350-401 Dumps

Implementing and Operating Cisco Enterprise Network Core Technologies

https://www.certleader.com/350-401-dumps.html

NEW QUESTION 1
- (Topic 4)
Graphical user interface, text, application, email Description automatically generated
Refer to the Exhibit. Running the script causes the output in the exhibit. What should be the first line of the script?

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

Answer: C

NEW QUESTION 2
- (Topic 4)

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

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

Reler to the exhibit The EtherChannel between SW1 and SW2 is not operational. Which a coon will resolve the issue?

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

Answer: C

NEW QUESTION 3
- (Topic 4)

```
                    10.1.1.3/24
                    E0/0
                                              WAN
   Inside
                    Serial 0/0
                    209.165.201.30/27
                    Outside

   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 --- ---
```

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

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

**Answer:** BC

NEW QUESTION 4
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the orchestration tool classifications on the right.

```
   ┌──────────────────────────────────┐     ┌─────────────────────────────────────┐
   │      mutable infrastructure      │     │ Configuration Management            │
   └──────────────────────────────────┘     │  ┌───────────────────────────────┐  │
                                            │  │                               │  │
   ┌──────────────────────────────────┐     │  └───────────────────────────────┘  │
   │     immutable infrastructure     │     │  ┌───────────────────────────────┐  │
   └──────────────────────────────────┘     │  │                               │  │
                                            │  └───────────────────────────────┘  │
   ┌──────────────────────────────────┐     └─────────────────────────────────────┘
   │   designed to provision the servers │   ┌─────────────────────────────────────┐
   └──────────────────────────────────┘     │ Orchestration                       │
                                            │  ┌───────────────────────────────┐  │
   ┌──────────────────────────────────┐     │  │                               │  │
   │ designed to install and manage software on existing servers │  └───────────────────────────────┘  │
   └──────────────────────────────────┘     │  ┌───────────────────────────────┐  │
                                            │  │                               │  │
                                            │  └───────────────────────────────┘  │
                                            └─────────────────────────────────────┘
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:

mutable infrastructure	**Configuration Management**
immutable infrastructure	mutable infrastructure
designed to provision the servers	designed to install and manage software on existing servers
designed to install and manage software on existing servers	**Orchestration**
	immutable infrastructure
	designed to provision the servers
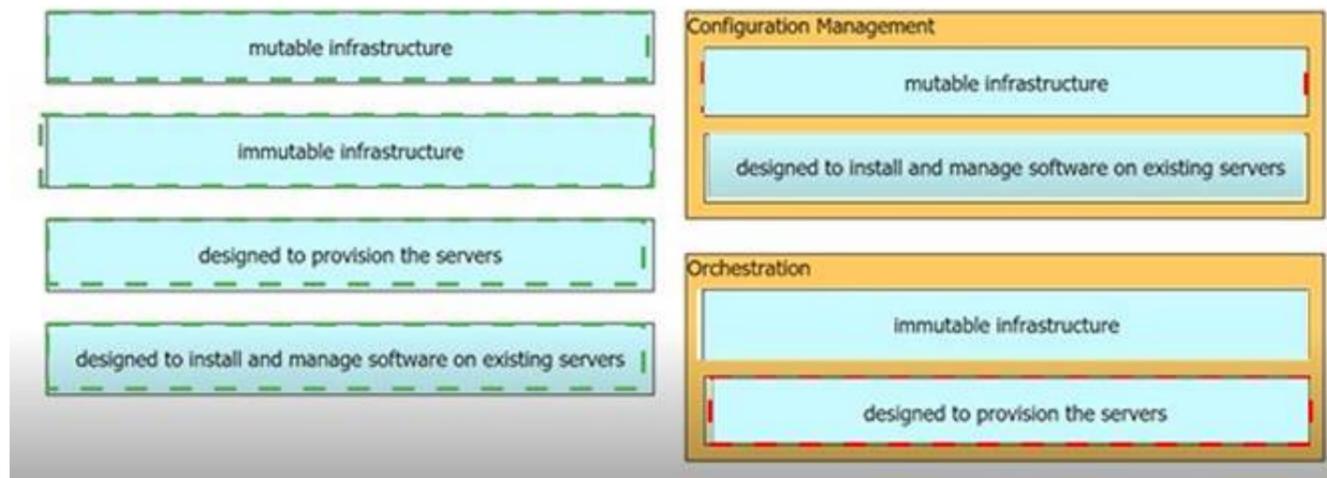
NEW QUESTION 5
- (Topic 4)

```
FastEthernet1/0/47 - Group 1 (version 2)
    State is Standby
        7 state changes, last state change 00:00:02
    Virtual IP address is 10.1.1.1
    Active virtual MAC address is 0000.0c9f.f001
        Local virtual MAC address is 0000.0c9f.f001 (v2 default)
    Hello time 3 sec, hold time 10 sec
        Next hello sent in 0.375 secs
    Authentication MD5, key-string "cisco"
    Preemption enabled, delay min 5 secs
    Active router is 10.1.1.2, priority 255 (expires in 9.396 sec)
    Standby router is local
    Priority 100 (default 100)
    IP redundancy name is "hsrp-Fa1/0/47-1" (default)
```

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

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

Answer: BE

NEW QUESTION 6
- (Topic 4)
Which Cisco DNA Center application is responsible for group-based access control permissions?

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

Answer: C

NEW QUESTION 7
- (Topic 4)
An engineer must contigure a rou'.er to allow users to run specHic configuration commands by validating the user against the router database. Which configuration must be applied?

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

Answer: C

NEW QUESTION 8
SIMULATION - (Topic 4)
Simulation 09

A. Mastered
B. Not Mastered

Answer: A

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

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

NEW QUESTION 9

- (Topic 4)
A customer has 20 stores located throughout a city. Each store has a single Cisco access point managed by a central WLC. The customer wants to gather analysis for users in each store. Which technique supports these requirements?

A. angle of arrival
B. hyperlocation
C. trilateration
D. presence

Answer: B

NEW QUESTION 10

- (Topic 4)
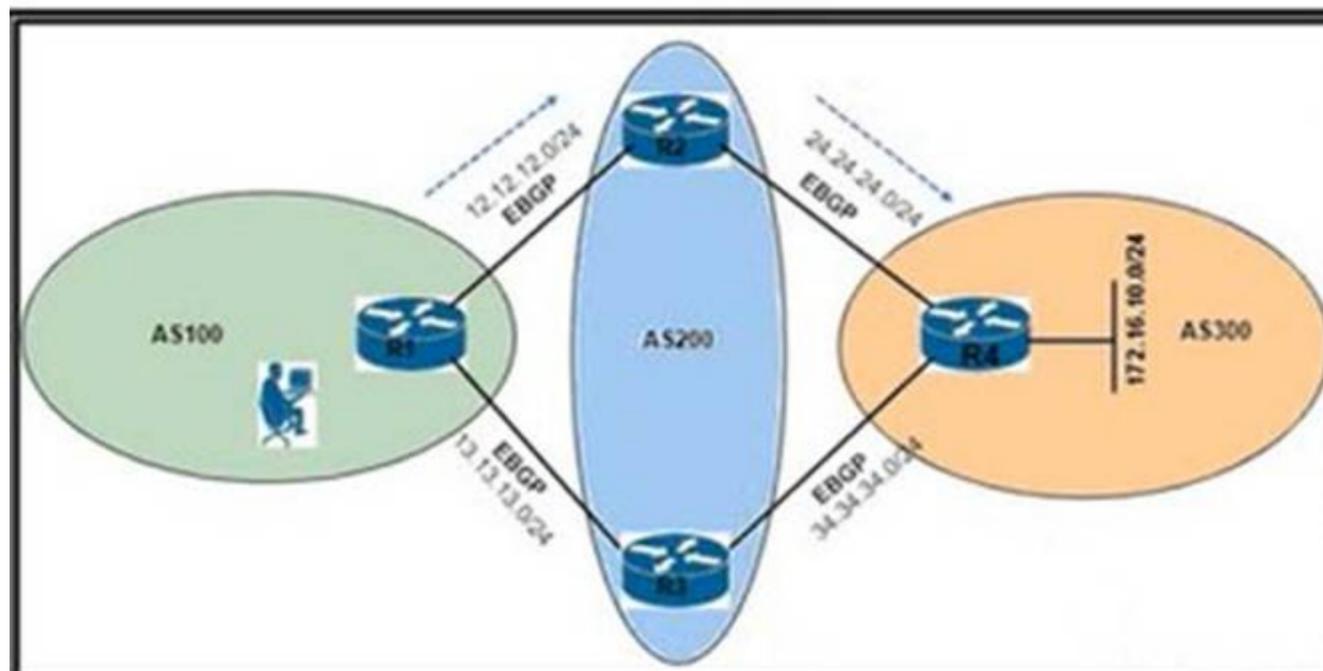

```
R1#sh ip bgp
BGP table version is 2, local router ID is 13.13.13.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
           r RIB-failure, S Stale, m multipath, b backup-path, f RT-
Filter,
           x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
       Network          Next
Hop         Metric       LocPrf       Weight       Path
*  172.16.1.0/24         13.13.13.3                              0
       200 300 i
*>                        12.12.12.2                             0
       200 300 i
```

Refer to the exhibit. An engineer is reaching network 172.16.10.0/24 via the R1-R2-R4 path. Which configuration forces the traffic to fake a path of R1-R3-R4?

A)

```
R2(config)#route-map RM_MED permit 10
R2(config-route-map)#set metric 1
R2(config-route-map)#exit
R2(config)#router bgp 200
R2(config-router)#neighbor 12.12.12.1 route-map RM_MED out
R2(config-router)#end
R2#clear ip bgp 12.12.12.1 soft out
```

B)

```
R1(config)#router bgp 100
R1(config-router)#neighbor 13.13.13.3 weight 1
R1(config-router)#end
```

C)

```
R1(config)#route-map RM_AS_PATH_PREPEND
R1(config-route-map)#set as-path prepend 200 200
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#neighbor 12.12.12.2 route-map RM_AS_PATH_PREPEND in
R1(config-router)#end
R1#clear ip bgp 12.12.12.2 soft in
```

D)

```
R1(config)#route-map RM_LOCAL_PREF permit 10
R1(config-route-map)#set local-preference 101
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#neighbor 13.13.13.3 route-map RM_LOCAL_PREF in
R1(config-router)#end
R1#clear ip bgp 13.13.13.3 soft in
```

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

Answer: D

NEW QUESTION 10
- (Topic 4)
Which security measure mitigates a man-in-the-middle attack of a REST API?

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

Answer: A

NEW QUESTION 11
- (Topic 4)
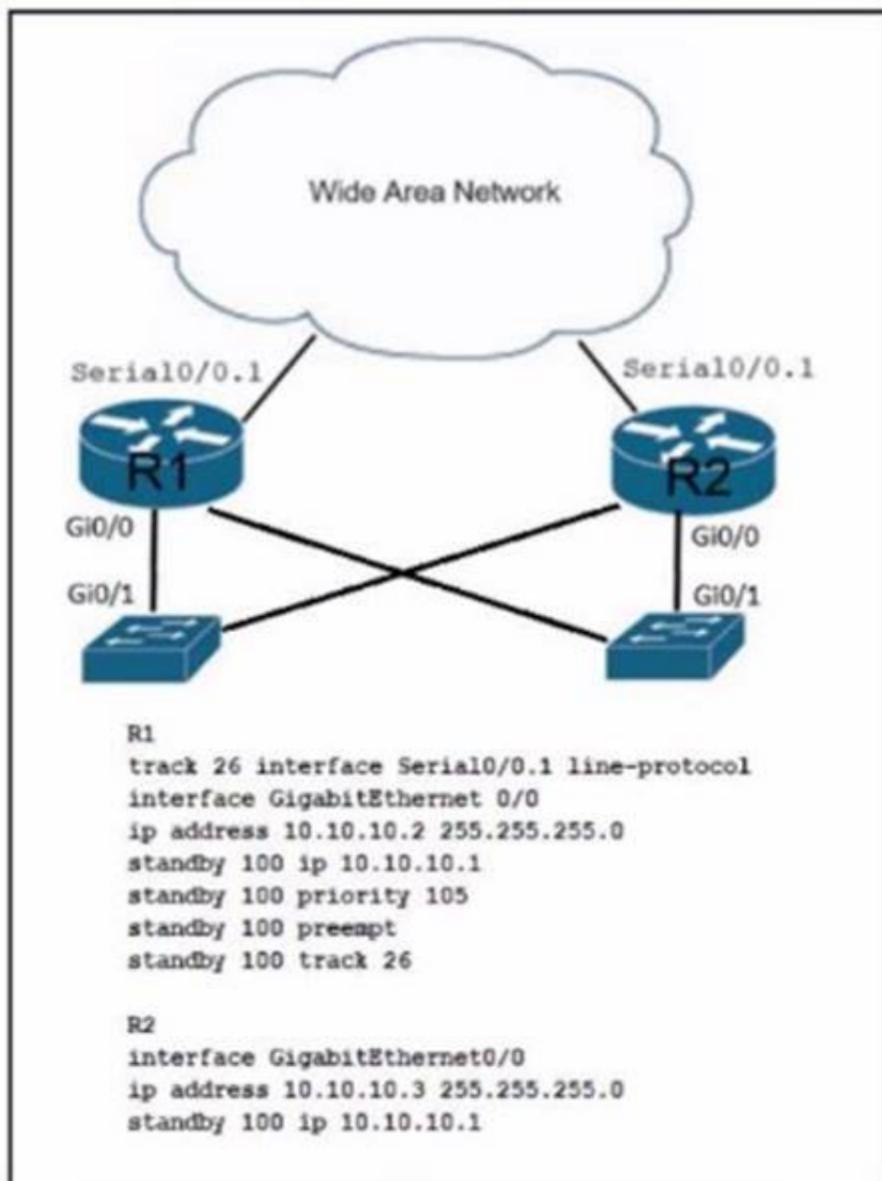Which tunnel type al'ows clients to perform a seamless Layer 3 roam between a Cisco AireOS WLC and a Cisco IOS XE WLC?

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

Answer: A

NEW QUESTION 14
- (Topic 4)
Relet lo lbe exhibit.

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

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

Answer: A

NEW QUESTION 18
- (Topic 4)
An engineer must configure router R1 to validate user logins via RADIUS and fall back to the local user database if the RADIUS server is not available. Which configuration must be applied?

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

Answer: C

NEW QUESTION 19
- (Topic 4)
What is the function of the fabric control plane node in a Cisco SD-Access deployment?
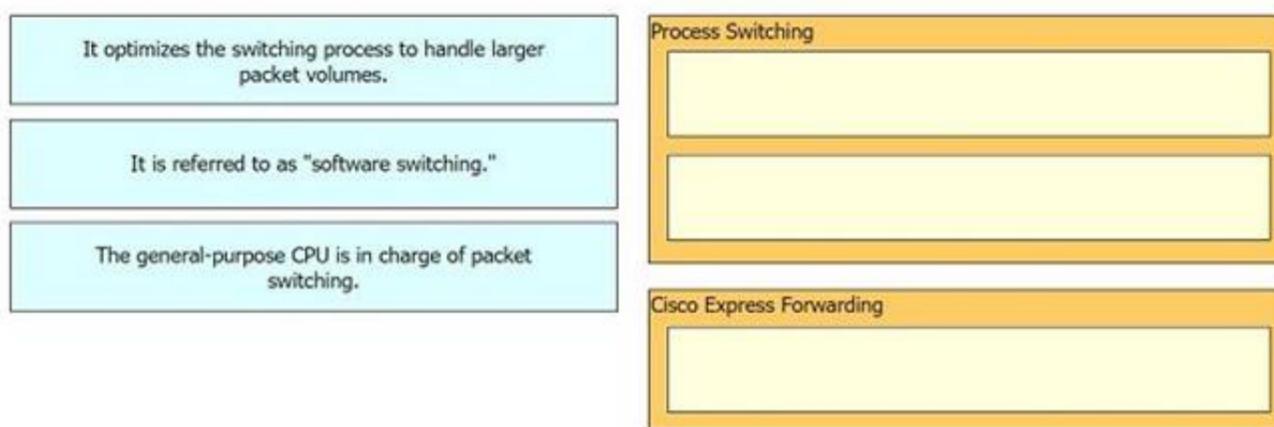
A. It is responsible for policy application and network segmentation in the fabric
B. It performs traffic encapsulation and security profiles enforcement in the fabric
C. It holds a comprehensive database that tracks endpoints and networks in the fabric
D. It provides integration with legacy nonfabric-enabled environments

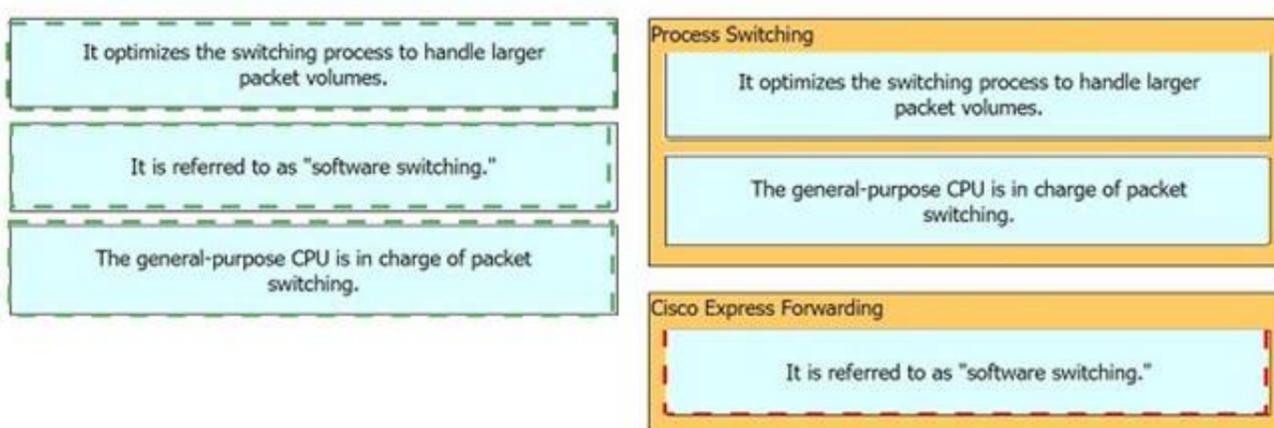**Answer:** C

NEW QUESTION 21
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the switching architectures on the right.

Process Switching		

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.

Cisco Express Forwarding		

A. Mastered
B. Not Mastered

Answer: A

Explanation:

It optimizes the switching process to handle larger packet volumes.
It is referred to as "software switching."
The general-purpose CPU is in charge of packet switching.

Process Switching
It optimizes the switching process to handle larger packet volumes.
The general-purpose CPU is in charge of packet switching.

Cisco Express Forwarding
It is referred to as "software switching."

NEW QUESTION 24
- (Topic 4)
A customer requires their wireless network to be fully functional, even if the wireless controller fails. Which wireless design supports these requirements?

A. FlexConnect
B. mesh
C. centralized
D. embedded

Answer: A

Explanation:
 This is because FlexConnect is a feature that allows wireless access points to operate in standalone mode when they lose connectivity to the wireless LAN controller. FlexConnect enables the access points to switch the data traffic locally, without sending it to the controller, and to perform local authentication, without relying on the central server. FlexConnect also allows the access points to maintain the wireless network functionality, such as SSIDs, security policies, and QoS, even if the wireless controller fails. FlexConnect is suitable for branch locations or remote offices that have limited WAN bandwidth or reliability. The source of this answer is the Cisco ENCOR v1.1 course, module 7, lesson 7.3: Implementing FlexConnect.

NEW QUESTION 28
- (Topic 4)
An engineer must protect the password for the VTY lines against over-the-shoulder attacks. Which configuration should be applied?

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

Answer: A

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

NEW QUESTION 33

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

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

B)

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

C)

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

D)

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

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

Answer: B

NEW QUESTION 34
- (Topic 4)
Which IP SLA operation requires the IP SLA responder to be configured on the remote end?

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

Answer: D

NEW QUESTION 38
- (Topic 4)

