

**350-401**

### Normal Questions

#### QUESTION 1

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

- A. Connects endpoints to the fabric and forwards their traffic.
- B. Encapsulates end-user data traffic into LISP.
- C. Connects the SD-Access fabric to another fabric or external Layer 3 networks.
- D. Provides reachability between border nodes in the fabric underlay.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 2

Refer to the exhibit.

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

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

Which privilege level is assigned to VTY users?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 3

What is the difference between a RIB and a FIB?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 4**

Which requirement for an Ansible-managed node is true?

- A. It must have an SSH server running.
- B. It must be a Linux server or a Cisco device.
- C. It must support ad hoc commands.
- D. It must have an Ansible Tower installed.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The above does not include special case where you use Ansible to connect to localhost and ask the localhost to make telnet connection to the device node for sending commands.

**QUESTION 5**

A client device fails to see the enterprise SSID, but other client devices are connected to it.

What is the cause of this issue?

- A. The client has incorrect credentials stored for the configured broadcast SSID.
- B. The hidden SSID was not manually configured on the client.
- C. The broadcast SSID was not manually configured on the client.
- D. The client has incorrect credentials stored for the configured hidden SSID.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 6**

Which two descriptions of FlexConnect mode for Cisco APs are true? (Choose two.)

- A. APs that operate in FlexConnect mode cannot detect rogue APs.
- B. When connected to the controller, FlexConnect APs can tunnel traffic back to the controller.
- C. FlexConnect mode is used when the APs are set up in a mesh environment and used to bridge between each other.
- D. FlexConnect mode is a feature that is designed to allow specified CAPWAP-enabled APs to exclude themselves from managing data traffic between clients and infrastructure.
- E. FlexConnect mode is a wireless solution for branch office and remote office deployments.

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 7**

Which OSPF network types are compatible and allow communication through the two peering devices?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

They are compatible since both are using the DR mechanism. However additional configuration settings e.g. tuning the timers are needed before they can form neighboring.

**QUESTION 8**

Which NGFW mode blocks flows crossing the firewall?

- A. tap
- B. inline
- C. passive
- D. inline tap

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 9**

Which statement about route targets is true when using VRF-Lite?

- A. Route targets control the import and export of routes into a customer routing table.
- B. When BGP is configured, route targets are transmitted as BGP standard communities.
- C. Route targets allow customers to be assigned overlapping addresses.
- D. Route targets uniquely identify the customer routing table.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 10**

How does Cisco TrustSec enable more flexible access controls for dynamic networking environments and data centers?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 11**

Refer to the exhibit.

```
R1#debug ip ospf hello
R1#debug condition interface Fa0\1
Condition 1 Set
```

Which statement about the OSPF debug output is true?

- A. The output displays OSPF hello messages which router R1 has sent or received on interface Fa0/1.
- B. The output displays all OSPF messages which router R1 has sent or received on all interfaces.
- C. The output displays all OSPF messages which router R1 has sent or received on interface Fa0/1.
- D. The output displays OSPF hello and LSACK messages which router R1 has sent or received.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 12**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 13**

Which two protocols are used with YANG data models? (Choose two.)

- A. TLS
- B. RESTCONF
- C. SSH
- D. NETCONF
- E. HTTPS

**Correct Answer:** BD

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 14**

Which HTTP status code is the correct response for a request with an incorrect password applied to a REST API session?

- A. HTTP Status Code: 200
- B. HTTP Status Code: 302
- C. HTTP Status Code: 401
- D. HTTP Status Code: 504

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 15**

The login method is configured on the VTY lines of a router with these parameters:

- The first method for authentication is TACACS
- If TACACS is unavailable, login is allowed without any provided credentials

Which configuration accomplishes this task?

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

**R1#sh run | section vty**

```
line vty 0 4
```

**R1#sh run | include username**

R1#

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

**R1#sh run | section vty**

```
line vty 0 4
```

```
    transport input none
```

R1#

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

**R1#sh run | section vty**

```
line vty 0 4
```

```
    password 7 02050D480809
```

**R1#sh run | include username**

R1#

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

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

**R1#sh run | include username**

**R1#**

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**  
Unless you are configuring a default login authentication list (e.g. answer D), otherwise you need to apply the list to line vty before it can be effective.

**QUESTION 16**

Which statement about multicast RPs is true?

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

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**  
After starting, Shortest Path Tree (SPF) will be formed between source and receivers.

**QUESTION 17**

To increase total throughput and redundancy on the links between the wireless controller and switch, the customer enabled LAG on the wireless controller.

Which EtherChannel mode must be configured on the switch to allow the WLC to connect?

- A. Active
- B. Passive
- C. On
- D. Auto

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 18**

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

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

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 19**

An engineer configures a WLAN with fast transition enabled. Some legacy clients fail to connect to this WLAN.

Which feature allows the legacy clients to connect while still allowing other clients to use fast transition based on their OUIs?

- A. over the DS
- B. 802.11k

- C. adaptive R
- D. 802.11v

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 20**

Which exhibit displays a valid JSON file?

- A. {  
    "hostname": "edge\_router\_1"  
    "interfaces": {  
        "GigabitEthernet1/1"  
        "GigabitEthernet1/2"  
        "GigabitEthernet1/3"  
    }  
}
- B. {  
    "hostname": "edge\_router\_1",  
    "interfaces": {  
        "GigabitEthernet1/1",  
        "GigabitEthernet1/2",  
        "GigabitEthernet1/3",  
    },  
}
- C. {  
    "hostname": "edge\_router\_1"  
    "interfaces": [  
        "GigabitEthernet1/1"  
        "GigabitEthernet1/2"  
        "GigabitEthernet1/3"  
    ]  
}
- D. {  
    "hostname": "edge\_router\_1",  
    "interfaces": [  
        "GigabitEthernet1/1",  
        "GigabitEthernet1/2",  
        "GigabitEthernet1/3"  
    ]  
}

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 21**

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

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

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

For E, both "TAB" and "Ctrl+L" can re-show the command.

For "TAB", it will also perform auto-completing the command if the incomplete keyword only corresponds to only one choice.

**QUESTION 22**

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

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

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

If RSSI value is -65 dBm and the noise floor is -85 dBm, then the SNR is 20dB.

**QUESTION 23**

Which statements are used for error handling in Python?

- A. try/catch
- B. catch/release
- C. block/rescue
- D. try/except

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 24**

What are two benefits of virtualizing the server with the use of VMs in a data center environment? (Choose two.)

- A. reduced rack space, power, and cooling requirements
- B. smaller Layer 2 domain
- C. increased security
- D. speedy deployment
- E. reduced IP and MAC address requirements

**Correct Answer:** AD

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 25**

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

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

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 26**

What is a benefit of data modeling languages like YANG?

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

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 27**

Refer to the exhibit.

Name is Bob Johnson

Age is 75

is alive

Favorite foods are:

- Cereal
- Mustard
- Onions

What is the JSON syntax that is formed from the data?

- A. {Name: Bob Johnson, Age: 75, Alive: true, Favorite Foods: [Cereal, Mustard, Onions]}
- B. {"Name": "Bob Johnson", "Age": 75, "Alive": true, "Favorite Foods": ["Cereal", "Mustard", "Onions"]}
- C. {'Name': 'Bob Johnson', 'Age': 75, 'Alive': True, 'Favorite Foods': 'Cereal', 'Mustard', 'Onions'}
- D. {"Name": "Bob Johnson", "Age": Seventyfive, "Alive": true, "Favorite Foods": ["Cereal", "Mustard", "Onions"]}

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

JSON standard requires double quotes for attribute names and value of String.

**QUESTION 28**

Based on this interface configuration, what is the expected state of OSPF adjacency?

R1:

```
interface GigabitEthernet0/1
  ip address 192.0.2.1 255.255.255.252
  ip ospf 1 area 0
  ip ospf hello-interval 2
  ip ospf cost 1
end
```

R2:

```
interface GigabitEthernet0/1
  ip address 192.0.2.2 255.255.255.252
  ip ospf 1 area 0
  ip ospf cost 500
end
```

A. 2WAY/DROTHER on both routers

B. not established

C. FULL on both routers

D. FULL/BDR on R1 and FULL/BDR on R2

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

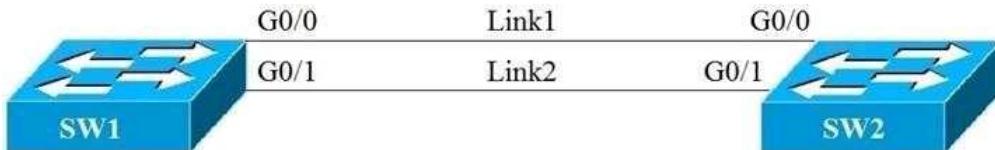
Hello timer mis-matched.

For Ethernet, default hello interval is 10 seconds.

Hence R2's g0/1 cannot match the hello interval of 2 configured in R1's g0/1.

**QUESTION 29**

Refer to the exhibit.



**SW2#show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

|            |                        |                                     |
|------------|------------------------|-------------------------------------|
| Root ID    | Priority               | 32769                               |
| Address    | 5000.0005.0000         |                                     |
| Cost       | 4                      |                                     |
| Port       | 1 (GigabitEthernet0/0) |                                     |
| Hello Time | 2 sec                  | Max Age 20 sec Forward Delay 15 sec |
| Bridge ID  | Priority               | 32769 (priority 32768 sys-id-ext 1) |
| Address    | 5000.0006.0000         |                                     |
| Hello Time | 2 sec                  | Max Age 20 sec Forward Delay 15 sec |
| Aging Time | 300 sec                |                                     |
| Interface  | Role                   | Sts Cost Prio.Nbr Type              |
| -----      | -----                  | -----                               |
| Gi0/0      | Root                   | FWD 4 128.1 P2p                     |
| Gi0/1      | Altn                   | BLK 4 32.2 P2p                      |

Link1 is a copper connection and Link2 is a fiber connection. The fiber port must be the primary port for all forwarding. The output of the show spanning-tree command on SW2 shows that the fiber port is blocked by spanning tree. An engineer enters the spanning-tree port-priority 32 command on G0/1 on SW2, but the port remains blocked.

Which command should be entered on the ports that are connected to Link2 to resolve the issue?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

You should configure the port priority of the neighbor switch connecting to Sw2 i.e. Sw1.

### QUESTION 30

Which JSON syntax is valid?

- A. {"switch": "name": "dist1", "interfaces": ["gig1", "gig2", "gig3"]}
- B. {"/switch": {"/name": "dist1", "/interfaces": ["gig1", "gig2", "gig3"]}}
- C. {"switch": {"name": "dist1", "interfaces": ["gig1", "gig2", "gig3"]}}
- D. {'switch': ('name': 'dist1', 'interfaces': ['gig1', 'gig2', 'gig3'])}

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Single quote is invalid.

For A, "switch": "name": "dist1" is a invalid syntax.

C is valid since the attribute "switch" has a object {"name": "dist1", "interfaces": ["gig1", "gig2", "gig3"]} as its value.

### QUESTION 31

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

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

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Microwave oven cause interference for WiFi, not conventional oven.

**QUESTION 32**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 33**

Which behavior can be expected when the HSRP version is changed from 1 to 2?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 34**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

For secure communication channel, HTTPS can be used instead of HTTP.

**QUESTION 35**

Refer to this output.

```
R1# *Feb 14 37:09:53.129: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

What is the logging severity level?

- A. notification
- B. emergency
- C. critical
- D. alert

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 36**

Refer to the exhibit.

