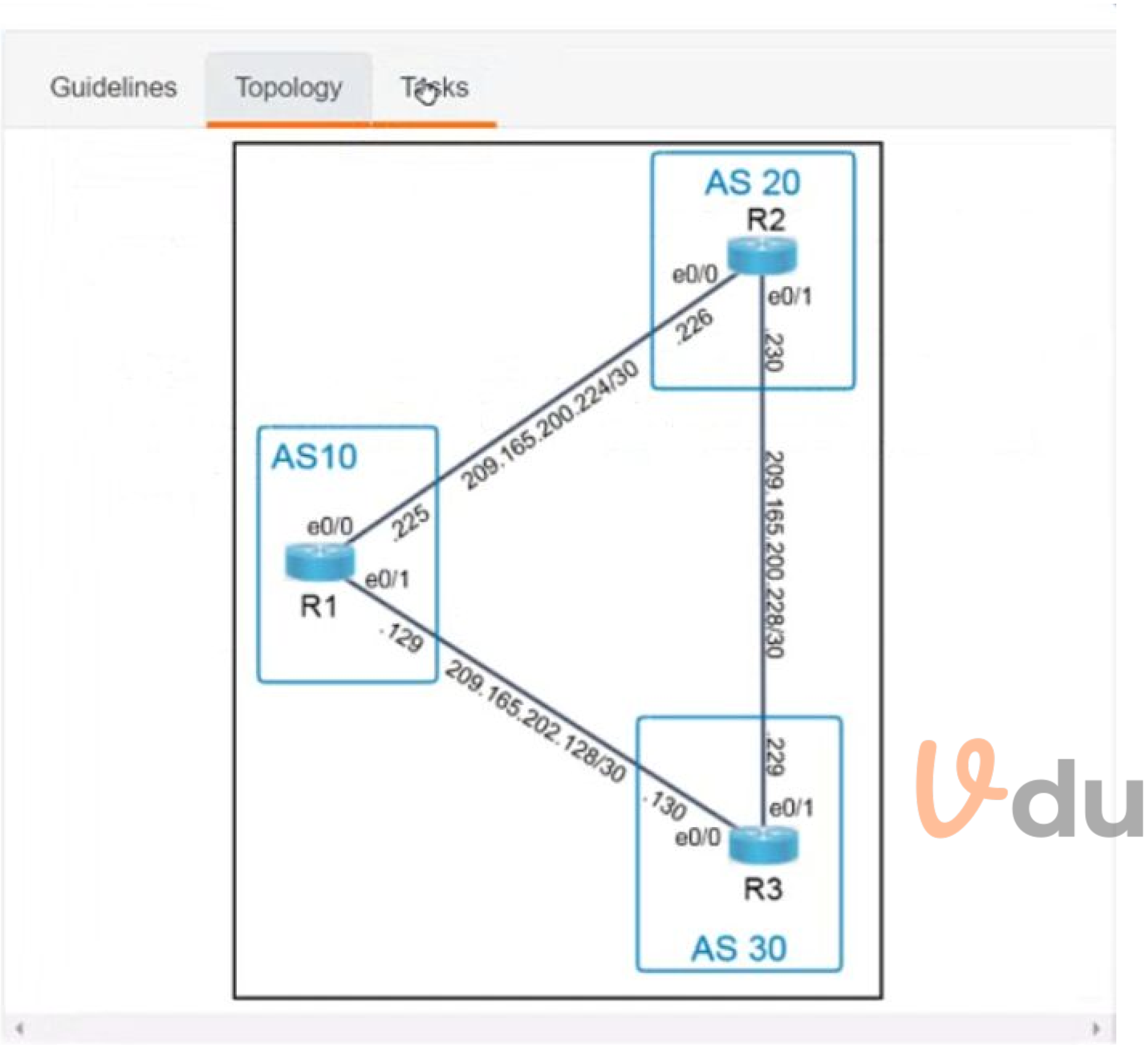
- The local user database is configured for the user "NetworkAdmin" to use the password "CiscoENCOR" and to have the highest level of privileges.
- The virtual terminal interfaces utilize the local user database for access and allow Telnet and Rlogin.
- Exec sessions on the auxiliary port should timeout after 20 minutes of inactivity.