```
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand—alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel—groups in use: 1
Number of aggregators:        1

Group  Port—channel  Protocol  Ports
------+-------------+--------+--------------------
1      Po1 (SD)         -      Fa0/1 (D)  Fa0/2 (D)
```

```
S1# show run | begin interface port-channel        S2# show run | begin interface port-channel
interface Port—channel1                            interface Port—channel1
  switchport mode trunk                               switchport mode trunk
!                                                  !
interface FastEthernet0/1                          interface FastEthernet0/1
  switchport mode trunk                               switchport mode trunk
  channel-group 1 mode on                             channel-group 1 mode desirable
!                                                  !
interface FastEthernet0/2                          interface FastEthernet0/2
  switchport mode trunk                               switchport mode trunk
  channel-group 1 mode on                             channel-group 1 mode desirable
!                                                  !
<Output omitted>                                   <Output omitted>
```

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

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

Answer: C

NEW QUESTION 41
- (Topic 4)
Which Python code snippet must be added to the script to store the changed interface configuration to a local JSON-formatted file?

```
import json
import requests

Creds = ("user", "Z#418208328$mnV")
Headers = { "Content-Type" : "application/yang-data+json",
            "Accept" : "application/yang-data+json" }

BaseURL = https://cpe/restconf/data"
URL = BaseURL + "/Cisco-IOS-XE-native:native/interface"

Response = requests.get(URL, auth = Creds, headers = Headers, verify = False)
UpdatedConfig = Response.text.replace("2001:db8:1:", "2001:db8:café:"
```

○ OutFile = open("ifaces.json", "w")
json.dump(UpdatedConfig,OutFile)
OutFile.close()

○ OutFile = open("ifaces.json", "w")
OutFile.write(UpdatedConfig)
OutFile.close()

○ OutFile = open("ifaces.json", "w")
OutFile.write(Response.text)
OutFile.close()

○ OutFile = open("ifaces.json", "w")
OutFile.write(Response.json())
OutFile.close()

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

Answer: B

NEW QUESTION 45
- (Topic 4)
Refer to the exhibit.

```
line vty 0 4
  session-timeout 30
  exec-timeout 120 0
  session-limit 30
  login local
line vty 5 15
  session-timeout 30
  exec-timeout 30 0
  session-limit 30
  login local
```

Only administrators from the subnet 10.10.10.0/24 are permitted to have access to the router. A secure protocol must be used for the remote access and management of the router instead of clear-text protocols. Which configuration achieves this goal?

○ access-list 23 permit 10.10.10.0 0.0.0.255
  line vty 0 4
  access-class 23 in
  transport input ssh

○ access-list 23 permit 10.10.10.0 0.0.0.255
  line vty 0 15
  access-class 23 in
  transport input ssh

○ access-list 23 permit 10.10.10.0 0.0.0.255
  line vty 0 15
  access-class 23 out
  transport input all

○ access-list 23 permit 10.10.10.0 255.255.255.0
  line vty 0 15
  access-class 23 in
  transport input ssh

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

Answer: B

NEW QUESTION 46
- (Topic 4)

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

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

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

☐ R1(config)#policy-map POLICY-CoPP
  R1(config-pmap)#class CLASS-CoPP-Management
  R1(config-pmap-c)#police 320000 conform-action transmit exceed-action transmit violate-action drop

☐ R1(config)#control-plane
  R1(config-cp)# service-policy input POLICY-CoPP

☐ R1(config-pmap)#class CLASS-CoPP-Management
  R1(config-pmap-c)#police 32 conform-action transmit exceed-action drop violate-action transmit

☐ R1(config)#control-plane
  R1(config-cp)# service-policy output POLICY-CoPP

☐ R1(config)#policy-map POLICY-CoPP
  R1(config-pmap)#class CLASS-CoPP-Management
  R1(config-pmap-c)#police 320000 conform-action transmit exceed-action drop violate-action drop

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

Answer: BE

NEW QUESTION 48
- (Topic 4)
What is a characteristic of para-virtualization?

A. Para-virtualization allows direct access between the guest OS and the hypervisor.
B. Para-virtualization allows the host hardware to be directly accessed.
C. Para-virtualization guest servers are unaware of one another.
D. Para-virtualization lacks support for containers.

Answer: A

NEW QUESTION 50
- (Topic 4)
Which DNS lookup does an access point perform when attempting CAPWAP discovery?

A. CISCO-DNA-CONTROLLER local
B. CAPWAP-CONTROLLER local
C. CISCO-CONTROLLER local
D. CISCO-CAPWAP-CONTROLLER local

Answer: D

NEW QUESTION 52
- (Topic 4)
An engineer is connected to a Cisco router through a Telnet session. Which command must be issued to view the logging messages from the current session as soon as they are generated by the router?

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

Answer: D

NEW QUESTION 53
- (Topic 4)
Which solution should be used in a high-density wireless environment to increase bandwidth for each user?

A. Increase antenna size
B. Increase the mandatory minimum data rate.
C. Increase the cell size of each AP.
D. Increase TX power.

Answer: B

NEW QUESTION 55
SIMULATION - (Topic 4)
Simulation 04
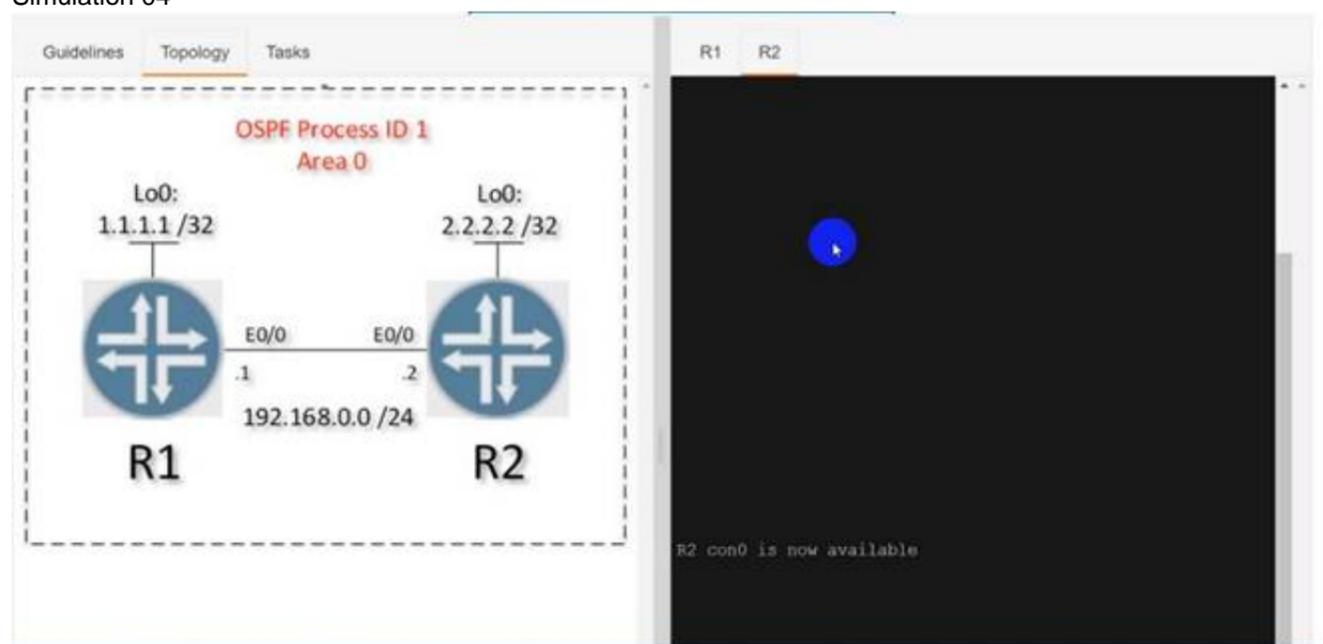
| Guidelines | Topology | Tasks | | R1 | R2 |

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

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

💬 Submit feedback about this item.

A. Mastered
B. Not Mastered

Answer: A

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

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

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

```
R1#sh ip ospf neighbor

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


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


                   Base Topology (MTID 0)


    Area BACKBONE(0)

    Intra-area Route List

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


    First Hop Forwarding Gateway Tree

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

NEW QUESTION 57
- (Topic 4)
An engineer must construct an access list tot a Cisco Catalyst 9800 Series WLC that will - edirect wireless guest users to a splash page that is hosted on a Cisco ISE server. The Cisco ISE servers are hosted at 10.9.11.141 and 10.1.11.141. Which access list meets the requirements?
A)

```
ip access-list extended ACL_WEBAUTH_REDIRECT
 70 permit   ip any host 10.9.11.141
 80 permit   ip any host 10.1.11.141
 500 permit tcp any any eq www
 600 permit tcp any any eq 443
 700 permit tcp any any eq 8443
 800 deny   udp any any eq domain
```

B)

```
ip access-list extended ACL_WEBAUTH_REDIRECT
70 permit ip any host 10.9.11.141
80 permit ip any host 10.1.11.141
500 deny   tcp any any eq www
600 deny   tcp any any eq 443
700 deny   tcp any any eq 8443
800 deny   udp any any eq domain
901 deny   ip any any
```

C)

```
ip access-list extended ACL_WEBAUTH_REDIRECT
70 deny   ip any host 10.9.11.141
80 deny   ip any host 10.1.11.141
500 permit tcp any any eq www
600 permit tcp any any eq 443
700 permit tcp any any eq 8443
800 deny   udp any any eq domain
```

D)

```
ip access-list extended ACL_WEBAUTH_REDIRECT
50 deny   ip host 10.9.11.141 any
60 deny   ip any host 10.9.11.141
70 deny   ip host 10.1.11.141 any
80 deny   ip any host 10.1.11.141
500 permit tcp any any eq www
600 permit tcp any any eq 443
700 permit tcp any any eq 80
```

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

Answer: D

Explanation:
Option D is the correct access list to redirect wireless guest users to a splash page that is hosted on a Cisco ISE server. The configuration steps are as follows12:
? Define an extended access list that permits TCP traffic from any source to the Cisco ISE servers on port 80 (HTTP) and port 443 (HTTPS). In this case, the access list is named ACL_WEBAUTH_REDIRECT and it allows any host to connect to the IP addresses 10.9.11.141 and 10.1.11.141 on port 80 and port 443: ip access-list extended ACL_WEBAUTH_REDIRECT and permit tcp any host 10.9.11.141 eq 80, permit tcp any host 10.9.11.141 eq 443, permit tcp any host 10.1.11.141 eq 80, permit tcp any host 10.1.11.141 eq 443.
? Apply the access list to the guest WLAN using the ip access-group command. This command filters the traffic on the interface based on the access list. In this case, the access list ACL_WEBAUTH_REDIRECT is applied to the guest WLAN interface in the inbound direction, which means that only the traffic that matches the access list can enter the interface: interface wlan-guest and ip access-group ACL_WEBAUTH_REDIRECT in.
Option A is incorrect because it does not permit TCP traffic to the Cisco ISE servers on port 80, which is required for HTTP redirection. Without this, the guest users will not be able to see the splash page on their web browsers12.
Option B is incorrect because it does not permit TCP traffic to the Cisco ISE servers on port 443, which is required for HTTPS redirection. Without this, the guest users will not be able to see the splash page on their web browsers if they use HTTPS12.
Option C is incorrect because it permits TCP traffic from any source to any destination on port 80 and port 443, which is too broad and may allow unwanted traffic to enter the guest WLAN interface. This may compromise the security and performance of the guest network12. References: 1: Configuring Web Authentication, 2: ISE and Catalyst 9800 Series Integration Guide

NEW QUESTION 59
- (Topic 4)

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

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

Answer: D

NEW QUESTION 62
DRAG DROP - (Topic 4)
Drag the characteristics from the left onto the routing protocols they describe on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 63
- (Topic 4)
Which behavior can be expected when the HSRP versions is changed from 1 to 2?

A. Each HSRP group reinitializes because the virtual MAC address has changed.
B. No changes occur because version 1 and 2 use the same virtual MAC OUI.
C. Each HSRP group reinitializes because the multicast address has changed.
D. No changes occur because the standby router is upgraded before the active router.

Answer: A

NEW QUESTION 65
- (Topic 4)
When using BFD in a network design, which consideration must be made?

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

Answer: C

NEW QUESTION 67
- (Topic 1)
What is used to perform OoS packet classification?

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

Answer: D

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

NEW QUESTION 70
- (Topic 1)
Which method should an engineer use to deal with a long-standing contention issue between any two VMs on the same host?

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

Answer: A

NEW QUESTION 75
- (Topic 2)
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.

Answer: B

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

NEW QUESTION 76
DRAG DROP - (Topic 2)
Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 78
- (Topic 2)
What is a characteristic of Cisco StackWise technology?

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

Answer: C

NEW QUESTION 81
- (Topic 2)
The login method is configured on the VTY lines of a router with these parameters.
? The first method for authentication is TACACS
? If TACACS is unavailable, login is allowed without any provided credentials
Which configuration accomplishes this task?

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

Answer: C

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

NEW QUESTION 86
- (Topic 2)

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

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

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

Answer: D

NEW QUESTION 87
- (Topic 2)
In a Cisco SD-WAN solution, which two functions are performed by OMP? (Choose two.)

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

Answer: AB

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

NEW QUESTION 92
- (Topic 2)
Which access point mode allows a supported AP to function like a WLAN client would, associating and identifying client connectivity issues?

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

Answer: C

Explanation:
As these wireless networks grow especially in remote facilities where IT professionals may not always be onsite, it becomes even more important to be able to quickly identify and resolve potential connectivity 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

NEW QUESTION 94
- (Topic 2)

Refer to the exhibit.