```
R1#show ip bgp
```

BGP table version is 32, local router ID is 192.168.101.5

Status codes: S suppressed, d damped, h history, \*valid, > best, i - internal,  
 r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,  
 x best-external, a additional-path, c RIB-compressed,

Origin codes: i - IGP, e - EGP, ? - incomplete

RPKI validation codes: V valid, I invalid, N Not found

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

Which IP address becomes the active next hop for 192.168.102.0/24 when 192.168.101.2 fails?

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

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

192.168.101.2 is more preferred due to highest weight. However after it is down, the best path will be selected based on:  
- Default Local Preference is 100 (more preferred than those with 80). Among the remaining paths, there are three paths with default local preference.  
- Entry with next hop 192.168.101.18 has the shortest AS path list among the two having default local preference (i.e. 192.168.101.10 and 192.168.101.6)..

**QUESTION 37**

Which PAgP mode combination prevents an EtherChannel from forming?

- A. auto/desirable
- B. desirable/desirable
- C. desirable/auto
- D. auto/auto

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 38**

If a VRRP master router fails, which router is selected as the new master router?

- A. router with the lowest priority
- B. router with the highest priority
- C. router with the highest loopback address
- D. router with the lowest loopback address

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 39**

Which QoS component alters a packet to change the way that traffic is treated in the network?

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

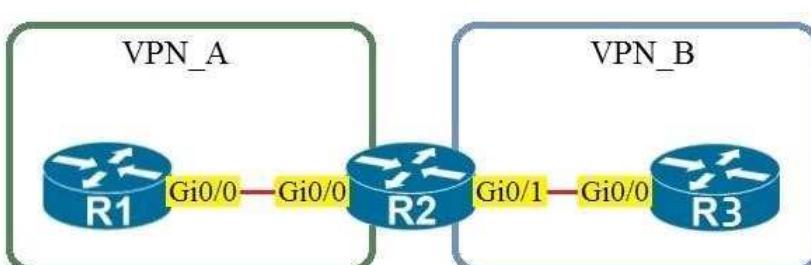
**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

Note that only marking makes alteration in the packet header by setting bits in ToS field.

**QUESTION 40**

Refer to the exhibit.



Assuming that R1 is a CE router, which VRF is assigned to Gi0/0 on R1?

- A. default VRF
- B. VRF VPN\_A
- C. VRF VPN\_B
- D. management VRF

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Since only R2 has multiple VRFs, VRF configuration is needed on R2 only.

**QUESTION 41**

Refer to the exhibit.

The screenshot shows a Cisco WLAN security configuration interface. At the top, there are tabs for General, Security, QoS, Advanced, Policy Mapping, General, Security, QoS, Advanced, and Policy Mapping. Below these are sub-tabs for Layer 2, Layer 3, and AAA Servers, with Layer 3 selected. The main configuration area is titled 'Fast Transition' and contains the following sections:

- Protected Management Frame:** PMF is set to Disabled.
- WPA+WPA2 Parameters:** WPA Policy is checked, while WPA2 Policy-AES is checked.
- Authentication Key Management:** It lists several authentication methods: 802.1X (unchecked), CCKM (unchecked), PSK (checked), FT 802.1X (unchecked), FT PSK (unchecked), and PSK Format (set to ASCII). A password field below shows '\*\*\*\*\*'.

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

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

**Correct Answer: A**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

For PSK, a text string is used for authentication.

**QUESTION 42**

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

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

**Correct Answer: CE**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 43**

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

- A. SSL
- B. Cisco TrustSec
- C. MACsec
- D. IPsec

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 44**

Refer to the exhibit.

```

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

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

Which explanation of this behavior is true?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 45**

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

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

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The FQDN for finding IP address of the controller should be:  
CISCO-CAPWAP-CONTROLLER.localdomain OR  
CISCO-LWAPP-CONTROLLER.localdomain

**QUESTION 46**

Which IP SLA operation requires the IP SLA responder to be configured on the remote end?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Unlike UDP jitter, ICMP jitter can be supported if the remote end supports ICMP Timestamp.

**QUESTION 47**

Which statement explains why Type 1 hypervisor is considered more efficient than Type2 hypervisor?

- A. Type 1 hypervisor is the only type of hypervisor that supports hardware acceleration techniques.
- B. Type 1 hypervisor relies on the existing OS of the host machine to access CPU, memory, storage, and network resources.
- C. Type 1 hypervisor runs directly on the physical hardware of the host machine without relying on the underlying OS.
- D. Type 1 hypervisor enables other operating systems to run on it.

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 48**

A client with IP address 209.165.201.25 must access a web server on port 80 at 209.165.200.225. To allow this traffic, an engineer must add a statement to an access control list that is applied in the inbound direction on the port connecting to the web server.

Which statement allows this traffic?

- A. permit tcp host 209.165.200.225 lt 80 host 209.165.201.25
- B. permit tcp host 209.165.201.25 host 209.165.200.225 eq 80
- C. permit tcp host 209.165.200.225 eq 80 host 209.165.201.25
- D. permit tcp host 209.165.200.225 host 209.165.201.25 eq 80

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

For inbound direction on the port connecting to the web server, packets from the web server will have a source port 80.

**QUESTION 49**

In OSPF, which LSA type is responsible for pointing to the ASBR router?

- A. type 1
- B. type 2
- C. type 3
- D. type 4

**Correct Answer: D**

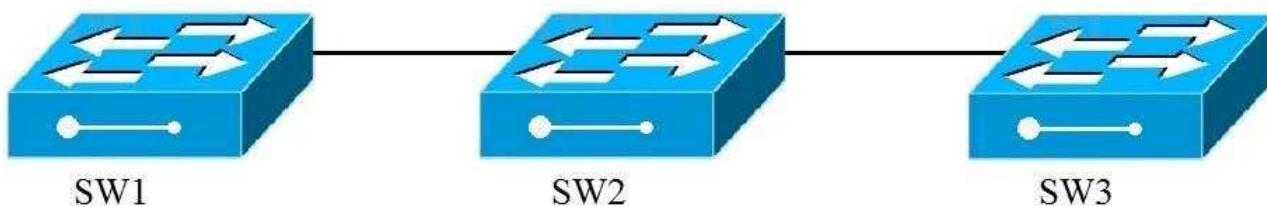
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 50**

Refer to the exhibit.



VLANs 50 and 60 exist on the trunk links between all switches. All access ports on SW3 are configured for VLAN 50 and SW1 is the VTP server.

Which command ensures that SW3 receives frames only from VLAN 50?

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

VTP pruning is enabled on VTP servers, all the VTP clients in the VTP domain will then automatically enable VTP pruning.

**QUESTION 51**

Which statement about a fabric access point is true?

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 52**

Which First Hop Redundancy Protocol maximizes uplink utilization and minimizes the amount of configuration that is necessary?

- A. GLBP
- B. HSRP v2
- C. VRRP
- D. HSRP v1

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 53**

Which standard access control entry permits traffic from odd-numbered hosts in the 10.0.0.0/24 subnet?

- A. permit 10.0.0.0 0.0.0.1
- B. permit 10.0.0.1 0.0.0.254
- C. permit 10.0.0.1 0.0.0.0
- D. permit 10.0.0.0 255.255.255.254

**Correct Answer:** B

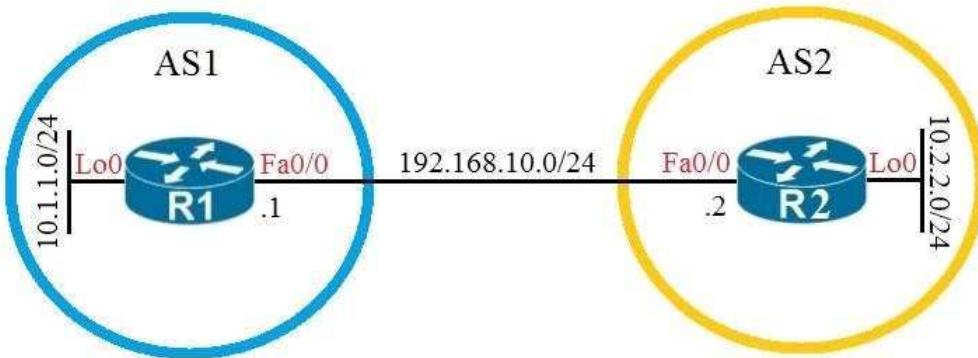
**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 54**

Refer to the exhibit.



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

- A. R1(config)#router bgp 1  
R1(config-router)#neighbor 192.168.10.2 remote-as 2  
R1(config-router)#network 10.1.1.0 mask 255.255.255.0  
R2(config)#router bgp 2  
R2(config-router)#neighbor 192.168.10.1 remote-as 1  
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
- B. R1(config)#router bgp 1  
R1(config-router)#neighbor 10.2.2.2 remote-as 2  
R1(config-router)#network 10.1.1.0 mask 255.255.255.0  
R2(config)#router bgp 2  
R2(config-router)#neighbor 10.1.1.1 remote-as 1  
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
- C. R1(config)#router bgp 1  
R1(config-router)#neighbor 192.168.10.2 remote-as 2  
R1(config-router)#network 10.0.0.0 mask 255.0.0.0  
R2(config)#router bgp 2  
R2(config-router)#neighbor 192.168.10.1 remote-as 1  
R2(config-router)#network 10.0.0.0 mask 255.0.0.0
- D. R1(config)#router bgp 1  
R1(config-router)#neighbor 10.2.2.2 remote-as 2  
R1(config-router)#neighbor 10.2.2.2 update-source lo0  
R1(config-router)#network 10.1.1.0 mask 255.255.255.0  
R2(config)#router bgp 2  
R2(config-router)#neighbor 10.1.1.1 remote-as 1  
R2(config-router)#neighbor 10.1.1.1 update-source lo0  
R2(config-router)#network 10.2.2.0 mask 255.255.255.0

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The question just asks to advertise loopback network. (not forming neighbor with loopback).

Hence you can just form BGP neighbor with directly connected network

Note that the mask configured in the `network` command must match the network mask (i.e. /24) of the loopback address.

**Important:**

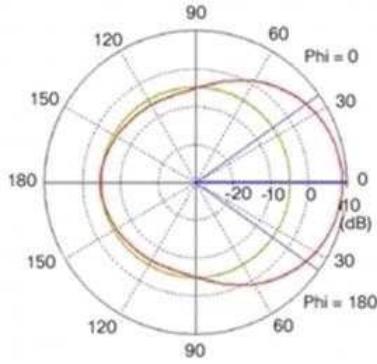
If the question ask you to use the loopback for RouterID, the answer is the same.

It is because loopback address will be used as RouterID by default (or you can manually configure it with "bgp router-id ..." command).

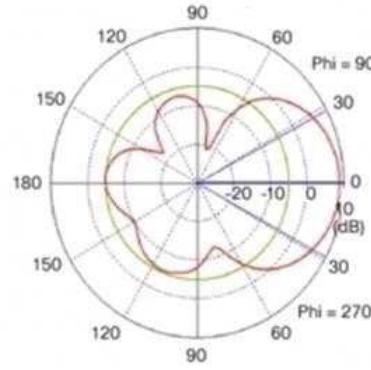
Actually you can even not advertising the loopback network with network command for this.

**QUESTION 55**

Refer to the exhibit.



**Antenna Azimuth  
Plane Pattern**



**Antenna Elevation  
Plane Pattern**

Which type of antenna do the radiation patterns present?

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 56**

Which method creates an EEM applet policy that is registered with EEM and runs on demand or manually?

- A. event manager applet ondemand  
event none  
action 1.0 syslog priority critical msg 'This is a message from ondemand'
- B. event manager applet ondemand  
action 1.0 syslog priority critical msg 'This is a message from ondemand'
- C. event manager applet ondemand  
event register  
action 1.0 syslog priority critical msg 'This is a message from ondemand'
- D. event manager applet ondemand  
event manual  
action 1.0 syslog priority critical msg 'This is a message from ondemand'

**Correct Answer: A**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

"event none" is required for EEM applet to be run manually.

**QUESTION 57**

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

Which device presents the web authentication for the WLAN?

- A. ISE server
- B. RADIUS server
- C. anchor WLC
- D. local WLC

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 58**

Which controller is the single plane of management for Cisco SD-WAN?