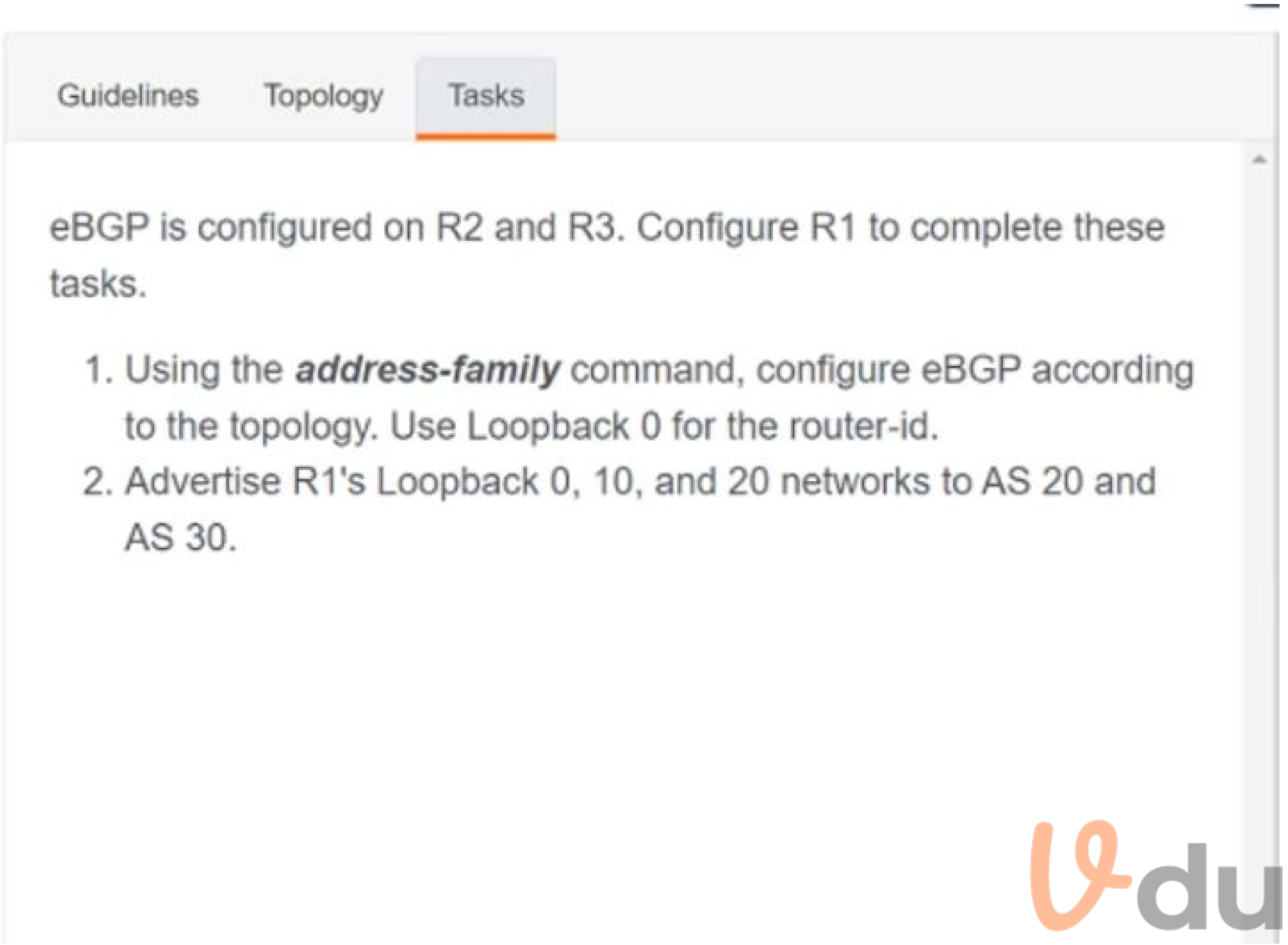
```
R1#
```

A. See the solution below in Explanation

Correct Answer: A
Section:
Explanation:

```
R2
config t
username NetworkAdmin privilege 15 password CiscoENCOR
line vty 0 4
login local
transport input telnet rlogin
exec-timeout 1200 0
```


Guidelines
Topology
Tasks
AS 20
R2
e0/0
e0/1
.226
.230
AS10
e0/0
.225
209.165.200.224/30
e0/1
R1
.129
209.165.200.228/30
209.165.202.128/30
.229
.130
e0/1
e0/0
R3
AS 30