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

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

Answer: A

NEW QUESTION 96
- (Topic 2)
What does a northbound API accomplish?

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

Answer: A

NEW QUESTION 100
- (Topic 2)
How cloud deployments differ from on-prem deployments?

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

Answer: C
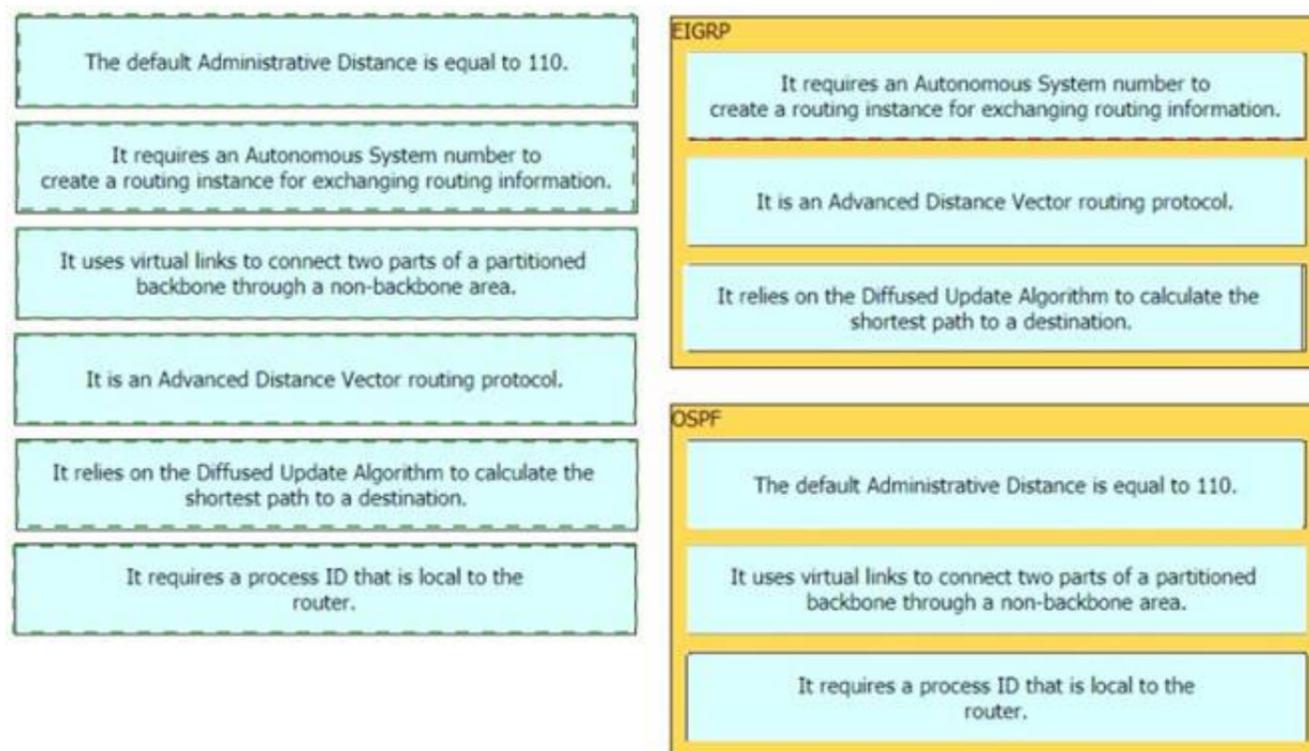

NEW QUESTION 102
DRAG DROP - (Topic 2)
Drag and drop the characteristics from the left onto the routing protocols they describe on the right.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 105
- (Topic 2)
When is the Design workflow used In Cisco DNA Center?

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

Answer: A

Explanation:
The Design area is where you create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network. Use the Design workflow if you do not already have an existing infrastructure. If you have an existing infrastructure, use the Discovery feature.
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/user_guide/b_cisco_dna_center_ug_2_1_2/b_cisco_dna_center_ug_2_1_1_chapter_011 0.html
Reference: https://synoptek.com/insights/it-blogs/greenfield-vs-brownfield-software- development/"Greenfield development refers to developing a system for a totally new environment and requires development from a clean slate – no legacy code around. It is an approach used when you're starting fresh and with no restrictions or dependencies."

NEW QUESTION 109
- (Topic 2)
What is the difference between a RIB and a FIB?

A. The RIB is used to make IP source prefix-based switching decisions
B. The FIB is where all IP routing information is stored
C. The RIB maintains a mirror image of the FIB
D. The FIB is populated based on RIB content

Answer: D

Explanation:
 CEF uses a Forwarding Information Base (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 those 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 earlier switching paths such as fast switching and optimum switching.
Note: In order to view the Routing information base (RIB) table, use the "show ip route" command. To view the Forwarding Information Base (FIB), use the "show ip cef" command. RIB is in Control plane while FIB is in Data plane.

NEW QUESTION 112
- (Topic 2)
An engineer is implementing a Cisco MPLS TE tunnel to improve the streaming experience for the clients of a video-on-demand server. Which action must the engineer perform to configure extended discovery to support the MPLS LDP session between the headend and tailend routers?

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

Answer: B

NEW QUESTION 115
- (Topic 2)
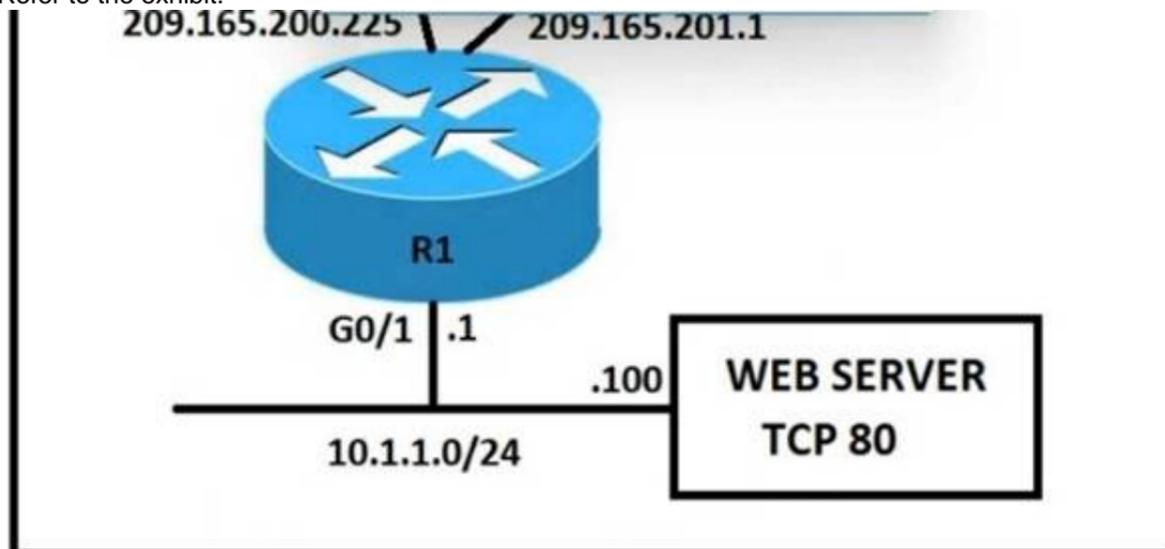In a Cisco SD-WAN solution, how Is the health of a data plane tunnel monitored?

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

Answer: C

NEW QUESTION 116
- (Topic 2)
Refer to the exhibit.

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

A. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 extendableip 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 80ip 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 80ip 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-aliasip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80 no-alias

Answer: B

NEW QUESTION 121
- (Topic 2)
Refer to the exhibit.

R2 is the neighboring router of R1. R2 receives an advertisement for network 192 168.10.50/32. Which configuration should be applied for the subnet to be advertised with the original /24 netmask?
A)

B)

C)

D)

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

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

Answer: C

NEW QUESTION 126
- (Topic 2)
Refer to the exhibit.

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

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

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

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

Answer: C

NEW QUESTION 127
- (Topic 2)
What is the function of a control-plane node In a Cisco SD-Access solution?

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

Answer: A

NEW QUESTION 128
- (Topic 2)
Refer to the exhibit.

```
import ncclient

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

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

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

Answer: D

NEW QUESTION 132
DRAG DROP - (Topic 2)
Drag and drop characteristics of PIM dense mode from the left to the right.

builds source-based distribution trees		PIM Dense Mode
uses a push model to distribute multicast traffic		
uses a pull model to distribute multicast traffic		
uses prune mechanisms to stop unwanted multicast traffic		
builds shared distribution trees		
requires a rendezvous point to deliver multicast traffic		

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 135
- (Topic 2)
An engineer configures GigabitEthernet 0/1 for VRRP group 115. The router must assume the primary role when it has the highest priority in the group. Which command set is required to complete this task?

```
interface GigabitEthernet0/1
ip address 10.10.10.2 255.255.255.0
vrrp 115 ip 10.10.10.1
vrrp 115 authentication 406530697

○ Router(config-if)# vrrp 115 priority 100

○ Router(config-if)# standby 115 priority 100
  Router(config-if)# standby 115 preempt

○ Router(config-if)# vrrp 115 track 1 decrement 10
  Router(config-if)# vrrp 115 preempt

○ Router(config-if)# vrrp 115 track 1 decrement 100
  Router(config-if)# vrrp 115 preempt
```

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

Answer: C

NEW QUESTION 140
- (Topic 2)
Refer to the exhibit.

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

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


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

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

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

Answer: B

NEW QUESTION 143
DRAG DROP - (Topic 2)
Drag and drop the descriptions from the left onto the routing protocol they describe on the right.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 148
- (Topic 2)
How is a data modeling language used?

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

Answer: A

NEW QUESTION 152
- (Topic 2)

Refer to the exhibit.

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

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

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

A)

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

B)

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

C)

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

D)

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

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

Answer: C

NEW QUESTION 156
- (Topic 2)
Refer to the exhibit.

An engineer is troubleshooting an application running on Apple phones. The application Is receiving incorrect QoS markings. The systems administrator confirmed that ail configuration profiles are correct on the Apple devices. Which change on the WLC optimizes QoS for these devices?

A. Enable Fastlane
B. Set WMM to required
C. Change the QoS level to Platinum
D. Configure AVC Profiles

Answer: C

NEW QUESTION 161
- (Topic 2)
Which two actions, when applied in the LAN network segment, will facilitate Layer 3
CAPWAP discovery for lightweight AP? (Choose two.)

A. Utilize DHCP option 17.
B. Configure WLC IP address on LAN switch.

C. Utilize DHCP option 43.
D. Configure an ip helper-address on the router interface
E. Enable port security on the switch port

Answer: CE

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

NEW QUESTION 165
DRAG DROP - (Topic 2)
Drag and drop the descriptions from the left onto the QoS components they describe on the right.

applied on traffic to convey information to a downstream device	shaping
distinguishes traffic types	marking
process used to buffer traffic that exceeds a predefined rate	trust
permits traffic to pass through the device while retaining DSCP/COS values	classification

A. Mastered
B. Not Mastered

Answer: A

Explanation:

applied on traffic to convey information to a downstream device	process used to buffer traffic that exceeds a predefined rate
distinguishes traffic types	applied on traffic to convey information to a downstream device
process used to buffer traffic that exceeds a predefined rate	permits traffic to pass through the device while retaining DSCP/COS values
permits traffic to pass through the device while retaining DSCP/COS values	distinguishes traffic types

NEW QUESTION 168
- (Topic 2)
Refer to the exhibit.

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

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

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

B)

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

C)

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

D)

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

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

Answer: D

NEW QUESTION 172
- (Topic 2)
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

Answer: A

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

NEW QUESTION 176
- (Topic 2)
Refer to the exhibit.

```
R1(config)#ip sla 1
R1(config-ip-sla)#icmp-echo 172.20.20.2 source-interface FastEthernet0/0
R1(config-ip-sla-echo)#timeout 5000
R1(config-ip-sla-echo)#frequency 10
R1(config-ip-sla-echo)#threshold 500
R1(config)#ip sla schedule 1 start-time now life forever
R1(config)#track 10 ip sla 1 reachability
R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2 track 10
R1(config)#no ip route 0.0.0.0 0.0.0.0 172.20.20.2
R1(config)#ip route 0.0.0.0 0.0.0.0 172.30.30.2 5
```

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

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

Answer: BE

NEW QUESTION 177
- (Topic 2)
A customer wants to use a single SSID to authenticate IoT devices using different passwords. Which Layer 2 security type must be configured in conjunction with Cisco ISE to achieve this requirement?

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

Answer: D

NEW QUESTION 179
- (Topic 2)
Refer to the exhibit.
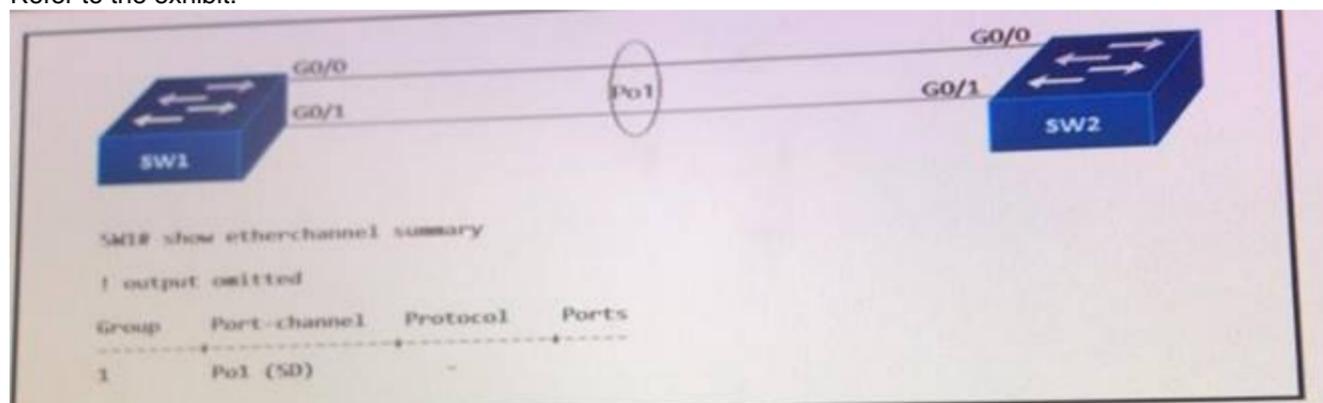
After an engineer configures an EtherChannel between switch SW1 and switch SW2, this error message is logged on switch SW2.
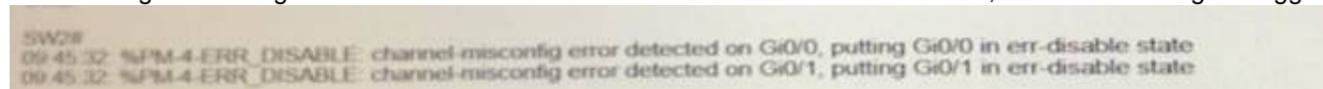
Based on the output from SW1 and the log message received on Switch SW2, what action should the engineer take to resolve this issue?

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

Answer: A

Explanation:
In this case, we are using your EtherChannel without a negotiation protocol. As a result, if the opposite switch is not also configured for EtherChannel operation on

the respective ports, there is a danger of a switching loop. The EtherChannel Misconfiguration Guard tries to prevent that loop from occuring by disabling all the ports bundled in the EtherChannel.

NEW QUESTION 183
- (Topic 2)
Refer to the exhibit.

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

Channel group 1
                              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      bndl         15          0x1     0x1     0x2      0x3C
```

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

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

Answer: D

NEW QUESTION 186
- (Topic 2)
What is the wireless received signal strength indicator?