- A. vBond
- B. vSmart
- C. vManage
- D. vEdge

**Correct Answer: C**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

**QUESTION 59**

A network is being migrated from IPv4 to IPv6 using a dual-stack approach. Network management is already 100% IPv6 enabled.

In a dual-stack network with two dual-stack NetFlow collectors, how many flow exporters are needed per network device in the flexible NetFlow configuration?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 60**

Drag and drop the descriptions from the left onto the correct QoS components on the right.

Which of the followings are the characteristics of Traffic Policing (Choose three)?

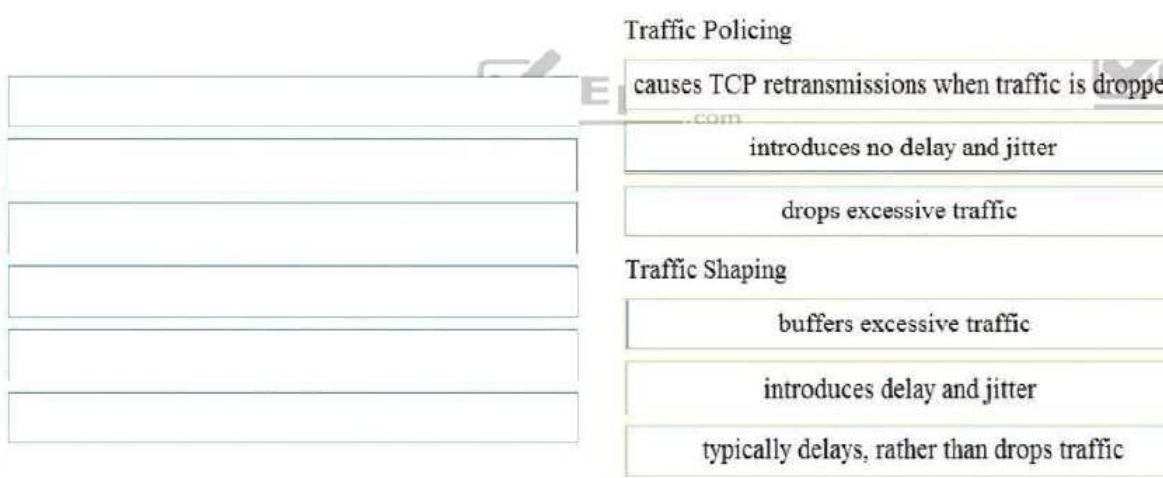
- A. causes TCP retransmissions when traffic is dropped
- B. buffers excessive traffic
- C. introduces no delay and jitter
- D. introduces delay and jitter
- E. drops excessive traffic
- F. typically delays, rather than drops traffic

**Correct Answer:** ACE

**Section:** (none)

**Explanation**

**Explanation/Reference:**



Shaping - a bandwidth management technique which can introduce delay and jitter (output only)

Policing - a bandwidth management technique which rate-limits traffic (input or output)

**QUESTION 61**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 62**

Which reason could cause an OSPF neighbor to be in the EXSTART/EXCHANGE state?

- A. mismatched OSPF link costs
- B. mismatched OSPF network type
- C. mismatched areas
- D. mismatched MTU size

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 63**

Which LISP device is responsible for publishing EID-to-RLOC mappings for a site?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 64**

Which method does the enable secret password option use to encrypt device passwords?

- A. MD5
- B. PAP
- C. CHAP
- D. AES

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 65**

Which statement about agent-based versus agentless configuration management tools is true?

- A. Agentless tools use proxy nodes to interface with slave nodes.
- B. Agentless tools require no messaging systems between master and slaves.
- C. Agent-based tools do not require a high-level language interpreter such as Python or Ruby on slave nodes.
- D. Agent-based tools do not require installation of additional software packages on the slave nodes.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Many agent clients are written by Python, Ruby ... etc. Hence agent-based nodes require them in order to run the agent client program codes.

**QUESTION 66**

Which statement about Cisco Express Forwarding is true?

- A. The CPU of a router becomes directly involved with packet-switching decisions.
- B. It uses a fast cache that is maintained in a router data plane.
- C. It maintains two tables in the data plane: the FIB and adjacency table.
- D. It makes forwarding decisions by a process that is scheduled through the IOS scheduler.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 67**

Refer to the exhibit.

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

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

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

- D. Inside source addresses are translated to the 209.165.201.0/27 subnet.
- E. The 10.1.1.0/27 subnet is assigned as the inside global address range.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

C may also be the answer.

**Remarks:**

Although all answers are in /27, the following shows how prefix length can be calculated:

- For 255.255.255.224 in the public address pool,  $256 - 224 = 32 = 2^5$ . Hence prefix length is  $32 - 5 = 27$ .
- For 0.0.0.31 in the NAT ACL,  $31 + 1 = 32 = 2^5$ . Hence prefix length is also  $32 - 5 = 27$ .

#### **QUESTION 68**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 69**

What is the structure of a JSON web token?

- A. three parts separated by dots: header, payload, and signature
- B. three parts separated by dots: version, header, and signature
- C. header and payload
- D. payload and signature

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

JSON Web token (JWT) is used for client authentication and is sent by client in HTTP request as JSON object.

#### **QUESTION 70**

A response code of 404 is received while using the REST API on Cisco DNA Center to POST to this URI: /dna/intent/api/v1/template-programmer/project

What does the code mean?

- A. The POST/PUT request was fulfilled and a new resource was created. Information about the resource is in the response body.
- B. The request was accepted for processing, but the processing was not completed.
- C. The client made a request for a resource that does not exist.
- D. The server has not implemented the functionality that is needed to fulfill the request.

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

#### **QUESTION 71**

What is a benefit of deploying an on-premises infrastructure versus a cloud infrastructure deployment?

- A. ability to quickly increase compute power without the need to install additional hardware
- B. less power and cooling resources needed to run infrastructure on-premises
- C. faster deployment times because additional infrastructure does not need to be purchased
- D. lower latency between systems that are physically located near each other

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 72**

A customer has several small branches and wants to deploy a Wi-Fi solution with local management using CAPWAP.

Which deployment model meets this requirement?

- A. local mode
- B. autonomous
- C. SD-Access wireless
- D. Mobility Express

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 73**

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

- A. PULL
- B. PUSH
- C. PATCH
- D. REMOVE
- E. ADD
- F. HEAD

**Correct Answer:** CF  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

**QUESTION 74**

Refer to the exhibit.

| Clients > Detail            |                                                |                       |                   |
|-----------------------------|------------------------------------------------|-----------------------|-------------------|
|                             |                                                | < Back                | Apply             |
| Client Properties           |                                                | AP Properties         |                   |
| MAC Address                 | 00:09:ef:0G:07:bd                              | AP Address            | 3c:ce:73:1b:33:39 |
| IP Address                  | 192.100.101.100                                | AP Name               | 172.22.253.20     |
| Client Type                 | Regular                                        | AP Type               | Mobile            |
| User Name                   |                                                | WLAN Profile          | Staff             |
| Port Number                 | 29                                             | Status                | Associated        |
| Interface                   | Staff                                          | Association ID        | 0                 |
| VLAN ID                     | 3602                                           | 802.11 Authentication | Open System       |
| CCX Version                 | Not Supported                                  | Reason Code           | 1                 |
| E2E Version                 | Not Supported                                  | Status Code           | 0                 |
| Mobility Role               | Anchor                                         | CF Pollable           | Not Implemented   |
| Mobility Peer IP Address    | 172.22.253.20                                  | CF Poll Request       | Not Implemented   |
| Policy Manager State        | RUN                                            | Short Preamble        | Implemented       |
| Management Frame Protection | No                                             | PBCC                  | Not Implemented   |
| UpTime (Sec)                | 3710                                           | Channel Agility       | Not Implemented   |
| Power Save Mode             | OFF                                            | Timeout               | 0                 |
| Current TxRateSet           |                                                | WEP State             | WEP Enable        |
| Data RateSet                | 5.5,11.0,6.0,9.0,12.0,19.0,24.0,36.0,40.0,54.0 |                       |                   |

The WLC administrator sees that the controller to which a roaming client associates has Mobility Role Anchor configured under Clients > Detail.

Which type of roaming is supported?

- A. indirect
- B. Layer 3 intercontroller
- C. intracontroller
- D. Layer 2 intercontroller

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

For layer 2 intercontroller roaming, the client database entry will just move to the new WLC.

For layer 3 intercontroller roaming, since the new WLC has to send the traffic back to the original WLC for accessing the original IP network, an Anchor entry has to be maintained in the original WLC.

**QUESTION 75**

In which part of the HTTP message is the content type specified?

- A. HTTP method
- B. body
- C. header

D. URI

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 76**

Which statement about VXLAN is true?

- A. VXLAN encapsulates a Layer 2 frame in an IP-UDP header, which allows Layer 2 adjacency across router boundaries.
- B. VXLAN uses the Spanning Tree Protocol for loop prevention.
- C. VXLAN extends the Layer 2 Segment ID field to 24-bits, which allows up to 4094 unique Layer 2 segments over the same network.
- D. VXLAN uses TCP as the transport protocol over the physical data center network.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 77**

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

Which of the followings are the characteristics of On Premises (Choose three)?

- A. **customizable hardware, purpose-built systems**
- B. **easy to scale and upgrade**
- C. **more suitable for companies with specific regulatory or security requirements**
- D. **resources can be over or underutilized as requirements vary**
- E. **requires a strong and stable internet connection**
- F. **built-in, automated data backups and recovery**

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

|  | <b>On Premises</b>                                                            |  |
|--|-------------------------------------------------------------------------------|--|
|  | customizable hardware, purpose-built systems                                  |  |
|  | more suitable for companies with specific regulatory or security requirements |  |
|  | resources can be over or underutilized as requirements vary                   |  |
|  | <b>Cloud</b>                                                                  |  |
|  | easy to scale and upgrade                                                     |  |
|  | requires a strong and stable internet connection                              |  |
|  | built-in, automated data backups and recovery                                 |  |

**Remarks:** More characteristics ..

**On-premises**

Large intial investment but low recurring costs.  
company has control over the physical security

**Cloud**

Pay as you go

Physical location of the data can be defined in contract with provider (e.g. London, New York, Singapore ... etc)  
fast delivery of changes in scale

**QUESTION 78**

Which statement about Cisco EAP-FAST is true?

- A. It requires a client certificate.
- B. It is an IETF standard.
- C. It does not require a RADIUS server certificate.
- D. It operates in transparent mode.

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 79**

What do Cisco DNA southbound APIs provide?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 80**

Which DNS lookup does an access point perform when attempting CAPWAP discovery?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 81**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 82**

Drag and drop the characteristics from the left onto the correct routing protocol types on the right.

Which of the following are the characteristics of OSPF (Choose three)?

- A. supports unequal path load balancing
- B. link state routing protocol
- C. distance vector routing protocol
- D. metric based on delay and reliability by default
- E. makes it easy to segment the network logically
- F. constructs three tables as part of its operation: neighbor table, topology table, and routing table

**Correct Answer:** BEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

Actually both OSPF and EIGRP maintain the three tables. Hence there are already three specific characteristics assigned to EIGRP, the answer about three tables is therefore assigned to OSPF.

**QUESTION 83**

Which statement about an RSPAN session configuration is true?

- A. Only one session can be configured at a time.
- B. A special VLAN type must be used as the RSPAN destination.
- C. A filter must be configured for RSPAN sessions.
- D. Only incoming traffic can be monitored.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 84**

Refer to the exhibit.

**Extended IP access list EGRESS**

```
10 permit ip 10.1.100.0 0.0.0.255 10.1.2.0 0.0.0.255
20 deny ip any any
```

An engineer must modify the access control list EGRESS to allow all IP traffic from subnet 10.1.10.0/24 to 10.1.2.0/24. The access control list is applied in the outbound direction on router interface GigabitEthernet 0/1.

Which configuration commands can the engineer use to allow this traffic without disrupting existing traffic flows?