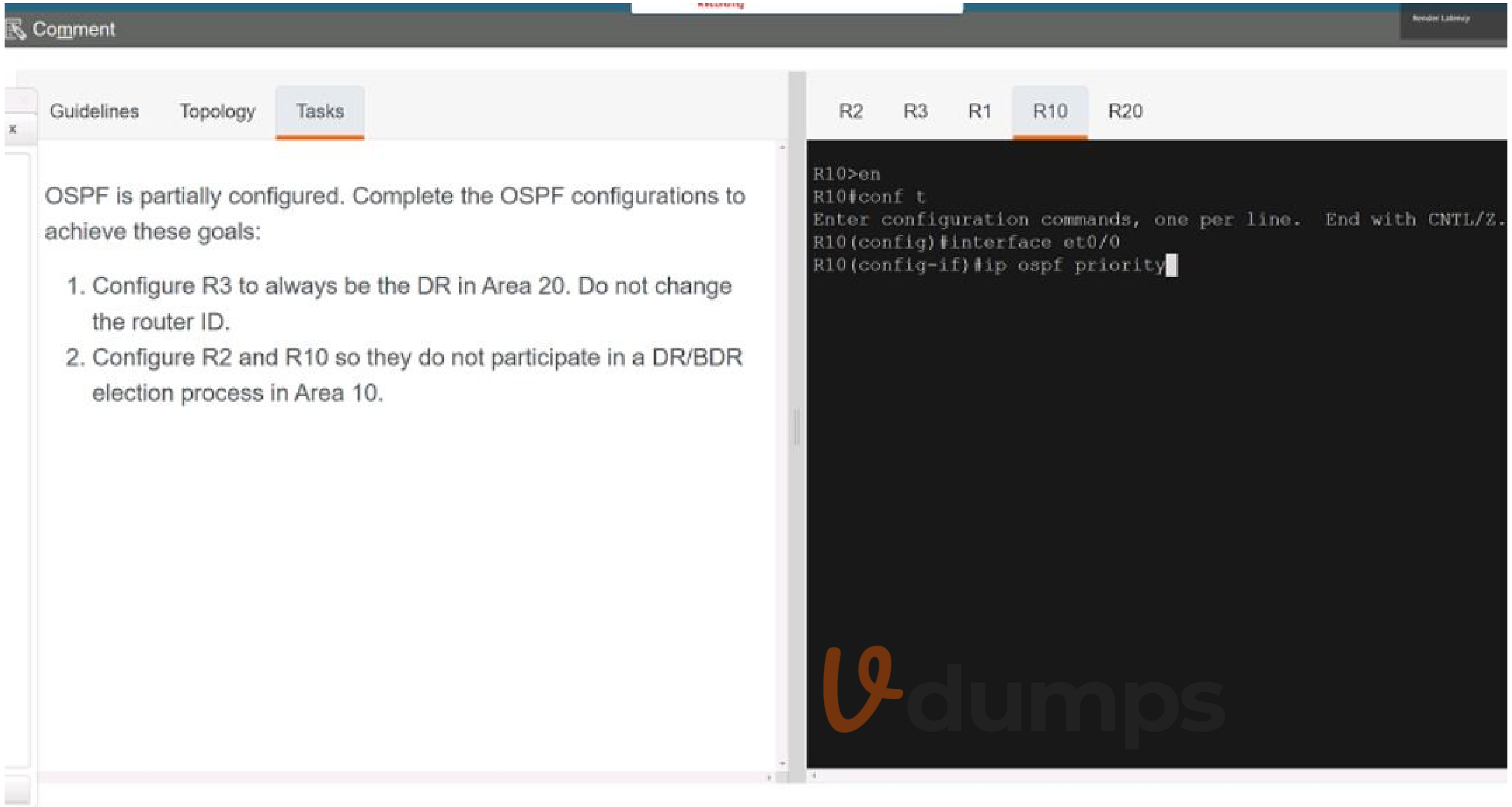
eBGP is configured on R2 and R3. Configure R1 to complete these tasks.

1. Using the ***address-family*** command, configure eBGP according to the topology. Use Loopback 0 for the router-id.
2. Advertise R1's Loopback 0, 10, and 20 networks to AS 20 and AS 30.

```
R1
router bgp 10
no bgp default ipv4-unicast
bgp router-id 10.1.1.111
neigh 209.165.200.226 remote-as 20
neigh 209.165.202.130 remote-as 30
address-family ipv4
network 10.1.1.10 mask 255.255.255.255
network 209.165.201.20 mask 255.255.255.255
network 209.165.201.10 mask 255.255.255.255
neigh 209.165.200.226 activate
neigh 209.165.202.130 activate
```