A. The value given to the strength of the wireless signal received compared to the noise level
B. The value of how strong the wireless signal Is leaving the antenna using transmit power, cable loss, and antenna gain
C. The value of how much wireless signal is lost over a defined amount of distance
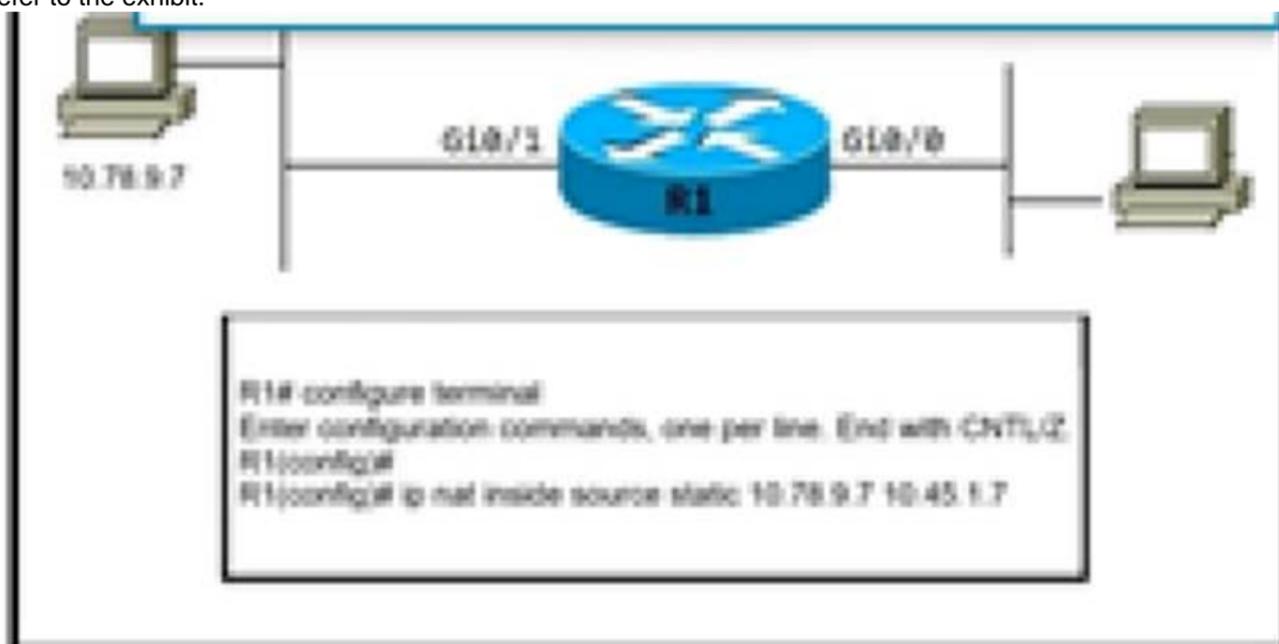D. The value of how strong a tireless signal is receded, measured in dBm

Answer: D

Explanation:
RSSI, or "Received Signal Strength Indicator," is a measurement of how well your device can hear a signal from an access point or router. It's a value that is useful for determining if you have enough signal to get a good wireless connection.
This value is measured in decibels (dBm) from 0 (zero) to -120 (minus 120). The closer to 0 (zero) the stronger the signal is which means it's better, typically voice networks require a - 65db or better signal level while a data network needs -80db or better.

NEW QUESTION 188
- (Topic 2)
Refer to the exhibit.

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)# ip nat inside source static 10.78.9.7 10.45.1.7
```

A network architect has partially configured static NAT. which commands should be asked to complete the configuration?

A. R1(config)#interface GigabitEthernet0/0 R1(config)#ip pat outside R1(config)#interface GigabitEthernet0/1 R1(config)#ip pat inside
B. R1(config)#interface GigabitEthernet0/0 R1(config)#ip nat outside R1(config)#interface GigabitEthernet0/1 R1(config)#ip nat inside
C. R1(config)#interface GigabitEthernet0/0 R1(config)#ip nat inside R1(config)#interface GigabitEthernet0/1 R1(config)#ip nat outside
D. R1(config)#interface GigabitEthernet0/0 R1(config)#ip pat inside R1(config)#interface GigabitEthernet0/1 R1(config)#ip pat outside

Answer: B

NEW QUESTION 189
- (Topic 2)
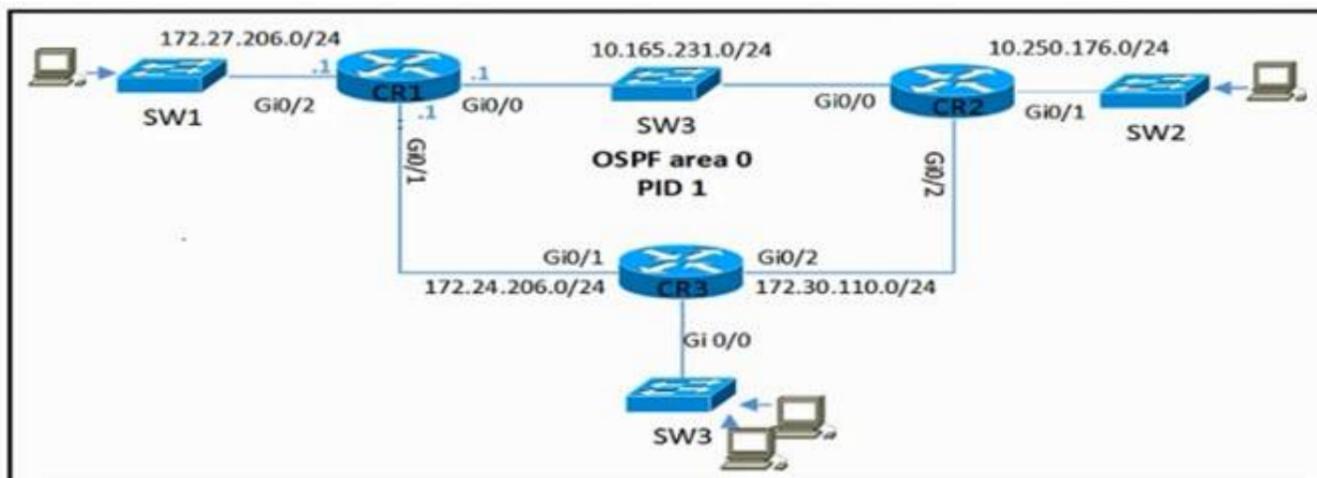Which two parameters are examples of a QoS traffic descriptor? (Choose two)

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

Answer: AC

NEW QUESTION 192
- (Topic 2)
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
```

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

Answer: D

NEW QUESTION 197
- (Topic 2)
What NTP Stratum level is a server that is connected directly to an authoritative time source?

A. Stratum 0
B. Stratum 1
C. Stratum 14
D. Stratum 15

Answer: B

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/routers/asr920/configuration/guide/bsm/16-6-1/b-bsm-xe-16-6-1-asr920/bsm-timecalendar- set.html

NEW QUESTION 198
- (Topic 2)
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

Answer: CE

NEW QUESTION 202
DRAG DROP - (Topic 2)
Drag and drop the characteristics from the left onto the infrastructure deployment models on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 204
- (Topic 2)
Refer to the exhibit.

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

Answer: A

Explanation:
 Features of the Cisco DNA Assurance solution includes Device 360 and client 360, which provides a detailed view of the performance of any device or client over time and from any application context. Provides very granular troubleshooting in seconds.

NEW QUESTION 205
- (Topic 2)
Refer to the exhibit.
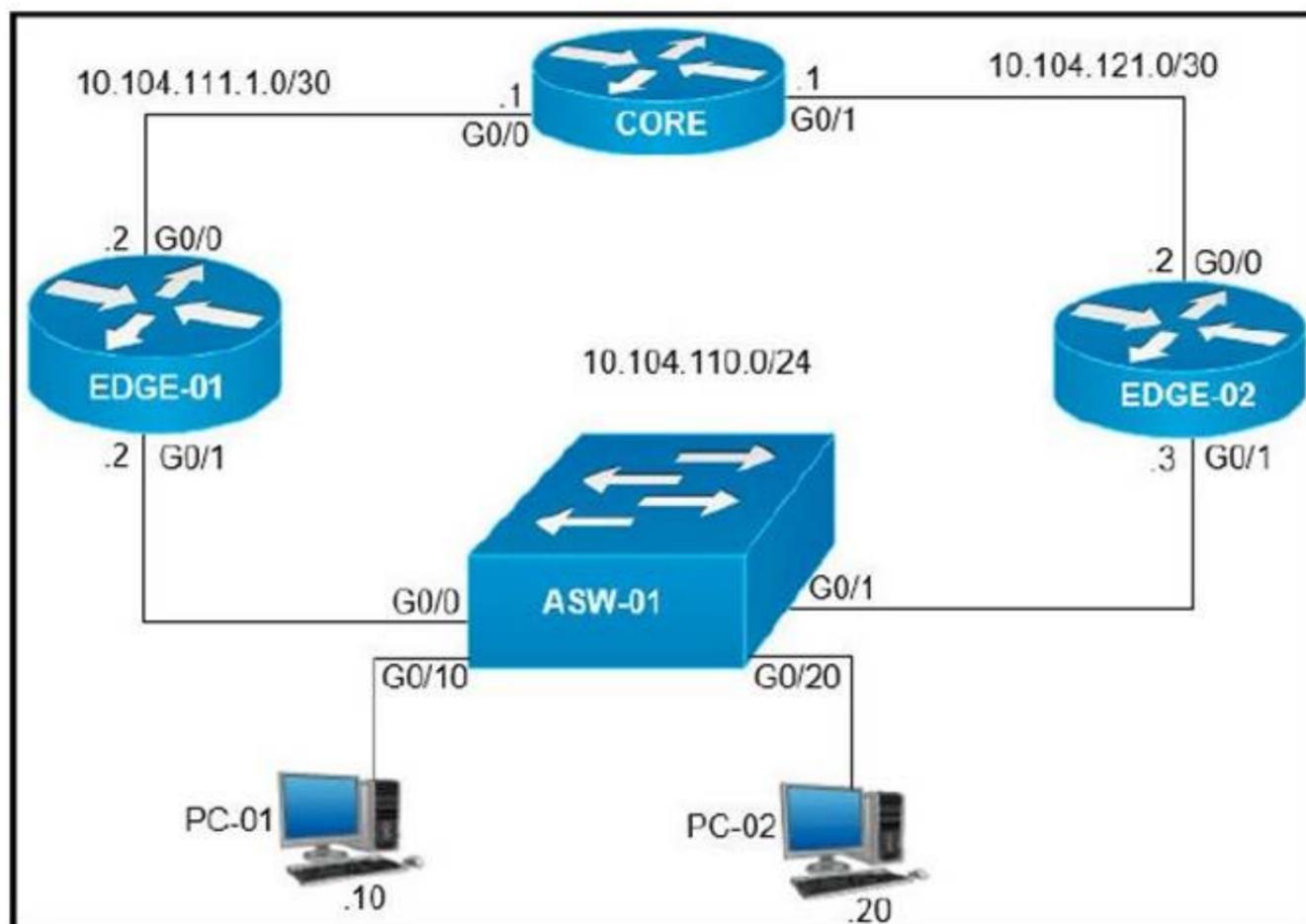
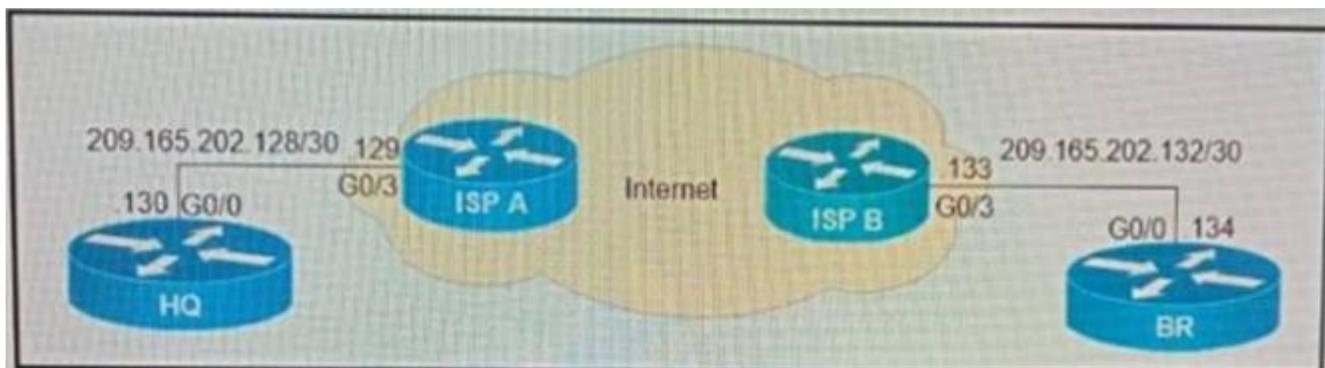On which interfaces should VRRP commands be applied to provide first hop redundancy to PC-01 and PC-02?

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

Answer: C

NEW QUESTION 208
- (Topic 2)
Refer to the exhibit.

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

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

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

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

Answer: B

NEW QUESTION 213
- (Topic 2)
Which technology is used as the basis for the cisco sd-access data plane?

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

Answer: C

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

NEW QUESTION 214
- (Topic 1)
Which component of the Cisco Cyber Threat Defense solution provides user and flow context analysis?

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

Answer: B

NEW QUESTION 217
- (Topic 1)

```
London                         NewYork

    [switch]----▲----------▲----[switch]

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

```
NewYork#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------
1      Po1(SD)       PAgP       Fa0/1(I) Fa0/2(D)
NewYork#
NewYork#show etherchannel port-channel
                Channel-group listing:
                ----------------------
Group: 1
----------
                Port-channels in the group:
                ----------------------------
Port-channel: Po1
----------------
Age of the Port-channel   = 00d:00h:14m:20s
Logical slot/port    = 2/1      Number of ports = 0
GC                   = 0x00000000      HotStandBy port = null
Port state           = Port-channel |
Protocol             =    PAGP
Port Security        = Disabled
```

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

A)

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

B)

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

C)

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

D)

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

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

Answer: D

NEW QUESTION 221
- (Topic 1)
What is the recommended MTU size for a Cisco SD-Access Fabric?

A. 1500
B. 9100
C. 4464
D. 17914

Answer: B

NEW QUESTION 223
- (Topic 1)
Which LISP component is required for a LISP site to communicate with a non-LISP site?

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

Answer: C

NEW QUESTION 227
- (Topic 1)
Which two mechanisms are available to secure NTP? (Choose two.)

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

Answer: DE

NEW QUESTION 231
- (Topic 1)
Which method of account authentication does OAuth 2.0 within REST APIs?

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

Answer: B

Explanation:
The most common implementations of OAuth (OAuth 2.0) use one or both of these tokens:
+ access token: sent like an API key, it allows the application to access a user's data; optionally, access tokens can expire.
+ refresh token: optionally part of an OAuth flow, refresh tokens retrieve a new access token if they have expired. OAuth2 combines Authentication and Authorization to allow more sophisticated scope and validity control.

NEW QUESTION 234
- (Topic 1)
What is a benefit of data modeling languages like YANG?

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

Answer: D

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

NEW QUESTION 235
- (Topic 1)
An engineer runs the code against an API of Cisco DMA Center, and the platform returns this output What does the response indicate?

```
import requests
import sys
import urllib3

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

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

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

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

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

Answer: D

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

NEW QUESTION 240
- (Topic 1)
In a wireless Cisco SD-Access deployment, which roaming method is used when a user moves from one access point to another on a different access switch using a single WLC?

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

Answer: B

Explanation:
A fabric edge node provides onboarding and mobility services for wired users and devices (including fabric-enabled WLCs and APs) connected to the fabric. It is a LISP tunnel router (xTR) that also provides the anycast gateway, endpoint authentication, and assignment to overlay host pools (static or DHCP), as well as group-based policy enforcement (for traffic to fabric endpoints).
From Cisco's guide, under SDA roaming - When a client on a fabric enabled WLAN, roams from an access point to another access point on a different access-switch, it is called Inter- xTR, like a highway. Intra is within intra is between. Like interstate highways. That's how I remember. https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config- guide/b_wl_16_10_cg/mobility.html

NEW QUESTION 242
- (Topic 1)
How is Layer 3 roaming accomplished in a unified wireless deployment?

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

Answer: D

NEW QUESTION 247
- (Topic 1)
Which measurement is used from a post wireless survey to depict the cell edge of the access points?