- A. config t
 

```
ip access-list extended EGRESS
      permit ip 10.1.10.0 255.255.255.0 10.1.2.0 255.255.255.0
```
- B. config t
 

```
ip access-list extended EGRESS2
      permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
      permit ip 10.1.100.0 0.0.0.255 10.1.2.0 0.0.0.255
      deny ip any any
      !
      interface g0/1
      no ip access-group EGRESS out
      ip access-group EGRESS2 out
```
- C. config t
 

```
ip access-list extended EGRESS
      permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
```

```

D. config t
    ip access-list extended EGRESS
        5 permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255

```

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**  
Since there is a rule deny ip any any, you cannot use answer C to append the new rule at the end  
For B, although it works, some unwanted traffic may be allowed temporarily. Moreover it is not modifying the access list EGRESS as required by the question.

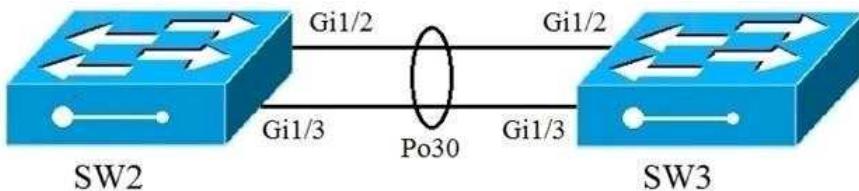
**QUESTION 85**  
What is the role of a fusion router in an SD-Access solution?

- A. acts as a DNS server
- B. provides additional forwarding capacity to the fabric
- C. performs route leaking between user-defined virtual networks and shared services
- D. provides connectivity to external networks

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 86**  
Refer to the exhibit.



```

Interface gi1/2
Channel-group 30 mode desirable
Port-channel load-balance src-ip

```

```

Interface gi1/3
Channel-group 30 mode desirable
Port-channel load-balance src-ip

```

```

Interface PortChannel 30
Switchport mode trunk
Switchport encapsulation dot1q
Switchport trunk allowed vlan 10-100

```

A port channel is configured between SW2 and SW3. SW2 is not running a Cisco operating system. When all physical connections are made, the port channel does not establish.

Based on the configuration excerpt of SW3, what is the cause of the problem?

- A. The port-channel mode should be set to auto.
- B. The port channel on SW2 is using an incompatible protocol.
- C. The port-channel trunk is not allowing the native VLAN.
- D. The port-channel interface load balance should be set to src-mac.

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**  
mode "desirable" means the using the Cisco PAgP which is a Cisco proprietary protocol for link aggregation.

**QUESTION 87**  
What does this EEM applet event accomplish?

```
"event snmp oid 1.3.6.1.3.7.0.9.5.3.1.2.9 get-type next entry-op gt entry-val 75 poll-interval 5"
```

- A. Upon the value reaching 75%, a SNMP event is generated and sent to the trap server.
- B. It reads an SNMP variable, and when the value exceeds 75%, it triggers an action.
- C. It issues email when the value is greater than 75% for five polling cycles.
- D. It presents a SNMP variable that can be interrogated.

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 88**

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

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

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

All event are configured as "syslog pattern", they are actually not synchronous EEM applet and therefore cannot write directly to console.

Among them, only D is valid for sending text string. However the text can only be sent to syslog since it is not a synchronous EEM applet. However, by default since logging console is 7, the text written to syslog will be shown in the syslog message displayed in console as follows:

\*May 9 13:12:18.181: %HA\_EM-6-LOG: boom: logging directly to console

A is wrong since there is no priority "direct" for syslog.

**QUESTION 89**

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

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

**Correct Answer:** BC  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

If you has previously set the IP MTU to a very low value, you can increase it to the maximum value allowed in your network setup (e.g. after subtracting GRE header).

However, if PMTUD is also available as a choice, the choice PMTID is more preferred than IP MTU.

**QUESTION 90**

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

- A. onboard vEdge nodes into the SD-WAN fabric
- B. gather telemetry data from vEdge routers
- C. distribute security information for tunnel establishment between vEdge routers
- D. manage, maintain, and gather configuration and status for nodes within the SD-WAN fabric

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 91**

Which description of an SD-Access wireless network infrastructure deployment is true?

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

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 92**

Which feature is supported by EIGRP but is not supported by OSPF?

- A. route filtering
- B. unequal-cost load balancing
- C. route summarization
- D. equal-cost load balancing

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 93**

What is the correct EBGP path attribute list, ordered from most preferred to least preferred, that the BGP best-path algorithm uses?

- A. local preference, weight, AS path, MED
- B. weight, local preference, AS path, MED
- C. weight, AS path, local preference, MED
- D. local preference, weight, MED, AS path

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 94**

At which layer does Cisco DNA Center support REST controls?

- A. session layer
- B. northbound APIs
- C. EEM applets or scripts
- D. YAML output from responses to API calls

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 95**

On which protocol or technology is the fabric data plane based in Cisco SD-Access fabric?

- A. VXLAN
- B. LISP
- C. Cisco TrustSec
- D. IS-IS

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 96**

What is the difference between the enable password and the enable secret password when service password encryption is enabled on an IOS device?

- A. The enable secret password is protected via stronger cryptography mechanisms.
- B. The enable password cannot be decrypted.
- C. The enable password is encrypted with a stronger encryption method.
- D. There is no difference and both passwords are encrypted identically.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The question can be viewed in two different meanings:

1.  
Assume the service password encryption is already enabled.  
What is the difference between the enable password and the enable secret password.  
In this case, although both are encrypted:
  - enable secret is protected via MD5 which is a stronger cryptography mechanism.
  - enable password is protected using type 7 algorithm which is very weak.Therefore A is the answer.
  
2.  
For the enable password and the enable secret password, what is the difference in the following case:
  - before service password encryption is enabled
  - after service password encryption has been enabledIn this case,
  - there is no change in enable secret.
  - enable password is protected using a stronger cryptography mechanism (i.e. type 7 algorithm) than clear text.Therefore C is the answer.

Most suggested answer in Internet use A.

Meaning in 2 may not correct since enable password is not protected before service password encryption is enabled and therefore the word "stronger" in choice C is not appropriate in this meaning.

#### QUESTION 97

Which access control list allows only TCP traffic with a destination port range of 22-443, excluding port 80?

- A. deny tcp any any eq 80  
    permit tcp any any gt 21 lt 444
- B. permit tcp any any range 22 443  
    deny tcp any any eq 80
- C. permit tcp any any ne 80
- D. deny tcp any any ne 80  
    permit tcp any any range 22 443
- E. deny tcp any any eq 80  
    permit tcp any any range 22 443

**Correct Answer:** E

**Section:** (none)

**Explanation**

**Explanation/Reference:**

For other answers:

A is wrong due to command syntax since gt and lt cannot be configured at the same time in a single rule.  
B the first rule will allow 80 and second rule will never be matched for denying port 80  
C all ports not equal to 80 (e.g. 8080) are allowed.  
D the first rule deny all ports not equal 80 and the second rule will not be used for permitting ports 22-443.

#### QUESTION 98

Which statement describes the IP and MAC allocation requirements for virtual machines on Type 1 hypervisors?

- A. Virtual machines do not require a unique IP or unique MAC. They share the IP and MAC address of the physical server.
- B. Each virtual machine requires a unique IP address but shares the MAC address with the physical server.
- C. Each virtual machine requires a unique IP and MAC addresses to be able to reach to other nodes.
- D. Each virtual machine requires a unique MAC address but shares the IP address with the physical server.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 99

A local router shows an EBGP neighbor in the Active state.

Which statement is true about the local router?

- A. The local router is attempting to open a TCP session with the neighboring router.
- B. The local router is receiving prefixes from the neighboring router and adding them in RIB-IN.
- C. The local router has active prefixes in the forwarding table from the neighboring router.
- D. The local router has BGP passive mode configured for the neighboring router.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 100

Which feature must be configured to allow packet capture over Layer 3 infrastructure?

- A. RSPAN
- B. ERSPAN
- C. VSPAN
- D. IPSPAN

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 101

Refer to the exhibit.

```

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

SwitchC#show vlan brief

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

SwitchC#show int trunk

Port Mode Encapsulation Status Native vlan
Gig1/1 on 802.1q trunking 1
Gig1/2 on 802.1q trunking 1

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

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

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

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

```

SwitchC connects HR and Sales to the Core switch. However, business needs require that no traffic from the Finance VLAN traverse this switch.

Which command meets this requirement?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since the switch is a VTP transparent mode switch, VTP pruning cannot be used.

#### QUESTION 102

Refer to the exhibit.

```

PYTHON CODE:
import requests
import json

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

myheaders={'content-type':'application/json'}
payload={
"ins_api": {
    "version": "1.0",
    "type": "cli_show",
    "chunk": "0",
    "sid": "1"
    "input": "show version",
    "output_format": "json"
}
}

response = requests.post(url,data=json.dumps(payload), headers=myheaders,auth=(switchuser,switchpassword)).json()
print(response['ins_api']['outputs']['output'][0]['body']['kickstart_ver_str'])

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

```

Which HTTP JSON response does the Python code output give?

- A. 7.0(3)|7(4)
- B. 7.61
- C. NameError: name `json` is not defined
- D. KeyError: `kickstart\_ver\_str`

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**  
The Python code prints the value for the field "kickstart\_ver\_str".

#### QUESTION 103

Which two namespaces does the LISP network architecture and protocol use? (Choose two.)

- A. TLOC
- B. RLOC
- C. DNS
- D. VTEP
- E. EID

**Correct Answer:** BE  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

#### QUESTION 104

A network administrator applies the following configuration to an IOS device:  
aaa new-model  
aaa authentication login default local group tacacs+

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

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

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 105**

Which two entities are Type 1 hypervisors? (Choose two.)

- A. Oracle VM VirtualBox
- B. Microsoft Hyper-V
- C. VMware server
- D. VMware ESX
- E. Microsoft Virtual PC

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 106**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 107**

Which feature of EIGRP is not supported in OSPF?

- A. load balancing of unequal-cost paths
- B. load balance over four equal-cost paths
- C. uses interface bandwidth to determine best path
- D. per-packet load balancing over multiple paths

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 108**

A company plans to implement intent-based networking in its campus infrastructure.

Which design facilitates a migration from a traditional campus design to a programmable fabric design?

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

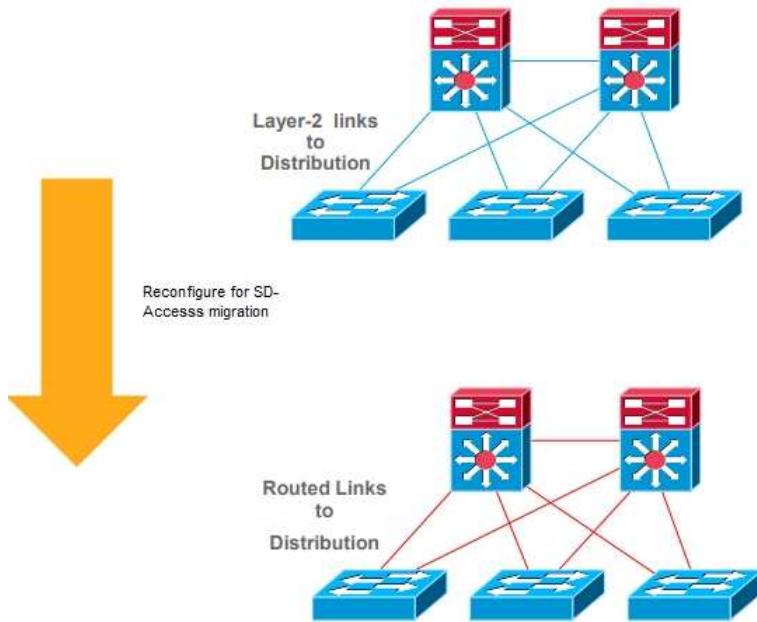
**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Routed access is the use of routed links between access and distribution layers. This network topology setup facilitates the migration to a programmable fabric design.