QUESTION 435

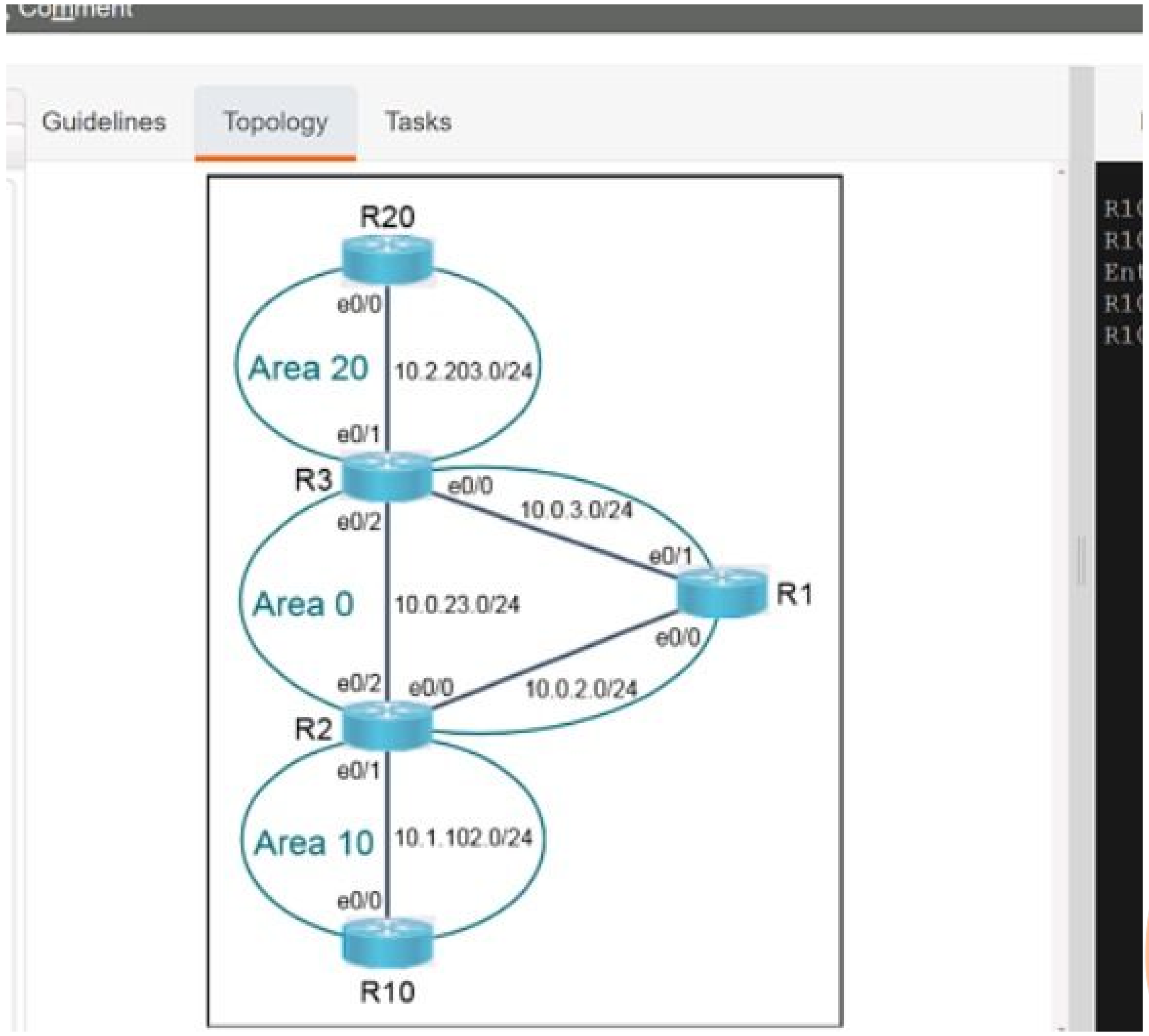
SIMULATION



OSPF is partially configured. Complete the OSPF configurations to achieve these goals:

1. Configure R3 to always be the DR in Area 20. Do not change the router ID.
2. Configure R2 and R10 so they do not participate in a DR/BDR election process in Area 10.

```
R10>en
R10#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R10(config)#interface et0/0
R10(config-if)#ip ospf priority
```



```
R1
R1
Ent
R1
R1
```

A. See the solution below in Explanation

Correct Answer: A
Section:
Explanation:
Solution:
R3
Int e0/1
Ip ospf priority 255
End
Copy run start
R2
Int e0/1
Ip ospf network point-to-point
End
Copy run start
R10
Int e0/0
Ip ospf network point-to-point
End
Copy run start