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

Answer: A

Explanation:

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

NEW QUESTION 249
DRAG DROP - (Topic 1)
Drag and drop the descriptions from the left onto the QoS components on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 252
- (Topic 1)

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

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

Answer: B

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

NEW QUESTION 255
- (Topic 1)

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

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

Answer: BC

NEW QUESTION 256
DRAG DROP - (Topic 1)
Drag and drop the threat defense solutions from the left onto their descriptions on the right.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

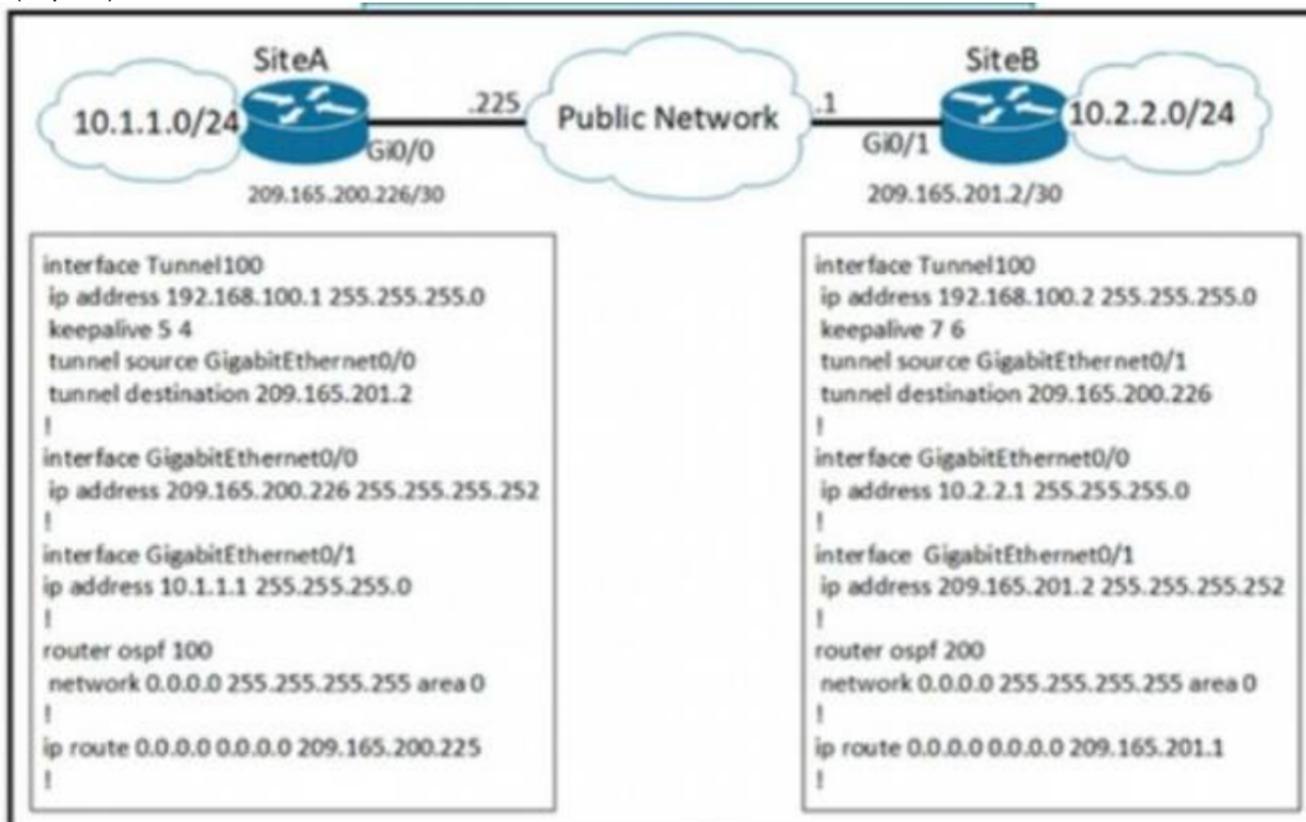| Umbrella		AMP4E
AMP4E		FTD
FTD		StealthWatch
StealthWatch		ESA
ESA		Umbrella
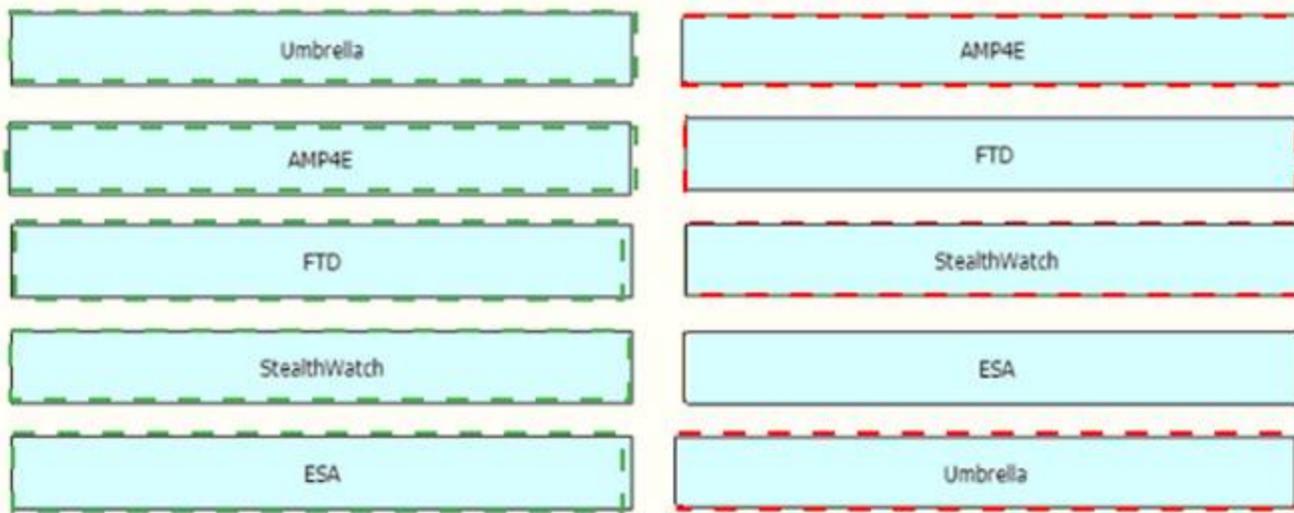
NEW QUESTION 257
- (Topic 1)

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

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

Answer: B

NEW QUESTION 261
- (Topic 1)
Refer to the exhibit.

```
Router#sh run | b vty

line vty 0 4

  session-timeout 30

  exec-timeout 120 0

  session-limit 30

  login local

line vty 5 15

  session-timeout 30

  exec-timeout 30 0

  session-limit 30

  login local
```

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

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

Answer: C

NEW QUESTION 266
- (Topic 1)
Which outbound access list, applied to the WAN interface of a router, permits all traffic except for http traffic sourced from the workstation with IP address 10.10.10.1?
A)

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

B)

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

C)

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

D)

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

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

Answer: A

NEW QUESTION 271
DRAG DROP - (Topic 1)
Drag and drop the characteristics from the left onto the orchestration tools they describe on the right.

	Ansible
utilizes a pull model	
utilizes a push model	
multimaster architecture	**Puppet**
primary/secondary architecture	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Ansible
utilizes a push model

primary/secondary architecture

Puppet
utilizes a pull model

multimaster architecture

NEW QUESTION 273
DRAG DROP - (Topic 1)
Drag and drop the Qos mechanisms from the left to the correct descriptions on the right

service policy	mechanism to create a scheduler for packets prior to forwarding
policy map	mechanism to apply a QoS policy to an interface
DSCP	portion of the IP header used to classify packets

A. Mastered
B. Not Mastered

Answer: A

Explanation:

service policy	policy map
policy map	service policy
DSCP	DSCP

NEW QUESTION 278
- (Topic 1)
Refer to the exhibit.

Which HTTP JSON response does the python code output give?

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

Answer: D

NEW QUESTION 280
- (Topic 1)
Which algorithms are used to secure REST API from brute attacks and minimize the impact?

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

Answer: D

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

NEW QUESTION 283
- (Topic 1)
Which protocol does REST API rely on to secure the communication channel?

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

Answer: B

Explanation:
 The REST API accepts and returns HTTP (not enabled by default) or HTTPS messages that contain JavaScript Object Notation (JSON) or Extensible Markup Language (XML) documents. You
can use any programming language to generate the messages and the JSON or XML documents that
contain the API methods or Managed Object (MO) descriptions.
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_Config
uration_Guide_chapter_01.html

NEW QUESTION 285
- (Topic 1)
Which AP mode allows an engineer to scan configured channels for rogue access points?

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

Answer: B

NEW QUESTION 288
DRAG DROP - (Topic 1)

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

customizable hardware, purpose-built systems

easy to scale and upgrade

more suitable for companies with specific regulatory or security requirements

resources can be over or underutilized as requirements vary

requires a strong and stable internet connection

built-in, automated data backups and recovery

On Premises

Cloud

A. Mastered
B. Not Mastered

Answer: A

Explanation:

On Premises
- customizable hardware, purpose-built systems
- more suitable for companies with specific regulatory or security requirements
- resources can be over or underutilized as requirements vary

Cloud
- easy to scale and upgrade
- requires a strong and stable internet connection
- built-in, automated data backups and recovery

Left column:
- customizable hardware, purpose-built systems
- easy to scale and upgrade
- more suitable for companies with specific regulatory or security requirements
- resources can be over or underutilized as requirements vary
- requires a strong and stable internet connection
- built-in, automated data backups and recovery

NEW QUESTION 290
- (Topic 1)
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 firs
B. If that check fail, a database is checked?
C. A TACACS+server is checked firs
D. If that check fail, a RADIUS server is checke
E. If that check fai
F. a local database is checked.
G. A local database is checked firs
H. If that fails, a TACACS+server is checked, if that check fails, a RADUIS server is checked.
I. A local database is checked firs
J. If that check fails, a TACACS+server is checked.

Answer: D

NEW QUESTION 291
- (Topic 1)
What are two characteristics of VXLAN? (Choose two)

A. It uses VTEPs to encapsulate and decapsulate frames.
B. It has a 12-bit network identifier

C. It allows for up to 16 million VXLAN segments
D. It lacks support for host mobility
E. It extends Layer 2 and Layer 3 overlay networks over a Layer 2 underlay.

Answer: AC

NEW QUESTION 296
- (Topic 1)
An engineer must provide wireless converge in a square office. The engineer has only one AP and believes that it should be placed it in the middle of the room. Which antenna type should the engineer use?

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

Answer: D

NEW QUESTION 300
- (Topic 1)
What is a fact about Cisco EAP-FAST?
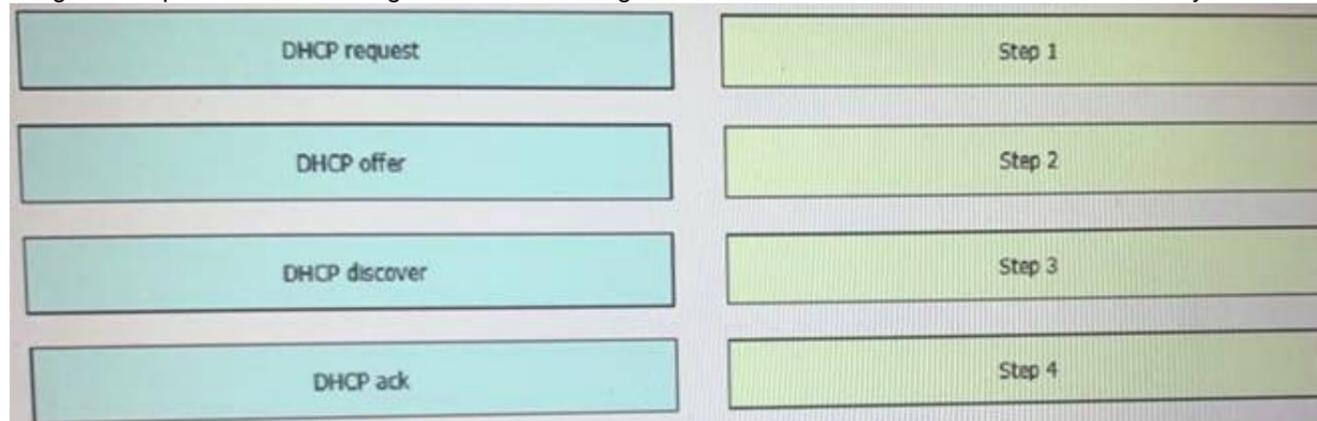
A. It does not require a RADIUS server certificate.
B. It requires a client certificate.
C. It is an IETF standard.
D. It operates in transparent mode.

Answer: A

NEW QUESTION 302
DRAG DROP - (Topic 1)
Drag and drop the DHCP messages that are exchanged between a client and an AP into the order they are exchanged on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
There are four messages sent between the DHCP Client and DHCP Server: DHCPD ISCOVER, DHCPOFFER, DHCPREQUEST and DHCPACKNOWLEDGEMENT.
This process is often abbreviated as DORA (for Discover, Offer, Request, Acknowledgement).

NEW QUESTION 304
- (Topic 1)
How is 802.11 traffic handled in a fabric-enabled SSID?

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

Answer: B

NEW QUESTION 307
- (Topic 1)
What are two differences between the RIB and the FIB? (Choose two.)

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

Answer: BE

NEW QUESTION 310
- (Topic 1)
Which characteristic distinguishes Ansible from Chef?

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

Answer: C

NEW QUESTION 312
- (Topic 1)
In a Cisco SD-Access solution, what is the role of the Identity Services Engine?

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

Answer: A

NEW QUESTION 316
- (Topic 1)

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.

Answer: A

NEW QUESTION 318
- (Topic 1)
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

Answer: A

NEW QUESTION 321
- (Topic 1)
What are two benefits of virtual switching when compared to hardware switching? (Choose two.)

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

Answer: CD

NEW QUESTION 323
- (Topic 1)
Refer to the exhibit.

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

What does the snippet of code achieve?

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

Answer: C

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

NEW QUESTION 327
- (Topic 1)
Refer to the exhibit.

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

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

Answer: AD

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

NEW QUESTION 328
- (Topic 1)
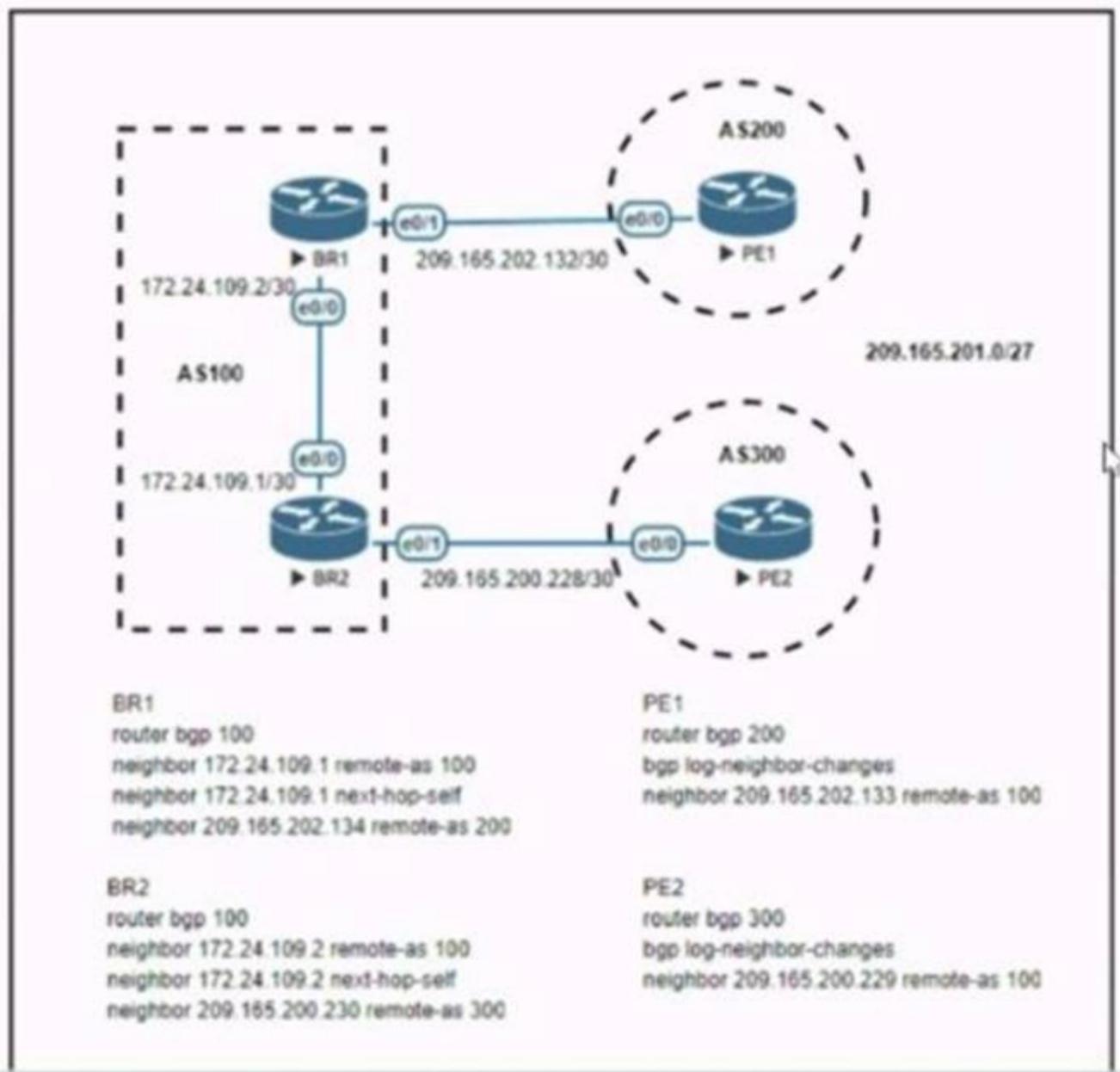
Refer to the exhibit. Which configuration change will force BR2 to reach 209 165 201 0/27 via BR1?