#### QUESTION 109

Which action is a function of VTEP in VXLAN?

- A. tunneling traffic from IPv6 to IPv4 VXLANs
- B. allowing encrypted communication on the local VXLAN Ethernet segment
- C. encapsulating and de-encapsulating VXLAN Ethernet frames
- D. tunneling traffic from IPv4 to IPv6 VXLANs

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 110

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 111

When a wireless client roams between two different wireless controllers, a network connectivity outage is experienced for a period of time.

Which configuration issue would cause this problem?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 112

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

- A. The RP maintains default aging timeouts for all multicast streams requested by the receivers.
- B. The RP acts as a control-plane node only and does not receive or forward multicast packets.
- C. The RP is the multicast router that is the root of the PIM-SM shared multicast distribution tree.
- D. The RP responds to the PIM join messages with the source of a requested multicast group.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 113**

How does QoS traffic shaping alleviate network congestion?

- A. It drops packets when traffic exceeds a certain bitrate.
- B. It buffers and queues packets above the committed rate.
- C. It fragments large packets and queues them for delivery.
- D. It drops packets randomly from lower priority queues..

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 114**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 115**

An engineer is describing QoS to a client.

Which two facts apply to traffic policing? (Choose two.)

- A. Policing should be performed as close to the source as possible.
- B. Policing adapts to network congestion by queuing excess traffic.
- C. Policing should be performed as close to the destination as possible.
- D. Policing drops traffic that exceeds the defined rate.
- E. Policing typically delays the traffic, rather than drops it.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

When Policing should be performed close to the source:

- Traffic for policing can be identified more easily near the network edge.
- Traffic traveling along the network path can be reduced since traffic exceeding specified rate is dropped near the source.

**QUESTION 116**

Which component handles the orchestration plane of the Cisco SD-WAN?

- A. vBond
- B. vSmart
- C. vManage
- D. vEdge

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 117**

Which First Hop Redundancy Protocol should be used to meet a design requirement for more efficient default gateway bandwidth usage across multiple devices?

- A. GLBP
- B. LACP
- C. HSRP
- D. VRRP

**Correct Answer:** A

**Section: Selected  
Explanation**

**Explanation/Reference:**

**QUESTION 118**

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

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

**Correct Answer: B**

**Section: Selected  
Explanation**

**Explanation/Reference:**

Cisco Stealthwatch system collects NetFlow data and therefore can perform flow analysis.

**QUESTION 119**

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

What type of roam occurs?

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 120**

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

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 121**

An engineer must protect their company against ransomware attacks.

Which solution allows the engineer to block the execution stage and prevent file encryption?

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

**Correct Answer: B**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

**QUESTION 122**

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

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**Important:**

Depending on the AP models, you need to configure option 43 either with ascii or hex format.

Assume the WLC IP address is 172.16.0.1:

- For some AP models, option 43 ascii 172.16.0.1

- For some other AP models, option 43 hex f104.ac10,0001  
A DHCP server should be configured to return the appropriate format based on the AP's DHCP Vendor Class Identifier (VCI) string.

For the hex value "f104.ac10,0001" in second method:

f1 represents the type, it is always f1  
04 represents the length of the hexadecimal value for WLC IP address. If there are two WLC IP addresses, this is 08.  
ac means 172  
10 means 16  
00 means 0  
01 means 1

**QUESTION 123**

What are two device roles in Cisco SD-Access fabric? (Choose two.)

- A. edge node
- B. vBond controller
- C. access switch
- D. core switch
- E. border node

**Correct Answer:** AE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 124**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 125**

What are two reasons why broadcast radiation is caused in the virtual machine environment? (Choose two.)

- A. vSwitch must interrupt the server CPU to process the broadcast packet.
- B. The Layer 2 domain can be large in virtual machine environments.
- C. Virtual machines communicate primarily through broadcast mode.
- D. Communication between vSwitch and network switch is broadcast based.
- E. Communication between vSwitch and network switch is multicast based.

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 126**

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

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

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 127**

A network administrator is preparing a Python script to configure a Cisco IOS XE-based device on the network. The administrator is worried that colleagues will make changes to the device while the script is running.

Which operation of the ncclient manager prevents colleagues from making changes to the devices while the script is running?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 128**

What does the Cisco DNA Center use to enable the delivery of applications through a network and to yield analytics for innovation?

- A. process adapters
- B. Command Runner
- C. intent-based APIs
- D. domain adapters

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 129**

Wireless users report frequent disconnections from the wireless network. While troubleshooting, a network engineer finds that after the user is disconnected, the connection re-establishes automatically without any input required. The engineer also notices these message logs:

AP 'AP2' is down. Reason: Radio channel set. 6:54:04 PM  
AP 'AP4' is down. Reason: Radio channel set. 6:44:49 PM  
AP 'AP7' is down. Reason: Radio channel set. 6:34:32 PM

Which action reduces the user impact?

- A. enable coverage hole detection
- B. increase the AP heartbeat timeout
- C. enable **BandSelect**
- D. increase the dynamic channel assignment interval

**Correct Answer: D**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

The messages appeared since the AP changed channel to avoid interferences.

**QUESTION 130**

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

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

**Correct Answer: C**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

**QUESTION 131**

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

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

**Correct Answer: B**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

**QUESTION 132**

When a wired client connects to an edge switch in an SDA fabric, which component decides whether the client has access to the network?

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 133**

Which benefit is offered by a cloud infrastructure deployment but is lacking in an on-premises deployment?

- A. virtualization
- B. supported systems
- C. storage capacity
- D. efficient scalability

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 134**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 135**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 136**

Which data modeling language is commonly used by NETCONF?

- A. HTML
- B. XML
- C. YANG
- D. REST

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 137**

Which two statements about EIGRP load balancing are true? (Choose two.)

- A. EIGRP supports 6 unequal-cost paths
- B. A path can be used for load balancing only if it is a feasible successor
- C. EIGRP supports unequal-cost paths by default
- D. Any path in the EIGRP topology table can be used for unequal-cost load balancing
- E. Cisco Express Forwarding is required to load-balance across interfaces

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 138**

What are three valid HSRP states? (Choose three.)

- A. listen
- B. learning
- C. full
- D. established
- E. speak
- F. INIT

**Correct Answer:** AEF

**Section:** (none)

**Explanation**

**Explanation/Reference:****HSRP States**

**Initial** This is the state at the start. This state indicates that HSRP does not run. This state is entered through a configuration change or when an interface first becomes available.

**Learn** The router has not determined the virtual IP address and has not yet seen an authenticated hello message from the active router. In this state, the router still waits to hear from the active router.

**Listen** The router knows the virtual IP address, but the router is neither the active router nor the standby router. It listens for hello messages from those routers.

**Speak** The router sends periodic hello messages and actively participates in the election of the active and/or standby router. A router cannot enter speak state unless the router has the virtual IP address.

**Standby** The router is a candidate to become the next active router and sends periodic hello messages. With the exclusion of transient conditions, there is, at most, one router in the group in standby state.

**Active** The router currently forwards packets that are sent to the group virtual MAC address. The router sends periodic hello messages. With the exclusion of transient conditions, there must be, at most, one router in active state in the group.

Both "B" and "F" are not the exact workings as the terms listed above. However, since Cisco router shows initial state as INIT in the output messages, F is therefore chosen as the answer. The following extracts the debugging messages for state changes shown by "debug standby"

```
*Dec 2 10:13:21.475: HSRP: Gi0/1 Grp 2 Disabled -> Init
*Dec 2 10:13:22.449: HSRP: Gi0/1 Grp 2 Init -> Listen
*Dec 2 10:13:33.635: HSRP: Gi0/1 Grp 2 Listen -> Speak
*Dec 2 10:13:43.825: HSRP: Gi0/1 Grp 2 Speak -> Standby
*Dec 2 10:13:46.112: HSRP: Gi0/1 Grp 2 Standby -> Active
```

**QUESTION 139**

What mechanism does PIM use to forward multicast traffic?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Dense mode is a push model since it pushes multicast traffic from the source to all network segments initially.

Sparse mode is a pull model since multicast traffic is pulled from network segments with multicast client only.

**QUESTION 140**

Which two security features are available when implementing NTP? (Choose two.)

- A. symmetric server passwords
- B. dock offset authentication
- C. broadcast association mode
- D. encrypted authentication mechanism
- E. access list-based restriction scheme

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 141**

What is calculated using the numerical values of the transmitter power level, cable loss, and antenna gain?

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

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

RSSI is measured on the client and is also depends on the distance to the client, any obstacle between the AP and the client antenna.

EIRP is Effective Isotropic Radiated Power and it measures the power that comes off an antenna. EIRP is calculated by adding the transmitter power (in dBm) to the antenna gain (in dBi) and subtract any cable losses (in dB). For example:

| Part                              | Cisco Part Number | Power        |
|-----------------------------------|-------------------|--------------|
| A Cisco Aironet Bridge            | AIR-BR350-A-K9    | 20 dBm       |
| That uses a 50 foot antenna cable | AIR-CAB050LL-R    | 3.35 dB loss |
| And a solid dish antenna          | AIR-ANT3338       | 21 dBi gain  |
| Has an EIRP of                    |                   | 37.65 dBm    |

**QUESTION 142**

Which two LISP infrastructure elements are needed to support LISP to non-LISP internetworking? (Choose two.)

- A. PETER
- B. PITR
- C. MR
- D. MS
- E. ALT

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Map server (MS): An MS configures LISP site policy to authenticate when LISP sites try to register to the MS. It also performs the following functions

- Provides a service interface to the ALT router and injects routes in the ALT BGP when the site registers.
- Receives MAP requests over the ALT router and encapsulates them to registered ETRs.

Map resolver (MR): The MR performs the following functions:

- Receives MAP requests, which are encapsulated by ITRs.
- Provides a service interface to the ALT router, de-encapsulates MAP requests, and forwards on the ALT topology.
- Sends negative MAP replies in response to MAP requests for non-LISP sites.

ALT router (ALT): An ALT router is a router that runs External Border Gateway Protocol (eBGP) over an alternate Generic Routing Encapsulation (GRE) tunnel topology. It is an off-the-shelf router that does not run LISP.

#### QUESTION 143

In an SD-WAN deployment, which action in the vSmart controller responsible for?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

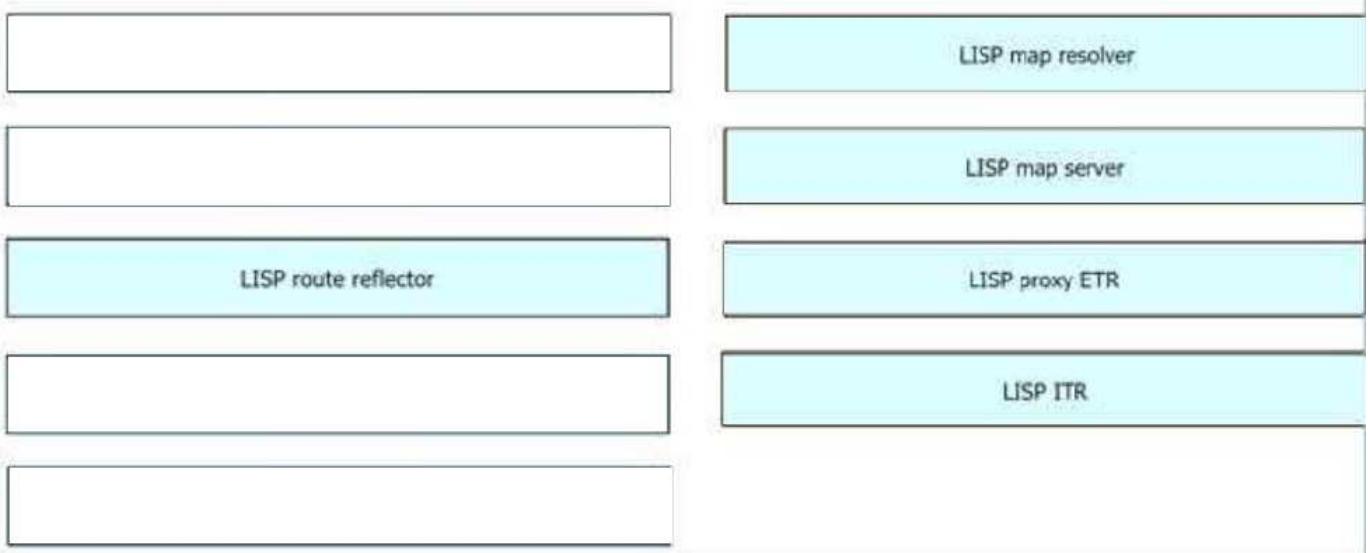
#### QUESTION 144

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

**Select and Place:**

|                      |                                                                 |
|----------------------|-----------------------------------------------------------------|
| LISP map resolver    | accepts LISP encapsulated map requests                          |
| LISP proxy ETR       | learns of EID prefix mapping entries from an ETR                |
| LISP route reflector | receives traffic from LISP sites and sends it to non-LISP sites |
| LISP ITR             | receives packets from site-facing interfaces                    |
| LISP map server      |                                                                 |

**Correct Answer:**



Section: (none)

Explanation

Explanation/Reference:

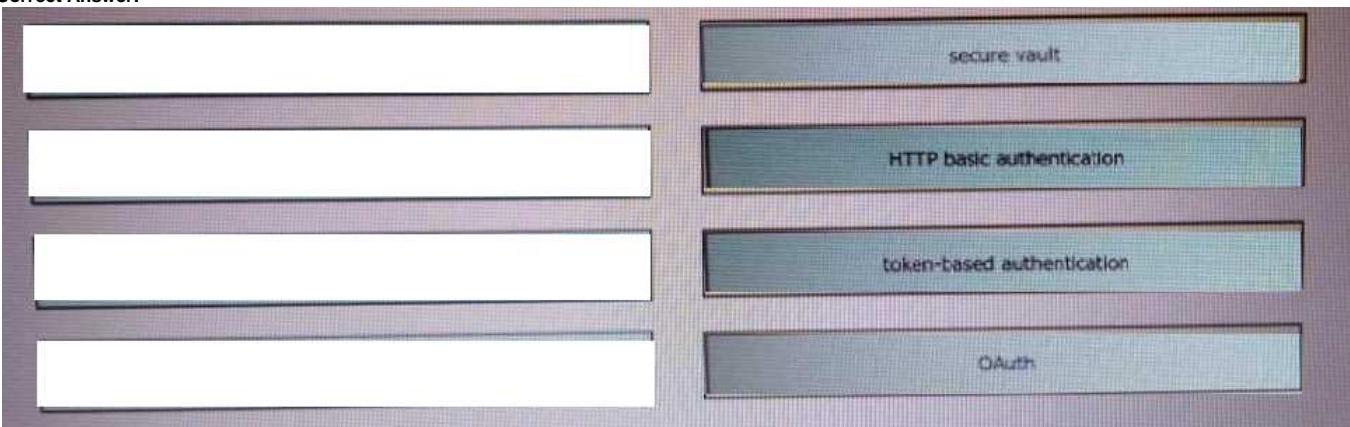
**QUESTION 145**

Drag and drop the REST API authentication method from the left to the description on the right.

Select and Place:



Correct Answer:



Section: (none)

Explanation

Explanation/Reference:

Vault is a tool for securely accessing secrets e.g. API keys, passwords, or certificates.

You can store your API Credentials and Tokens in the vault and get them securely when needed (e.g. obtain the tokens for accessing Cisco DNA API). Many vaults allow you to use API for getting the secrets.

**QUESTION 146**

What is the difference between CEF and process switching?

- A. CEF processes packets that are too complex for process switching to manage.
- B. CEF is more CPU-intensive than process switching.
- C. CEF uses the FIB and the adjacency table to make forwarding decisions, whereas process switching punts each packet.
- D. Process switching is faster than CEF.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 147**

How does the RIB differ from the FIB?

- A. The RIB is used to create network topologies and routing tables. The FIB is a list of routes to particular network destinations.
- B. The FIB includes many routes to a single destination. The RIB is the best route to a single destination.
- C. The RIB includes many routes to the same destination prefix. The FIB contains only the best route.
- D. The FIB maintains network topologies and routing tables. The RIB is a list of routes to particular network destinations.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Important:** Many variations in the choices can be created for this question. In General:

- RIB is populated / derived based on / from control plane.
- RIB contains network routing prefixes and is used to create routing tables.
- FIB is populated / derived based on / from RIB.
- FIB is a list of routes to particular destination. Each of them contains the egress interface / next hop address for reaching the destination.

**QUESTION 148**

Which two actions provide controlled Layer 2 network connectivity between virtual machines running on the same hypervisor? (Choose two.)

- A. Use a single trunk link to an external Layer2 switch.
- B. Use a virtual switch provided by the hypervisor.
- C. Use a virtual switch running as a separate virtual machine.
- D. Use a single routed link to an external router on stick.
- E. Use VXLAN fabric after installing VXLAN tunneling drivers on the virtual machines.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Most virtual switch provided by the hypervisor do not support custom configuration settings for controlling layer 2 traffic.

**QUESTION 149**

What is a type 1 hypervisor?

- A. runs directly on a physical server and depends on a previously installed operating system
- B. runs directly on a physical server and includes its own operating system
- C. runs on a virtual server and depends on an already installed operating system
- D. runs on a virtual server and includes its own operating system

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

NEW

**QUESTION 150**

How does SSO work with HSRP to minimize network disruptions?

- A. It enables HSRP to elect another switch in the group as the active HSRP switch.
- B. It ensures fast failover in the case of link failure.
- C. It enables data forwarding along known routes following a switchover, while the routing protocol reconverges.
- D. It enables HSRP to failover to the standby RP on the same device.

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 151**

Which two characteristics define the Intent API provided by Cisco DNA Center? (Choose two.)

- A. northbound API
- B. business outcome oriented

- C. device-oriented
- D. southbound API
- E. procedural

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 152**

How is a data modeling language used?

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

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 153**

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

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

**Correct Answer:** ACF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 154**

What are two reasons a company would choose a cloud deployment over an on-prem deployment? (Choose two.)

- A. In a cloud environment, the company controls technical issues. On-prem environments rely on the service provider to resolve technical issue.
- B. Cloud costs adjust up or down depending on the amount of resources consumed. On-prem costs for hardware, power, and space are ongoing regardless of usage.
- C. Cloud deployments require long implementation times due to capital expenditure processes. On-Prem deployments can be accomplished quickly using operational expenditure processes.
- D. Cloud resources scale automatically to an increase in demand. On-prem requires additional capital expenditure.
- E. In a cloud environment, the company is in full control of access to their data. On-prem risks access to data due to service provider outages.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 155**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 156**

What is the purpose of an RP in PIM?

- A. send join messages toward a multicast source SPT
- B. ensure the shortest path from the multicast source to the receiver
- C. receive IGMP joins from multicast receivers
- D. secure the communication channel between the multicast sender and receiver

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 157**

You are configuring a controller that runs Cisco IOS XE by using the CLI. Which three configuration options are used for 802.11w Protected Management Frames? (Choose three.)

- A. mandatory
- B. association-comeback
- C. SA teardown protection
- D. saquery-retry-time
- E. enable
- F. comeback-time

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

```
security pmf [ association-comeback association-comeback-time-in-seconds | mandatory | optional | saquery saquery-time-interval-milliseconds ]
```

**QUESTION 158**

During deployment, a network engineer notices that voice traffic is not being tagged correctly as it traverses the network. Which COS to DSCP map must be modified to ensure that voice traffic is treated properly?

- A. COS of 5 to DSCP 46
- B. COS of 7 to DSCP 48
- C. COS of 6 to DSCP 46
- D. COS of 3 to DSCP 26

**Correct Answer:** A

**Section:** (none)

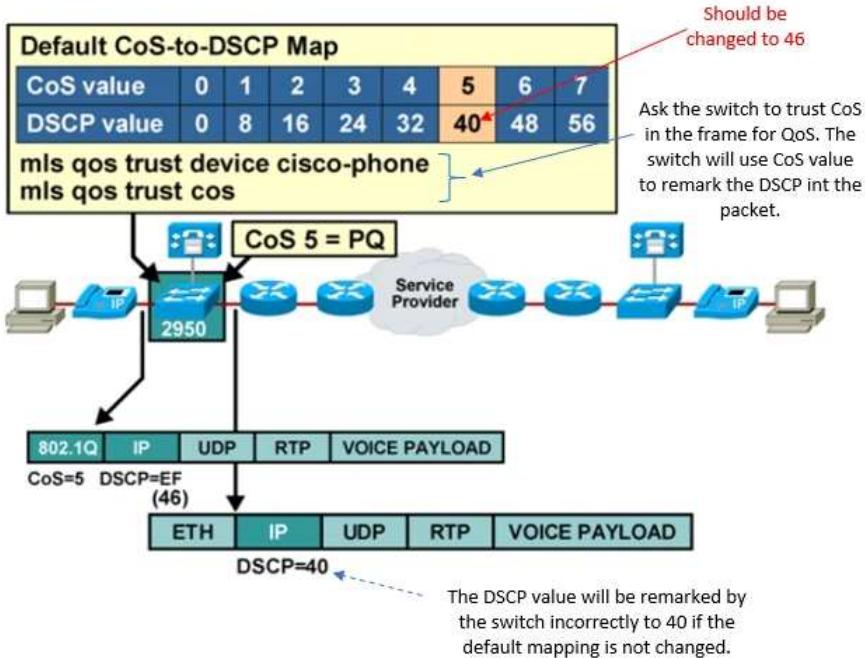
**Explanation**

**Explanation/Reference:**

Packets of VoIP traffic is often marked with the DSCP class called Expedited Forwarding (EF) with bits 1001110 (i.e. 46 in decimal value).

On the other hand, if a switch receives a VoIP packet which is carried by a Ethernet Frame marked with CoS 5 in the 802.1p field (a field in Dot1q for marking QoS setting), the switch can use the CoS to mark / remark the DSCP value in the IP header of the VoIP packet. Since Etherent frame for VoIP packet is often marked with CoS 5, the mapping should be set to CoS 5 --> DSCP value 46.

This mapping may be needed since some switch uses multiples of 8 for the default mapping between CoS and DSCP.



**QUESTION 159**

What would be the preferred way to implement a loopless switch network where there are 1500 defined VLANs and it is necessary to load the shared traffic through two main aggregation points based on the VLAN identifier?