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

Answer: C

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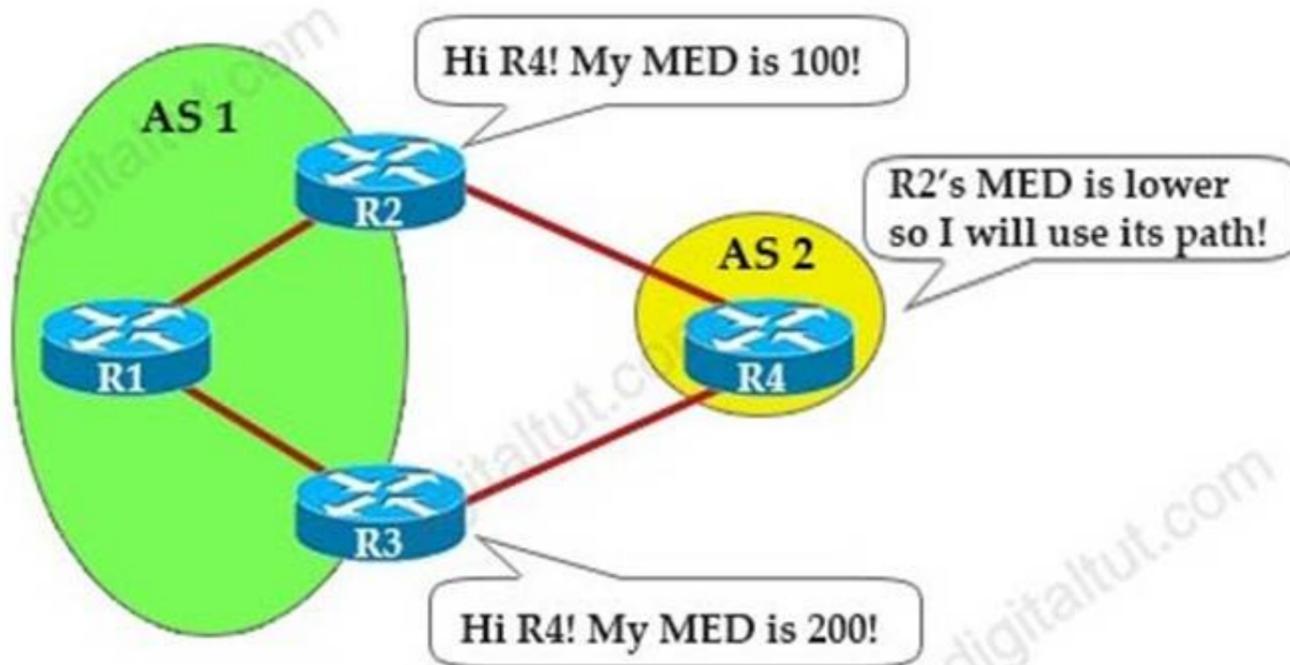
Diagrama Descripción generada automáticamenteMED Attribute:+ Optional nontransitive attribute (nontransitive means that we can only advertise MED to routers that are one AS away)+ Sent through ASes to external BGP neighbors+ Lower value is preferred (it can be considered the external metric of a route)+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

NEW QUESTION 332
- (Topic 1)
Refer to the exhibit.

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

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

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

Answer: C

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

NEW QUESTION 333
- (Topic 1)
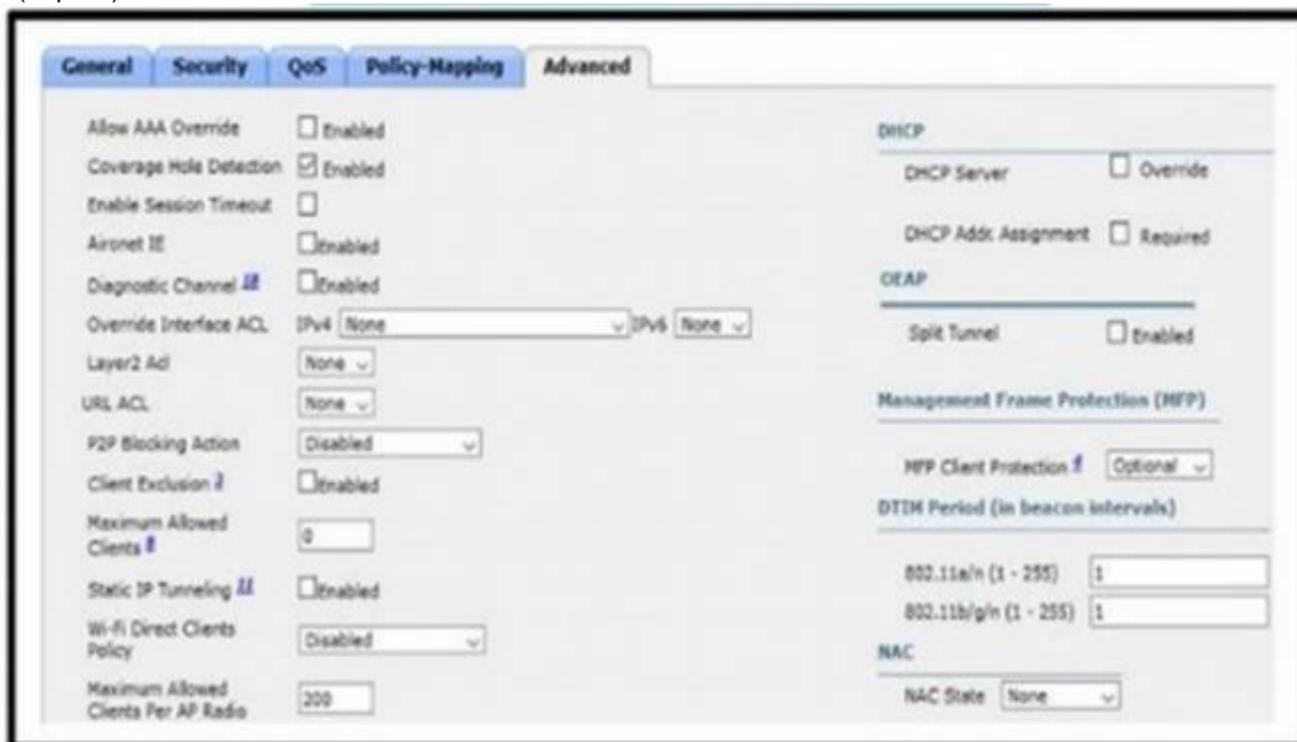
Refer to the exhibit. An engineer has configured Cisco ISE to assign VLANs to clients based on their method of authentication, but this is not working as expected. Which action will resolve this issue?

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

Answer: B

NEW QUESTION 336
- (Topic 1)
If the noise floor is -90 dBm and wireless client is receiving a signal of -75 dBm, what is the SNR?

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

Answer: A

NEW QUESTION 339
- (Topic 1)
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

Answer: BC

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

NEW QUESTION 340
- (Topic 1)

```
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

Answer: A

NEW QUESTION 345
- (Topic 1)
An engineer must configure HSRP group 300 on a Cisco IOS router. When the router is functional, it must be the must be the active HSRP router. The peer router has been configured using the default priority value. Which command set is required?
A)

standby 300 priority 110
standby 300 timers 1 110

B)

standby version 2
standby 300 priority 110
standby 300 preempt

C)

standby 300 priority 90
standby 300 preempt

D)

standby version 2
standby 300 priority 90
standby 300 preempt

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

Answer: B

NEW QUESTION 349
- (Topic 1)
Where is radio resource management performed in a cisco SD-access wireless solution?

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

Answer: C

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

NEW QUESTION 353
- (Topic 1)
How does an on-premises infrastructure compare to a cloud infrastructure?

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

Answer: D

NEW QUESTION 357
- (Topic 1)
Which TCP setting is tuned to minimize the risk of fragmentation on a GRE/IP tunnel?

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

Answer: D

Explanation:

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

NEW QUESTION 358
- (Topic 1)
What is the output of this code?

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

print(get_credentials())
```

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

Answer: D

NEW QUESTION 362
- (Topic 1)
"HTTP/1.1 204 content" is returned when cur –I –x delete command is issued. Which situation has occurred?

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

Answer: B

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

NEW QUESTION 365
- (Topic 1)
A customer requests a network design that supports these requirements:

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

Which protocol does the design include?

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

Answer: D

NEW QUESTION 370
- (Topic 1)

```
{
  "response": [
    {
      "family": "Routers",
      "interfaceCount": "12",
      "lineCardCount": "9",
      "platformId": "ASR1001-X",
      "reachabilityFailureReason": "",
      "reachabilityStatus": "Reachable",
      "hostname": "RouterASR-1",
      "macAddress": "00:c8:8b:80:bb:00",
    },
    {
      "family": "Switches and Hubs",
      "interfaceCount": "41",
      "lineCardCount": "2",
      "platformId": "C9300-24UX",
      "reachabilityFailureReason": "",
      "reachabilityStatus": "Authentication Failed",
      "hostname": "cat9000-1",
      "macAddress": "18:7b:20:67:62:80",
    },
    {
      "family": "Switches and Hubs",
      "interfaceCount": "59",
      "lineCardCount": "2",
      "platformId": "WS-C3850-48U-E",
      "reachabilityFailureReason": "",
      "reachabilityStatus": "Unreachable",
      "hostname": "cat3850-1",
      "macAddress": "cc:d8:c1:15:d2:80",
    }
  ],
  "version": "1.0"
}
```

What does the cisco DNA REST response indicate?

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

Answer: C

NEW QUESTION 371
- (Topic 1)
Refer to the exhibit.
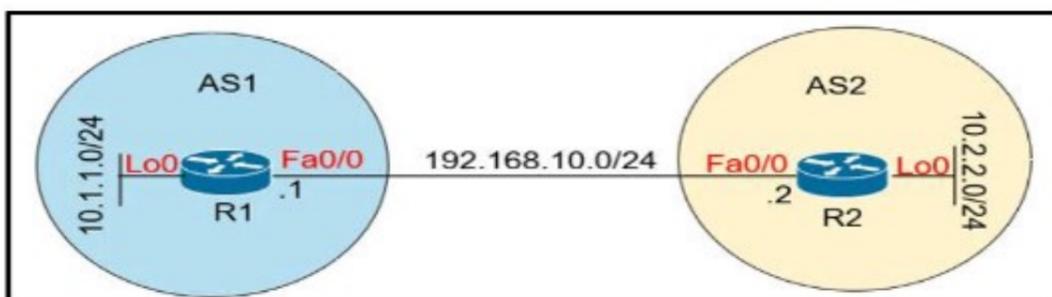
Which configuration establishes EBGP neighborship between these two directly connected neighbors and exchanges the loopback network of the two routers through BGP?
A)

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

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

B)

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

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

C)

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

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

D)

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

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

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

Answer: A

Explanation:
With BGP, we must advertise the correct network and subnet mask in the "network" command (in this case network 10.1.1.0/24 on R1 and network 10.2.2.0/24 on R2). BGP is very strict in the
routing advertisements. In other words, BGP only advertises the network which exists exactly in
the routing table. In this case, if you put the command "network x.x.0.0 mask 255.255.0.0" or
"network x.0.0.0 mask 255.0.0.0" or "network x.x.x.x mask 255.255.255.255" then BGP will not
advertise anything.
It is easy to establish eBGP neighborship via the direct link. But let's see what are required when
we want to establish eBGP neighborship via their loopback interfaces. We will need two commands:
+ the command "neighbor 10.1.1.1 ebgp-multihop 2" on R1 and "neighbor 10.2.2.2 ebgpmultihop
2" on R1. This command increases the TTL value to 2 so that BGP updates can reach the BGP neighbor which is two hops away.
+ Answer 'R1 (config) #router bgp 1
R1 (config-router) #neighbor 192.168.10.2 remote-as 2
R1 (config-router) #network 10.1.1.0 mask 255.255.255.0 R2 (config) #router bgp 2
R2 (config-router) #neighbor 192.168.10.1 remote-as 1
R2 (config-router) #network 10.2.2.0 mask 255.255.255.0 Quick Wireless Summary
Cisco Access Points (APs) can operate in one of two modes: autonomous or lightweight
+ Autonomous: self-sufficient and standalone. Used for small wireless networks.
+ Lightweight: A Cisco lightweight AP (LAP) has to join a Wireless LAN Controller (WLC) to function.
LAP and WLC communicate with each other via a logical pair of CAPWAP tunnels.
– Control and Provisioning for Wireless Access Point (CAPWAP) is an IETF standard for control
messaging for setup, authentication and operations between APs and WLCs. CAPWAP is similar to
LWAPP except the following differences:
+CAPWAP uses Datagram Transport Layer Security (DTLS) for authentication and encryption to
protect traffic between APs and controllers. LWAPP uses AES.
+ CAPWAP has a dynamic maximum transmission unit (MTU) discovery mechanism.
+ CAPWAP runs on UDP ports 5246 (control messages) and 5247 (data messages) An LAP operates in one of six different modes:
+ Local mode (default mode): measures noise floor and interference, and scans for intrusion
detection (IDS) events every 180 seconds on unused channels
+ FlexConnect, formerly known as Hybrid Remote Edge AP (H-REAP), mode: allows data traffic
to be switched locally and not go back to the controller. The FlexConnect AP can perform standalone
client authentication and switch VLAN traffic locally even when it's disconnected to the WLC (Local
Switched). FlexConnect AP can also tunnel (via CAPWAP) both user wireless data and control traffic to
a centralized WLC (Central Switched).
+ Monitor mode: does not handle data traffic between clients and the infrastructure. It acts like a
sensor for location-based services (LBS), rogue AP detection, and IDS
+ Rogue detector mode: monitor for rogue APs. It does not handle data at all.
+ Sniffer mode: run as a sniffer and captures and forwards all the packets on a particular
channel to a remote machine where you can use protocol analysis tool (Wireshark, Airopeek, etc) to review the packets and diagnose issues. Strictly used for
troubleshooting purposes.
+ Bridge mode: bridge together the WLAN and the wired infrastructure together.
Mobility Express is the ability to use an access point (AP) as a controller instead of a real WLAN
controller. But this solution is only suitable for small to midsize, or multi-site branch locations where
you might not want to invest in a dedicated WLC. A Mobility Express WLC can support up to 100 Aps

NEW QUESTION 373
- (Topic 4)
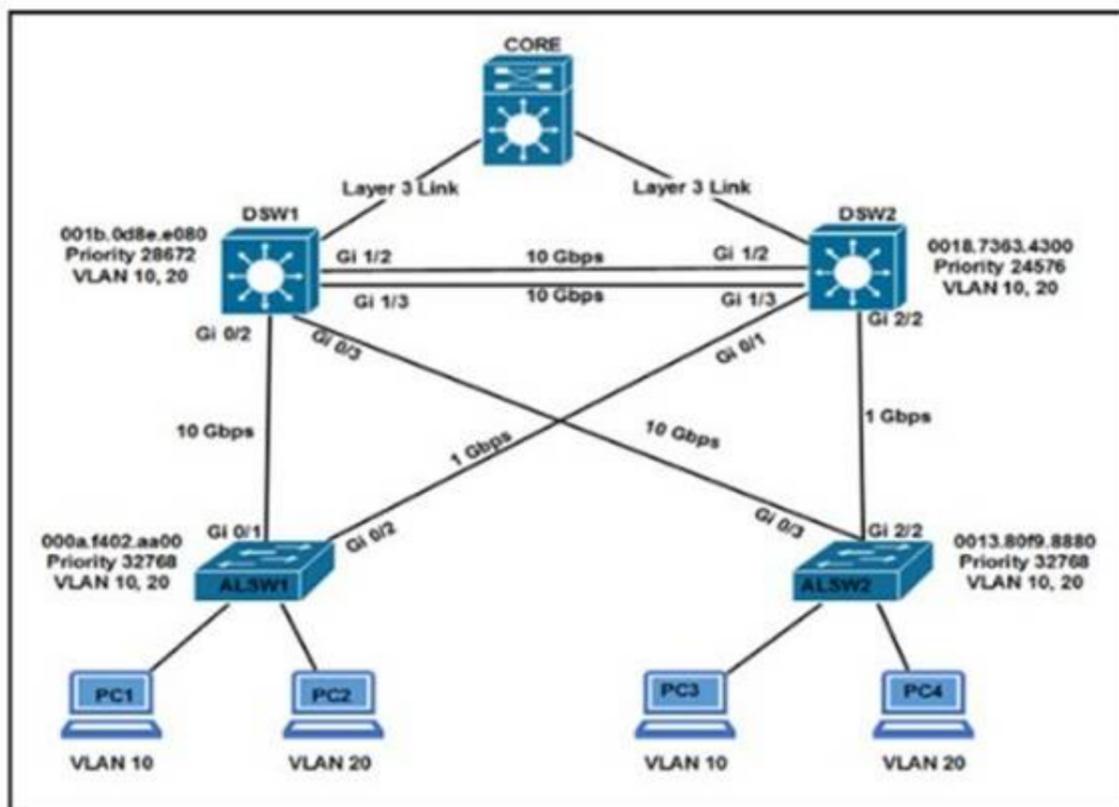
Refer to the exhibit. Which two commands ensure that DSW1 becomes root bridge for VLAN 10? (Choose two)

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

Answer: CD

Explanation:
 Ref: Scaling Networks v6 Companion Guide
"STP
…
Extended System ID
…
Bridge Priority
The bridge priority is a customizable value that can be used to influence which switch becomes the root bridge. The switch with the lowest priority, which implies the lowest BID, becomes the root bridge because a lower priority value takes precedence.
…
The default priority value for all Cisco switches is the decimal value 32768. The range is 0 to 61440, in increments of 4096. Therefore, valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. A bridge priority of 0 takes precedence over all other bridge priorities. All other values are rejected.