- A. 802.1D
- B. 802.1S
- C. 802.1W
- D. 802.1AE

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 160**

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

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

**Correct Answer:** D

**Section:** (none)

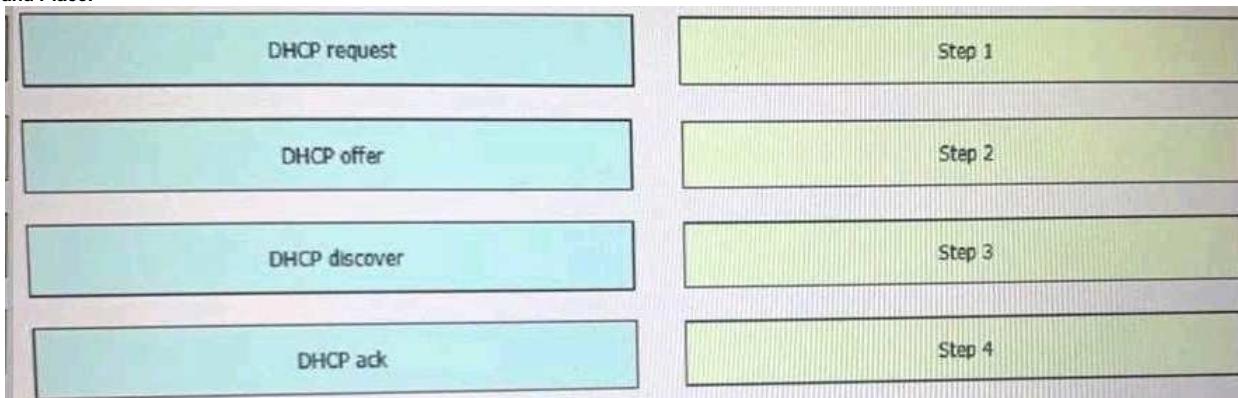
**Explanation**

**Explanation/Reference:**

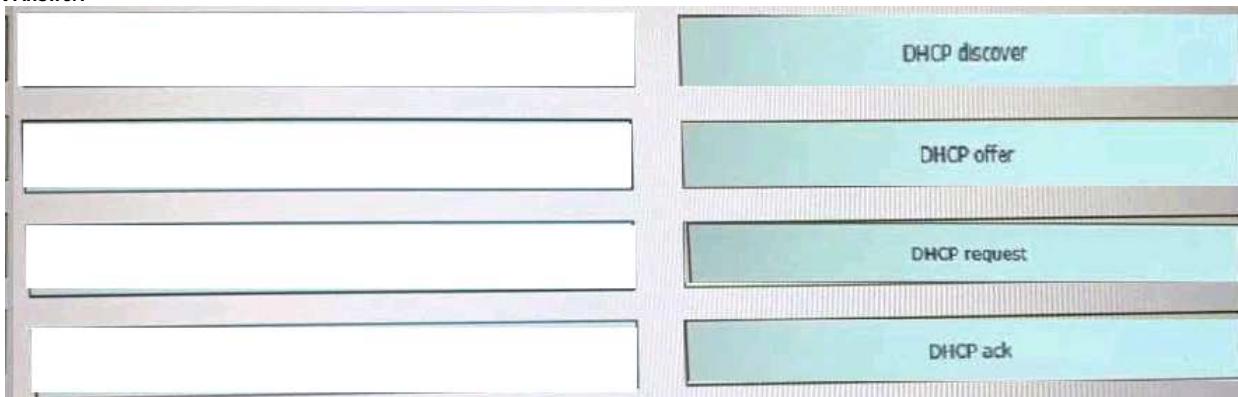
**QUESTION 161**

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

**Select and Place:**



**Correct Answer:**



**Section: Selected**  
**Explanation**

**Explanation/Reference:**

DORA

**QUESTION 162**

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

**Select and Place:**



**Correct Answer:**



**Section: Selected Explanation**

**Explanation/Reference:**

**QUESTION 163**

Refer to the exhibit.

```
event manager applet LARGECONFIG
event cli pattern "show running-config" sync yes
.action 1.0 puts "Warning! This device has a VERY LARGE configuration
and may take some time to process"
.action 1.1 puts nonewline "Do you wish to continue [Y/N]?"
.action 1.2 gets response
.action 1.3 string toupper "$response"
.action 1.4 string match "$_string_result" "Y"
.action 2.0 if $_string_result eq 1
.action 2.1 cli command "enable"
.action 2.2 cli command "show running-config"
.action 2.3 puts $_cli_result
.action 2.4 cli command "exit"
.action 2.9 end
```

Which two statements about the EEM applet configuration are true? (Choose two.)

- A. The EEM applet runs after the CLI command is executed
- B. The running configuration is displayed only if the letter Y is entered at the CLI
- C. The EEM applet runs before the CLI command is executed
- D. The EEM applet requires a case-insensitive response

**Correct Answer: CD**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

B is NOT correct since you can enter the lower-case "y" and there is an applet action 1.3 that converts it to the upper-case "Y" before evaluating the if statement.  
 E is therefore correct as you can enter "y" or "Y".

"sync yes" runs the applet actions first, the original CLI command that the user has typed may be run (although the CLI command will not be run since set\_exit\_status 1 is NOT configured in the action).

**QUESTION 164**

Which IPv6 migration method relies on dynamic tunnels that use the 2002::/16 reserved address space?

- A. GRE
- B. 6RD
- C. 6to4
- D. ISATAP

**Correct Answer: C**

**Section: (none)**

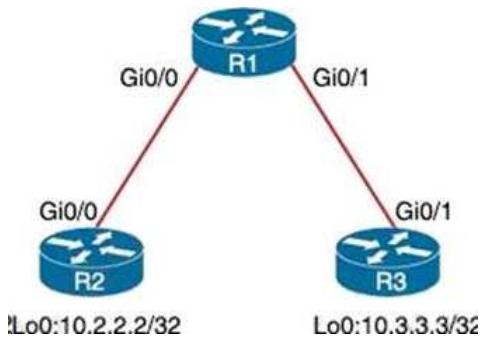
**Explanation**

**Explanation/Reference:**

This does not look like a question of the exam 350-401.

**QUESTION 165**

Refer to the exhibit.



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

Which command accomplish this task?

- A. R3(config)#time-range WEEKEND  
R3(config-time-range)#periodic Saturday Sunday 00:00 to 23:59  
R3(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND  
R3(config)#access-list 150 permit ip any any time-range WEEKEND  
R3(config)#interface Gi0/1  
R3(config-if)#ip access-group 150 out
- B. R1(config)#time-range WEEKEND  
R1(config-time-range)#periodic Friday Sunday 00:00 to 00:00  
R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND  
R1(config)#access-list 150 permit ip any any  
R1(config)#interface Gi0/1  
R1(config-if)#ip access-group 150 in
- C. R1(config)#time-range WEEKEND  
R1(config-time-range)#periodic weekend 00:00 to 23:59  
R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND  
R1(config)#access-list 150 permit ip any any  
R1(config)#interface Gi0/1  
R1(config-if)#ip access-group 150 in
- D. R3(config)#time-range WEEKEND  
R3(config-time-range)#periodic weekend 00:00 to 23:59  
R3(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND  
R3(config)#access-list 150 permit ip any any time-range WEEKEND  
R3(config)#interface Gi0/1  
R3(config-if)#ip access-group 150 out

**Correct Answer:** C

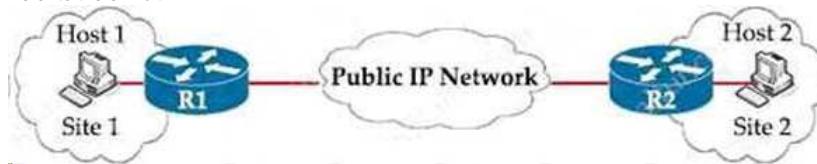
**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 166

Refer to the exhibit.



Which LISP component do routers in the public IP network use to forward traffic between the two networks?

- A. RLOC
- B. map resolver
- C. EID
- D. map server

**Correct Answer:** A

**Section:** (none)

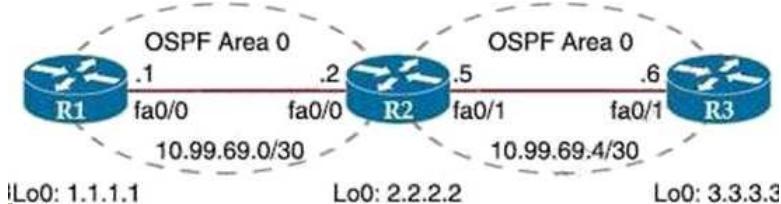
**Explanation**

**Explanation/Reference:**

Since RLOC (Routing Locator) is the IP address of the router connecting to the hosts / VMs, it can be routed by routers of the public IP network normally.

#### QUESTION 167

Refer to the exhibit.



```

R1#ping
Protocol [ip]:
Target IP address: 3.3.3.3
Repeat count [5]: 3
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 1.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]: yes
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: Record
Number of hops [9]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
Packet sent with the DF bit set
Packet has IP options: Total option bytes= 39, padded length=40
Record route: <">
(0.0.0.0)
(0.0.0.0)

:Unreachable from 10.99.69.2, maximum MTU 1492, Received packet has options
Total option bytes= 39, padded length=40
Record route: <">
(0.0.0.0)
(0.0.0.0)
<output omitted>

```

R1 is able to ping the R3 fa0/1 interface.

Why do the extended pings fail?

- A. The maximum packet size accepted by the command is 1476 bytes.
- B. R3 is missing a return route to 10.99.69.0/30
- C. R2 and R3 do not have an OSPF adjacency
- D. The DF bit has been set

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since you enter the following in the extended ping:

- Datagram size: 1500
  - Set DF bit in IP header: yes
- and the output of the ping shows "Unreachable from 10.99.69.2, maximum MTU 1492 ...".

The ping fails since its packets of 1500 bytes cannot be fragmented for sending through a link with 1492.

#### QUESTION 168

Refer to the exhibit.

\*\*\* missing diagram for standard browser warning message about "YOUR CONNECTION IS NOT PRIVATE WARNING" \*\*\*

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

Which issue is occurring?

- A. The server that is providing the portal has an expired certificate
- B. The server that is providing the portal has a self-signed certificate
- C. The connection is using an unsupported protocol
- D. The connection is using an unsupported browser

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 169

Which two statements about HSRP are true? (Choose two)

- A. It supports unique virtual MAC addresses
- B. Its virtual MAC is 0000.0C07.ACxx
- C. Its default configuration allows for pre-emption
- D. It supports tracking
- E. Its multicast virtual MAC is 0000.5E00.01xx

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Important :** More characteristics...

- Hello and hold timers of two peers does NOT need to be matched.
- Authentication is supported but the case-sensitive key string configured in the key chain of both peers must match (e.g. "cisco" and "Cisco" do NOT match and this will cause both peers to become Active).

#### QUESTION 170

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

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

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 171

**Select and Place:**

|                |                                                                 |
|----------------|-----------------------------------------------------------------|
| service policy | mechanism to create a scheduler for packets prior to forwarding |
| shaping        | mechanism to apply a QoS policy to an interface                 |
| DSCP           | portion of the IP header used to classify packets               |
| policy map     | bandwidth management technique which delays datagrams           |
| policing       | tool to enforce rate-limiting on ingress/egress                 |
| CoS            | portion of the 802.1Q header used to classify packets           |

**Correct Answer:**

|  |                |
|--|----------------|
|  | policy map     |
|  | service policy |
|  | DSCP           |
|  | shaping        |
|  | policing       |
|  | CoS            |

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 172**

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

- A. ip access-list extended 100  
  deny tcp host 10.10.10.1 any eq 80  
  permit ip any any
- B. ip access-list extended 200  
  deny tcp host 10.10.10.1 eq 80 any  
  permit ip any any
- C. ip access-list extended NO\_HTTP  
  deny tcp host 10.10.10.1 any eq 80
- D. ip access-list extended 10  
  deny tcp host 10.10.10.1 any eq 80  
  permit ip any any

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

D is wrong since 10 is not the range for extended ACL.

**QUESTION 173**

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

Which of the followings are the characteristics of OSPF (Choose two)?

- A. summaries can be created anywhere in the IGP topology
- B. uses areas to segment a network
- C. DUAL algorithm
- D. summarizes can be created in specific parts of the IGP topology

**Correct Answer: BD**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 174**

Which statement about the default QoS configuration on a Cisco switch is true?

- A. The Cos value of each tagged packet is modified
- B. Port trust is enabled
- C. The Port Cos value is 0
- D. All traffic is sent through four egress queues

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 175**

Refer to the exhibit.

\*Jun19 11:12: BGP(4):10.1.1.2 rcvd UPDATE w/ attr:nexthop 10.1.1.2, origin ?, localpref 100,metric 0,extended community RT:999:999  
 \*Jun19 11:12: BGP(4):10.1.1.2 rcvd 999:999:192.168.1.99/32,label 29--DENIED due to extended community not supported

You have just created a new VRF on PE3.

You have enabled debug ip bgp vpnv4 unicast updates on PE1, and you can see the route in the debug, but not in the BGP VPNv4 table.