NEW QUESTION 374
- (Topic 4)
What is a characteristic of a traditional WAN?

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

Answer: D

NEW QUESTION 376
- (Topic 4)
What is a client who is running 802.1x for authentication reffered to as?

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

Answer: A

NEW QUESTION 379
- (Topic 4)
Which two features are available only in next-generation firewalls? (Choose two.)

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

E. packet filtering

Answer: CD

NEW QUESTION 380
- (Topic 4)
Refer to the exhibit.
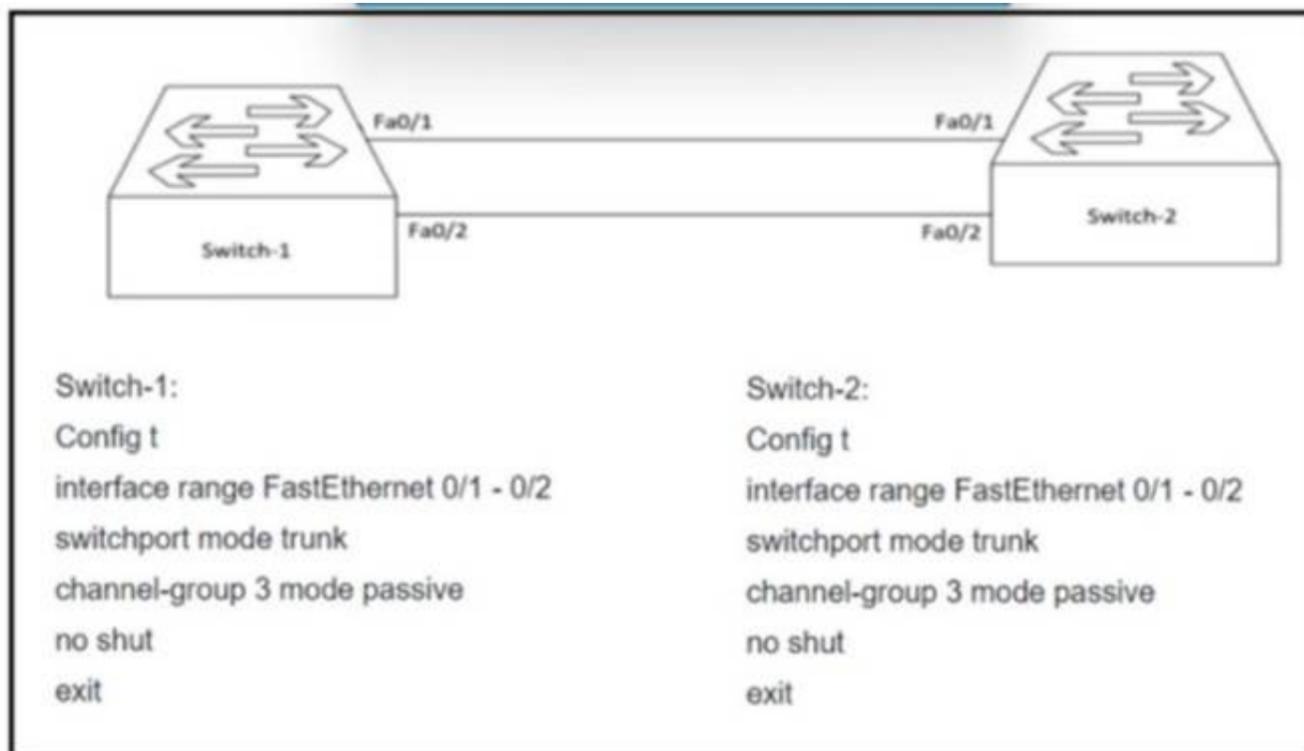
An LACP port channel is configured between Switch-1 and Switch-2, but It falls to come up. Which action will resolve the issue?

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

Answer: A

NEW QUESTION 384
- (Topic 4)
Which device, in a LISP routing architecture, receives and de-encapsulates LISP traffic for endpoints within a LISP-capable site?

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

Answer: B

NEW QUESTION 385
- (Topic 4)
An engineer applies this EEM applet to a router:

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

What does the applet accomplish?

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

Answer: B

NEW QUESTION 389

- (Topic 4)
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.

Answer: D

NEW QUESTION 390
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the routing protocol they describe on the right

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 393
- (Topic 4)
What do Chef and Ansible have in common?

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

Answer: B

NEW QUESTION 398
- (Topic 4)

```
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 me configuration What toes the output confirm?

A. The first pocket triggered NAT to add an entry to the NAT table
B. R1 is configured with NAT overload parameters.
C. A Telnet session from 160.1.1.1 to 10.1.1.10 has been initiated.
D. R1 a configured win PAT overload parameters

Answer: A

NEW QUESTION 403
- (Topic 4)
When a branch location loses connectivity, which Cisco FlexConnect state rejects new users but allows existing users to function normally?

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

Answer: A

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

NEW QUESTION 407
- (Topic 4)
When a DNS host record is configured for a new Cisco AireOS WLC, which hostname must be added to allow APs to successfully discover the WLC?

A. CONTROLLER-CAPWAP-CISCO
B. CISCO-CONTROLLER-CAPWAP
C. CAPWAP-CISCO-CONTROLLER
D. CISCO-CAPWAP-CONTROLLER

Answer: D

NEW QUESTION 412
DRAG DROP - (Topic 4)
An engineer must create a script to append and modify device entries in a JSON-formatted file. The script must work as follows:
? Until interrupted from the keyboard, the script reads in the hostname of a device, its management IP address, operating system type, and CLI remote access protocol.
? After being interrupted, the script displays the entered entries and adds them to the JSON-formatted file, replacing existing entries whose hostname matches. The contents of the JSON-formatted file are as follows:

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

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

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

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

Options:
- while True:
- except
- import json
- File.open()
- File.close()
- File = open

A. Mastered
B. Not Mastered

Answer: A

Explanation:

```
import json

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

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

Draggable blocks:
- while True:
- except
- import json
- File.open()
- File.close()
- File = open

NEW QUESTION 414
- (Topic 4)
Which authorization framework gives third-party applications limited access to HTTP services?

A. iPsec
B. Basic Auth
C. GRE
D. OAuth 2.0

Answer: D

NEW QUESTION 415
- (Topic 4)
Refer to the exhibit.
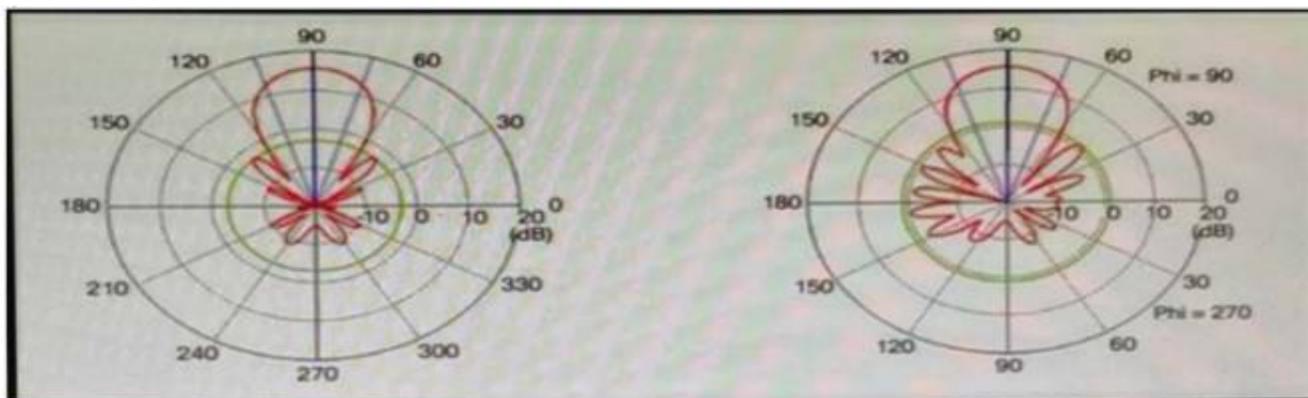
Which type of antenna is shown on the radiation patterns?

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

Answer: A

NEW QUESTION 419
- (Topic 4)
Which Cisco WLC feature allows a wireless device to perform a Layer 3 roam between two separate controllers without changing the client IP address?

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

Answer: B

NEW QUESTION 421
- (Topic 4)

```
<?xml version-"1.0"?>

<nc:rpc message-id-"101" xmlns:nc-"urn:ietf:params:xml:ns:netconf:base:1.0">

    <nc:get>

        <nc:filter type="subtree">

            <native xmlns-"http://cisco.com/ns/yang/ned/ios">

                <interface>

                 <GigabitEthernet>

                  <name>1</name>

                    <ip></ip>

                </GigabitEthernet>

              </interface>

            </native>

        </nc:filter>

    </nc:get>

</nc:rpc>

]]>]]>
```

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

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

Answer: A

NEW QUESTION 426
- (Topic 4)
A script contains the statement "while loop != 999:" Which value terminates the loop?

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

Answer: A

NEW QUESTION 427
- (Topic 4)
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.

Answer: D

NEW QUESTION 428
- (Topic 4)
What is a benefit of using segmentation with TrustSec?

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

Answer: B

NEW QUESTION 431
- (Topic 4)

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

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

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

Answer: B

NEW QUESTION 433
- (Topic 4)
Which function does a virtual switch provide?

A. CPU context switching (or multitasking between virtual machines
B. RAID storage for virtual machines
C. emulation of power for virtual machines.
D. connectivity between virtual machines

Answer: D

Explanation:
This is because a virtual switch is a software-based switch that operates at the data link layer of the OSI model and provides connectivity between virtual machines that are running on the same physical host or different hosts. A virtual switch can also connect virtual machines to external networks, such as the Internet or a local area network, by using physical network adapters on the host. A virtual switch can perform the same functions as a physical switch, such as learning MAC addresses, forwarding frames, and applying VLANs. The source of this answer is the Cisco ENCOR v1.1 course, module 9, lesson 9.1: Implementing Network Virtualization.

NEW QUESTION 436
- (Topic 4)
A company hires a network architect to design a new OTT wireless solution within a Cisco
SD-Access Fabric wired network. The architect wants to register access points to the WLC to centrally switch the traffic. Which AP mode must the design include?

A. Bridge
B. Fabric
C. FlexConnect
D. local

Answer: D

NEW QUESTION 440
- (Topic 4)
A customer wants to connect a device to an autonomous Cisco AP configured as a WGB. The WGB is configured properly: however, it fails to associate to a CAPWAP- enabled AP. Which change must be applied in the advanced WLAN settings to resolve this issue?

A. Enable Aironet IE.
B. Enable passive client.
C. Disable AAA override.
D. Disable FlexConnect local switching.

Answer: A

NEW QUESTION 444
- (Topic 4)
An engineer uses the Design workflow to create a new network infrastructure in Cisco DNA Center. How is the physical network device hierarchy structured?

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

Answer: B

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

NEW QUESTION 445
- (Topic 4)
Which two steps are required for a complete Cisco DNA Center upgrade? (Choose two.)

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

Answer: DE

NEW QUESTION 446
- (Topic 4)

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

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

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

Answer: B

NEW QUESTION 451
- (Topic 4)
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

Save   Cancel

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

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

Answer: A

NEW QUESTION 452
- (Topic 4)
In a wireless network environment, what is calculated using the numerical values of the transmitter power level, cable loss, and antenna gain?

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

Answer: B

NEW QUESTION 453
- (Topic 4)
By default, which virtual MAC address does HSRP group 15 use?

A. 05:5e:ac:07:0c:0f
B. c0:42:34:03:73:0f
C. 00:00:0c:07:ac:0f
D. 05:af:1c:0f:ac:15

Answer: C

Explanation:
interface Ethernet0/0.100 encapsulation dot1Q 100
ip address 10.0.111.1 255.255.255.0
standby 15 ip 10.0.111.254
!
cisco(config-subif)#do s stand Ethernet0/0.100 - Group 15
State is Speak
Virtual IP address is 10.0.111.254 Active virtual MAC address is unknown
Local virtual MAC address is 0000.0c07.ac0f (v1 default) Hello time 3 sec, hold time 10 sec
Next hello sent in 1.200 secs Preemption disabled
Active router is unknown Standby router is unknown

NEW QUESTION 455
- (Topic 4)
In lhe Cisco DNA Center Image Repository, what is a golden image?

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

Answer: B

NEW QUESTION 456
- (Topic 4)
Which JSON script is properly formatted?
A)

```
[
    "Session":{

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

B)

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

C)

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

D)

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

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

Answer: A

Explanation:
Option A is the properly formatted JSON script. JSON (JavaScript Object Notation) is a standard text-based format for representing structured data based on JavaScript object syntax. It is commonly used for transmitting data in web applications (e.g., sending some data from the server to the client, so it can be displayed on a web page, or vice versa). The JSON syntax rules are as follows12:
? Data is in name/value pairs, separated by commas. A name/value pair consists of a field name (in double quotes), followed by a colon, followed by a value: "name": "value".
? Curly braces hold objects. An object can contain multiple name/value pairs: {"name": "value", "name": "value", ...}.
? Square brackets hold arrays. An array can contain multiple values, separated by commas: ["value", "value", ...].
? Values can be strings (in double quotes), numbers, booleans (true or false), null, objects, or arrays.
Option A follows these rules and is a valid JSON script. It defines an object with four name/value pairs: "name", "age", "hobbies", and "address". The value of "name" is a string, the value of "age" is a number, the value of "hobbies" is an array of strings, and the value of "address" is another object with two name/value pairs: "city" and "country". The object is enclosed in curly braces and the name/value pairs are separated by commas.
Option B is not a valid JSON script because it uses single quotes instead of double quotes for the field names and string values. JSON requires double quotes for strings12.
Option C is not a valid JSON script because it does not use commas to separate the name/value pairs. JSON requires commas to separate the data elements within an object or an array12.
Option D is not a valid JSON script because it uses a semicolon instead of a colon to separate the field name and the value. JSON requires a colon to separate the name and the value in a name/value pair12. References: 1: JSON Introduction, 2: JSON Syntax

NEW QUESTION 459
- (Topic 4)
A company recently rearranged some users' workspaces and moved several users to different desks. The network administrator receives a report that all of the users who were moved are having connectivity issues. Which of the following is the most likely reason?

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

Answer: A

Explanation:
This is because ports can become error disabled when they detect certain errors or violations on the network, such as a loop, a security breach, or a duplex mismatch. When a port is error disabled, it shuts down and stops forwarding traffic until it is manually re-enabled by the administrator. The users who were moved to different desks may have plugged their devices into ports that were configured with different settings or security policies than their original ports, and this may

have triggered the error disable state. The source of this answer is the Cisco ENCOR v1.1 course, module 3, lesson 3.3: Implementing EtherChannel.

NEW QUESTION 462
- (Topic 4)
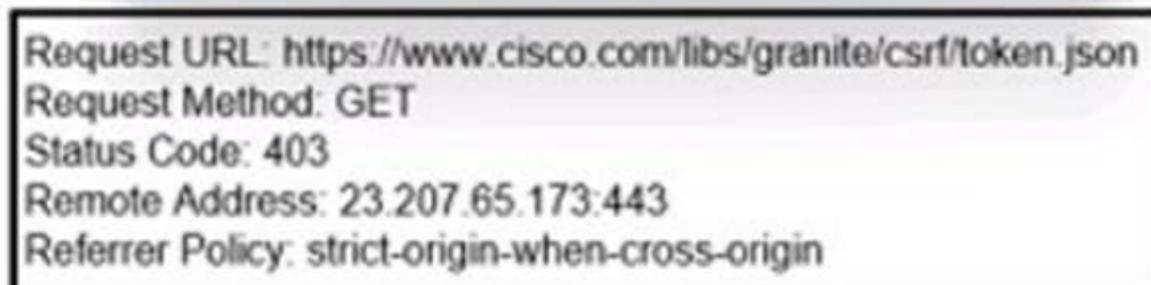In which two ways does the routing protocol OSPF differ from EIGRP? (Choose two.)

A. OSPF supports an unlimited number of hop
B. EIGRP supports a maximum of 255 hops.
C. OSPF provides shorter convergence time than EIGRP.
D. OSPF is distance vector protoco
E. EIGRP is a link-state protocol.
F. OSPF supports only equal-cost load balancin
G. EIGRP supports unequal-cost load balancing.
H. OSPF supports unequal-cost load balancin
I. EIGRP supports only equal-cost load balancing.

Answer: AD

NEW QUESTION 464
- (Topic 4)
Which QoS feature uses the IP Precedence bits in the ToS field of the IP packet header to partition traffic into different priority levels?

A. marking
B. shaping
C. policing
D. classification

Answer: D

NEW QUESTION 467
- (Topic 4)
A customer has a pair of Cisco 5520 WLCs set up in an SSO cluster to manage all APs. Guest traffic is anchored to a Cisco 3504 WLC located in a DMZ. Which action is needed to ensure that the EoIP tunnel remains in an UP state in the event of failover on the SSO cluster?

A. Configure back-to-back connectivity on the RP ports.
B. Enable default gateway reachability check.
C. Use the same mobility domain on all WLCs.
D. Use the mobility MAC when the mobility peer is configured.

Answer: B

NEW QUESTION 471
- (Topic 4)
A VoIP phone is plugged in to a port but cannot receive calls. Which of the following needs to be done on the port to address the issue?

A. Trunk all VLANs on the port.
B. Configure the native VLAN.
C. Tag the traffic to voice VLAN.
D. Disable VLANs.

Answer: C

Explanation:
This is because the voice VLAN is a special VLAN that is used to separate the voice traffic from the data traffic on a switch port. The voice VLAN allows the VoIP phone to communicate with the voice server and receive calls. The voice VLAN is usually configured with a higher priority than the data VLAN to ensure the quality of service for the voice traffic. The voice VLAN is tagged with a VLAN ID that is different from the data VLAN ID. The switch port must be configured to tag the traffic to the voice VLAN, either manually or automatically using protocols such as CDP or LLDP. The source of this answer is the Cisco ENCOR v1.1 course, module 3, lesson 3.2: Implementing VLANs and Trunks.

NEW QUESTION 475
DRAG DROP - (Topic 4)
Drag and drop the code snippets from the bottom onto the blanks in the script to convert a Python object into a JSON string. Not all options are used.

```
import json

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

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

print(obj)
```

JSONEncoder
.encode
data
JSONDecoder
decode

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 480
- (Topic 4)
When is GLBP preferred over HSRP?

A. When encrypted helm are required between gateways h a single group.
B. When the traffic load needs to be shared between multiple gateways using a single virtual IP.
C. When the gateway routers are a mix of Cisco and non-Cisco routers
D. When clients need the gateway MAC address lo Be the same between multiple gateways

Answer: B

NEW QUESTION 484
- (Topic 4)
An engineer must configure Interface and sensor monitoring on a router. The NMS server is located in a trusted zone with IP address 10.15.2.19. Communication between the router and the NMS server must be encrypted and password-protected using the most secure algorithms. Access must be allowed only for the NMS server and with the minimum permission levels needed. Which configuration must the engineer apply?
A)

```
ip access-list standard nms
   permit 10.15.2.19 255.255.255.255

snmp-server view ro cisco included

snmp-server view ro ifEntry included

snmp-server group nms v3 priv read ro access nms
   snmp-server user user1 nms v3 auth 3des Password1 pri aes 192  Password123
```

B)

```
ip access-list standard nms
   permit 10.15.2.19 0.0.0.0

snmp-server view rw iso included

snmp-server view rw ifEntry included

snmp-server group nms v3 auth write rw access nms
   snmp-server user user1 nms v3 auth des Password1 pri des Password123
```

C)

```
ip access-list  extended nms
   permit 1 host 10.15.2.19  any

snmp-server view ro internet included

snmp-server view ro ifEntry included

snmp-server group nms v3 priv notify ro access nms
snmp-server user user1 nms v3 encrypted auth md5 Password1 pri 3des  Password123
```

D)

```
ip access-list standard nms
   permit 10.15.2.19 0.0.0.0

snmp-server view ro iso included
```

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

Answer: A

Explanation:
 Option A is the correct configuration to apply interface and sensor monitoring on a router with the given requirements. This option uses SNMPv3, which is the most secure version of SNMP that supports encryption and authentication. The configuration steps are as follows12:
? Create an access list named nms that permits only the NMS server with IP address 10.15.2.19 to access the router: ip access-list standard nms and permit 10.15.2.19 0.0.0.0.
? Create a view named rw that includes all the SNMP objects: snmp-server view rw included.
? Create a group named nms that uses SNMPv3 with privacy (encryption) and authentication, and assigns the view rw and the access list nms to the group: snmp-server group nms v3 priv read rw access nms.
? Create a user named nms that belongs to the group nms and uses DES for authentication and AES for encryption, with the passwords despass and aespass respectively: snmp-server user nms nms v3 auth des despass priv aes 192 aespass.
Option B is incorrect because it does not use encryption for SNMP communication, which is required by the question. The noauth keyword in the snmp-server group command means that no authentication or encryption is used, which makes the SNMP packets vulnerable to eavesdropping and tampering1.
Option C is incorrect because it does not use the most secure algorithms for SNMP communication, which is required by the question. The md5 and des keywords in the snmp-server user command mean that MD5 and DES are used for authentication and encryption respectively, which are considered weak and outdated algorithms. AES and SHA are recommended instead1.
Option D is incorrect because it does not restrict the access to the NMS server only, which is required by the question. The snmp-server community command creates a community string that acts as a password for SNMP access, but it does not specify an access list to limit the source IP addresses that can use the community string. Therefore, any device that knows the community string can access the router via SNMP1. References: 1: Configuring SNMPv3, 2: SNMP Configuration Guide, Cisco IOS XE Gibraltar 16.12.x

NEW QUESTION 488
- (Topic 4)

```
>traceroute www.crmABC.com

Tracing route to www.crmABC.com [192.168.100.1]

1    3ms    5ms    3ms    10.10.10.1

2    4ms    6ms    4ms    10.100.100.1

3    4ms    6ms    4ms    10.100.200.1


4    4ms    6ms    4ms    10.100.100.1

5    4ms    6ms    4ms    10.100.200.1

6    4ms    6ms    4ms    10.100.100.1

7    4ms    6ms    4ms    10.100.200.1

<output truncated>
```

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

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

Answer: C

NEW QUESTION 493
- (Topic 4)
Refer to the exhibit.

```
R1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 65001
<output omitted>
Neighbor          V        AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.50.2      4     65002     10        9        5    0    0 00:04:56       2

R1#show ip bgp 2.2.2.2
BGP routing table entry for 2.2.2.2/32, version 2
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
  65002
     192.168.50.2 from 192.168.50.2 (172.20.0.2)
       Origin IGP, metric 0, localpref 100, valid, external, best
       rx pathid: 0, tx pathid: 0x0

  <CONFIGURATION CHANGE MADE>

R1#show ip bgp 2.2.2.2
BGP routing table entry for 2.2.2.2/32, version 6
Paths: (1 available, best #1, table default, RIB-failure(17))
  Not advertised to any peer
  Refresh Epoch 1
  65002
     192.168.50.2 from 192.168.50.2 (172.20.0.2)
       Origin IGP, metric 0, localpref 100, valid, external, best
       rx pathid: 0, tx pathid: 0x0
```

R1 has a BGP neighborship with a directly connected router on interface Gi0/0. Which command set is applied between the iterations of show ip bgp 2.2.2.2?

A. R1(config)#router bgp 65001R1(config-router)#neighbor 192.168.50.2 shutdown
B. R1(config)#router bgp 65002R1(config-router)#neighbor 192.168.50.2 shutdown
C. R1(config)#no ip route 192.168.50.2 255.255.255.255 Gi0/0
D. R1(config)#ip route 2.2.2.2 255.255.255.255 192.168.50.2

Answer: D

NEW QUESTION 496
- (Topic 4)

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

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

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

Answer: A

NEW QUESTION 501
- (Topic 4)

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**

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

Answer: C

NEW QUESTION 505
- (Topic 4)
Which tool is used in Cisco DNA Center to build generic configurations that are able to be applied on device with similar network settings?

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

Answer: B

NEW QUESTION 509
- (Topic 4)
Refer to the exhibit.

```
R2#
*May 27 15:33:59.642: OSPF-1 ADJ   Gi1: Send DBD to 192.168.201.137 seq 0xDE7 opt 0x52 flag 0x7 len 32
*May 27 15:33:59.642: OSPF-1 ADJ   Gi1: Retransmitting DBD to 192.168.201.137 [15]
*May 27 15:33:59.645: OSPF-1 ADJ   Gi1: Rcv DBD from 192.168.201.137 seq 0xDE7 opt 0x52 flag 0x2 len 112  mtu 9100 state EXSTART
```

The OSPF neighborship fails between two routers. What is the cause of this issue?

A. The OSPF router ID is missing on this router.
B. The OSPF process is stopped on the neighbor router.
C. There is an MTU mismatch between the two routers.
D. The OSPF router ID is missing on the neighbor router.

Answer: C

Explanation:
cisco_R2(config-subif)#do debug ip osp adj OSPF adjacency debugging is on
cisco_R2(config-subif)#ip mtu 1111 <<<<<<<<<<<<<<<< cisco_R2(config-subif)#
cisco_R2(config-subif)# cisco_R2(config-subif)#do clear ip ospf
!!!debug shows this: cisco_R2(config-subif)#
*Dec 23 13:02:27.164: OSPF-1 ADJ Et0/0.10: Rcv DBD from 6.6.6.6 seq 0x19FD opt 0x52
flag 0x7 len 32 mtu 1500 state EXSTART <<<<<<<<<<<<<
*Dec 23 13:02:27.164: OSPF-1 ADJ Et0/0.10: Nbr 6.6.6.6 has larger interface MTU
<<<<<<<<<
*Dec 23 13:02:27.164: OSPF-1 ADJ Et0/0.10: Rcv DBD from 6.6.6.6 seq 0x26B opt 0x52
flag 0x2 len 112 mtu 1500 state EXSTART
*Dec 23 13:02:27.164: OSPF-1 ADJ Et0/0.10: Nbr 6.6.6.6 has larger interface MTU
*Dec 23 13:02:27.395: OSPF-1 ADJ Et0/0.10: Rcv DBD from 6.6.6.6 seq 0x26B opt 0x52
flag 0x2 len 112 mtu 1500 state EXSTART
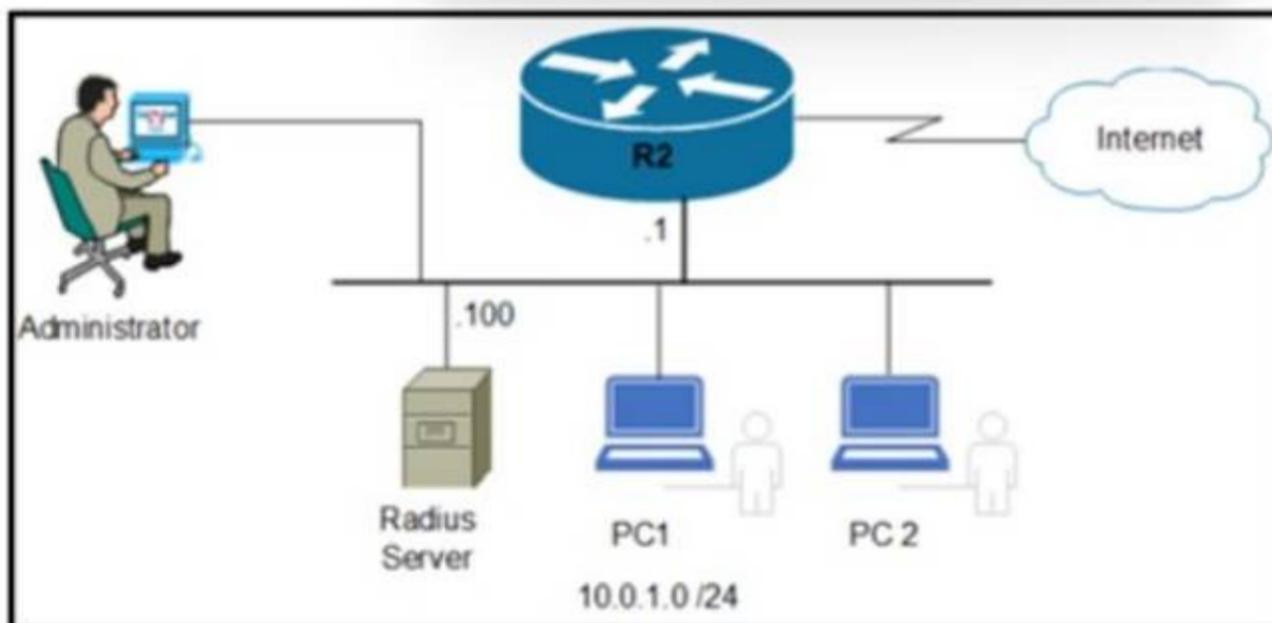
NEW QUESTION 511
- (Topic 4)

Refer to the exhibit. An engineer must save the configuration of router R2 using the NETCONF protocol. Which script must be used?

○ <?xml version="1.0" encoding="utf-8"?>
    <rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
       <cisco-ia:reset xmlns:cisco-ia="http://cisco.com/yang/cisco-ia">
       <cisco-ia:reinitialize>true</cisco-ia:reinitialize>
      </cisco-ia:reset>
    </rpc>

○ <?xml version="1.0" encoding="utf-8"?>
    <rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
     <get>
      <filter type="subtree">
       <ncm:netconf-state xmlns:ncm="urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring">
        <ncm:capabilities/>
       </ncm:netconf-state>
      </filter>
     </get>
    </rpc>

○ <?xml version="1.0" encoding="utf-8"?>
    <rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
     <cisco-ia:save-config xmlns:cisco-ia="http://cisco.com/yang/cisco-ia"/>
    </rpc>

○ <?xml version="1.0" encoding="utf-8"?>
    <rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
      <cisco-ia:sync-from xmlns:cisco-ia="http://cisco.com/yang/cisco-ia"></cisco-ia:sync-from>
    </rpc>

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

Answer: C

NEW QUESTION 513
- (Topic 4)
Which JSON script is properly formatted?
A)


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

B)

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

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

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

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

Answer: A

Explanation:
 Option A is the properly formatted JSON script. JSON (JavaScript Object Notation) is a standard text-based format for representing structured data based on JavaScript object syntax. It is commonly used for transmitting data in web applications (e.g., sending some data from the server to the client, so it can be displayed on a web page, or vice versa). The JSON syntax rules are as follows12:
? Data is in name/value pairs, separated by commas. A name/value pair consists of a field name (in double quotes), followed by a colon, followed by a value: "name": "value".
? Curly braces hold objects. An object can contain multiple name/value pairs: {"name": "value", "name": "value", ...}.
? Square brackets hold arrays. An array can contain multiple values, separated by commas: ["value", "value", ...].
? Values can be strings (in double quotes), numbers, booleans (true or false), null, objects, or arrays.
Option A follows these rules and is a valid JSON script. It defines an object with four name/value pairs: "name", "age", "hobbies", and "address". The value of "name" is a string, the value of "age" is a number, the value of "hobbies" is an array of strings, and the value of "address" is another object with two name/value pairs: "city" and "country". The object is enclosed in curly braces and the name/value pairs are separated by commas.
Option B is not a valid JSON script because it uses single quotes instead of double quotes for the field names and string values. JSON requires double quotes for strings12.
Option C is not a valid JSON script because it does not use commas to separate the name/value pairs. JSON requires commas to separate the data elements within an object or an array12.
Option D is not a valid JSON script because it uses a semicolon instead of a colon to separate the field name and the value. JSON requires a colon to separate the name and the value in a name/value pair12. References: 1: JSON Introduction, 2: JSON Syntax

NEW QUESTION 516
DRAG DROP - (Topic 4)
Drag and drop the code snippets from the bottom onto the blanks in the Python script to convert a Python object into a JSON string. Not all options are used.

```
import [        ]

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

json_string = [          ] (data)

print( [        ] )
```

| model |
| json.loads |
| json |
| json_string |
| json.dumps |

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 517
- (Topic 4)
Refer to the exhibit. What is the result of this Python code?

A. 1
B. 7
C. 7.5

Answer: D

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

NEW QUESTION 519
- (Topic 4)
Users have reported an issue connecting to a server over the network. A workstation was recently added to the network and configured with a shared USB printer. Which of the following is most likely causing the issue?

A. The switch is oversubscribed and cannot handle the additional throughput.
B. The printer is tying up the server with DHCP discover messages.
C. The web server's back end was designed for only single-threaded applications.
D. The workstation was configured with a static IP that is the same as the server.

Answer: D

Explanation:
 The workstation was configured with a static IP that is the same as the server. This is because if two devices on the same network have the same IP address, they will cause an IP address conflict, which will prevent them from communicating with other devices on the network. The users who were moved to different desks may have been assigned static IP addresses that were not updated after the move, and they may have accidentally used the same IP address as the server. The source of this answer is the Cisco ENCOR v1.1 course, module 3, lesson 3.1: Implementing IPv4 and IPv6 Addressing.

NEW QUESTION 524
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your 350-401 Exam with Our Prep Materials Via below:

https://www.certleader.com/350-401-dumps.html