Which two statements are true? (Choose two)

- A. After you configure route-target import 999:999 for a VRF on PE1, the route will be accepted
- B. VPNv4 is not configured between PE1 and PE3
- C. address-family ipv4 vrf is not configured on PE3
- D. PE1 will reject the route due to automatic route filtering
- E. After you configure route-target import 999:999 for a VRF on PE3, the route will be accepted

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

This does not look like a question of the exam 350-401.

#### QUESTION 176

Which two statements about Cisco Express Forwarding load balancing are true? (Choose two)

- A. Each hash maps directly to a single entry in the RIB
- B. It combines the source IP address subnet mask to create a hash for each destination
- C. Cisco Express Forwarding can load-balance over a maximum of two destinations
- D. It combines the source and destination IP addresses to create a hash for each destination
- E. Each hash maps directly to a single entry in the adjacency table

**Correct Answer:** DE

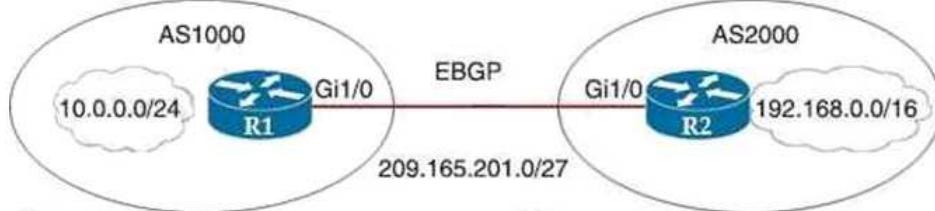
**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 177

Refer to the exhibit.



R1

```
router bgp 1000
address-family ipv4 unicast
neighbor 209.165.201.2 remote-as 2000
network 10.0.0.0 mask 255.255.255.0
description Peer Router B
```

R2

```
router bgp 2000
address-family ipv4 unicast
neighbor 209.165.201.1 remote-as 1000
network 10.0.0.0 mask 255.255.255.0
description Peer Router A
```

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

**Correct Answer:** BC

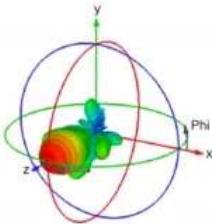
**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 178

Refer to the exhibit.



Which type of antenna do the radiation patterns present?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 179

Refer to the exhibit.

```

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

```

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

username CCNP autocommand show run

If the above is configured, after the user CCNP has authenticated, the "show run" command will be run automatically. Then the session will terminate automatically.

#### QUESTION 180

Refer to the exhibit.

```

R1
interface GigabitEthernet0/0
ip address 192.168.0.2 255.255.255.0
standby 1 ip 192.168.0.1
standby 1 priority 120

```

```

R2
interface GigabitEthernet0/0
ip address 192.168.0.3 255.255.255.0
standby 1 ip 192.168.0.1
standby 1 priority 110

```

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

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

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

For C, it assumes that the two router boots / is configured with HSRP at the same time.

For E, HSRP is not enabled with Pre-empt by default.

#### QUESTION 181

Refer to the exhibit.

```

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

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

```

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Destination is not configured. If it is configured, the output will be shown similar to the following:

```

Session 1
-----
Type : Remote Destination Session
Source RSPAN VLAN : 50
Destination Ports : Fa0/9

```

#### QUESTION 182

Which technology is used to provide Layer 2 and Layer 3 logical networks in the Cisco SD-Access architecture?

- A. underlay network
- B. VPN routing and forwarding
- C. easy virtual network
- D. overlay network

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 183

Refer to the exhibit.

```

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

```

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

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

**Correct Answer:** A

**Section:** Selected

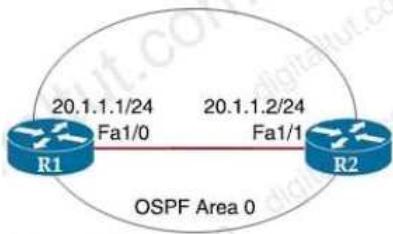
**Explanation**

**Explanation/Reference:**

An example is: You want to show the running configuration with filtering for interface g1/2 but the interface does not exist in the device.

#### QUESTION 184

Refer to the exhibit



```

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

```

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

- A. network 20.1.1.2 255.255.255.255 area 0
- B. network 20.1.1.2 0.0.255.255 area 0
- C. network 20.1.1.2 0.0.0.0 area 0
- D. network 20.1.1.2 255.255.0.0 area 0

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The network command in R2 does not cover 20.1.1.2/24.

There are more than one answers since most IOS can perform the following conversion::

- network mask to wildcard mask automatically. AND/OR
- network address 20.1.1.2 will be converted to 20.1.0.0 if the wildcard mask is 0.0.255.255

For example: network 192.168.1.2 255.255.0.0 area 0 will be changed by Cisco IOS to:  
network 192.168.0.0 0.0.255.255 area 0

However, in general, the followings are usually recommended:

network 20.1.1.2 0.0.0.0 area 0 OR  
network 20.1.1.0 0.0.0.255 area 0

Hence, C is the best answer.

#### QUESTION 185

Refer to the exhibit.

```

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

A different port number is needed since you want to use the same destination IP.

#### QUESTION 186

Refer to the exhibit.

DSW1#show spanning-tree

MST1

Spanning tree enabled protocol mstp  
Root ID Priority 32769  
Address 0018.7363.4300  
Cost 2  
Port 13 (FastEthernet1/0/11)  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

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

| Interface | Role     | Sts | Cost   | Prio.Nbr | Type             |
|-----------|----------|-----|--------|----------|------------------|
| Fa1/0/7   | Desg FWD | 2   | 128.1  | 32769    | P2p Bound (PVST) |
| Fa1/0/10  | Desg FWD | 2   | 128.12 | 32769    | P2p Bound (PVST) |
| Fa1/0/11  | Root FWD | 2   | 128.13 | 32769    | P2p              |
| Fa1/0/12  | Altn BLK | 2   | 128.14 | 32769    | P2p              |

DSW1#show spanning-tree mst

##### MST1 vlans mapped: 10,20  
Bridge address 001b.0d0e.e000 priority 32769 (32768 sysid 1)  
Root address 0018.7363.4300 priority 32769 (32768 sysid 1)  
port Fa1/0/11 cost 2 (rem hops 19)

----- output omitted -----

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

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

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

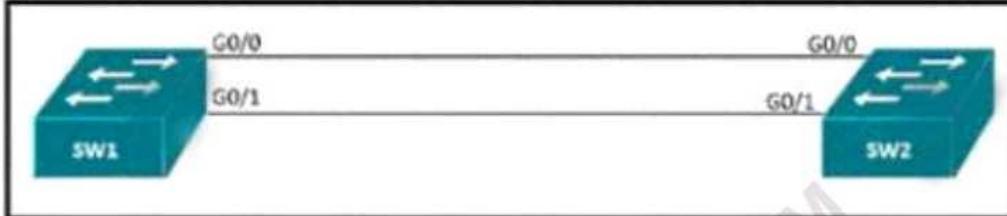
For C, "1" is not an acceptable priority since not 4096 increments.

Note that although MST is not a Per-VLAN STP, since the number of MST configurable is 0-4094, the same increment rules applies to the configuration of bridge priority.

```
Switch(config-mst)#instance ?  
<0-4094> MST instance id  
  
Switch(config)#spanning-tree mst 1 priority ?  
<0-61440> bridge priority in increments of 4096
```

**QUESTION 187**

Refer to the exhibit



An engineer reconfigures the portchannel between SW1 and SW2 from an access port to a trunk and immediately notices this error in SW1's log:  
%PM-SP-4-ERR\_DISABLE: bpduerror detected on Gi0/0, putting Gi0/0 in err-disable state

Which command set can resolves this error?

- A. interface Gi0/0  
spanning-tree bpduerror enable  
shut  
no shut
- B. interface Gi0/0  
no spanning-tree bpduerror enable  
shut  
no shut
- C. interface Gi0/0  
no spanning-tree bpdufilter  
shut

no shut  
D. interface Gi0/1  
spanning-tree bpduguard enable  
shut  
no shut

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**  
BPDU Guard is not enabled by default. Most probably someone had configured it in Sw1 port g0/0 previously.  
After disabling BPDU Guard, you need to shut and then no shut to clear the err-disable state.

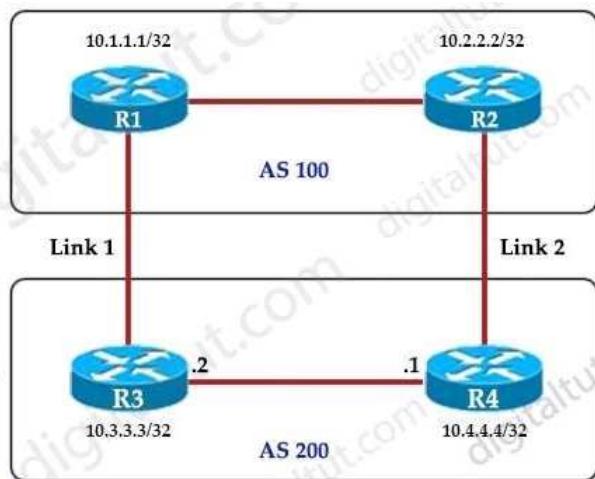
**QUESTION 188**  
Which of the followings are characteristics for On-Premises Infrastructure? (Choose 3)

- A. enterprise owns the hardware
- B. low capital expenditure
- C. provider maintains the infrastructure
- D. slow upgrade lifecycle
- E. high capital expenditure
- F. fast upgrade lifecycle

**Correct Answer:** ADE  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**  
The remaining choices i.e. BCF are the characteristics for Cloud-Hosted Infrastructure.

**QUESTION 189**  
Refer to the exhibit.



An engineer must ensure that all traffic leaving AS 200 will choose R4's as the exit point to networks in other ASs. Assuming that all BGP neighbor relationships have been formed and that the attributes have not been changed on any of the routers, which configuration accomplishes this task?

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

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**  
Since weight affects the configured router only, C is required since all BGP routes announced by R4 to R3 will have a higher local preference.

**QUESTION 190**  
What is the result of applying this access control list?

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

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

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

For others, they are only allowed if additional ACK or RST bit is also set.

**QUESTION 191**

Refer to the exhibit

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

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

- A. The RSPAN VLAN is replaced by VLAN 223.
- B. RSPAN traffic is sent to VLANs 222 and 223.
- C. An error is flagged for configuring two destinations.
- D. RSPAN traffic is split between VLANs 222 and 223.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Only one remote vlan is allowed for each RSPAN monitor session.

**QUESTION 192**

Refer to the exhibit.

```
<errors xmlns="urn:ietf:params:xml:ns:yang:ietf-restconf">
  <error>
    <error-message>End-of-file reached in XML
stream</error-message>
    <error-path>/ietf-interfaces:interfaces/interface=Gigabi
tEthernet2</error-path>
    <error-tag>malformed-message</error-tag>
    <error-type>application</error-type>
  </error>
</errors>
```

An engineer is using XML in an application to send information to a RESTCONF-enabled device. After sending the request, the engineer gets this response message and a HTTP response code of 400. What do these responses tell the engineer?

- A. The Accept header sent was application/xml.
- B. POST was used instead of PUT to update
- C. The Content-Type header sent was application/xml.
- D. JSON body was used.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The error message mentioned errors in the XML data received. Probably the request has a content header set to use XML i.e. "application/yang-data+xml" but JSON data content is actually included.

Remarks :

Note that "application/xml" is not an acceptable content type in RESTCONF and the following error message will be received instead.

```
<errors xmlns="urn:ietf:params:xml:ns:yang:ietf-restconf">
  <error>
    <error-message>Unsupported media type: application/xml ; Should be one of: application/yang-data+xml, application/
yang-data+json.</error-message>
    <error-tag>malformed-message</error-tag>
    <error-type>application</error-type>
  </error>
</errors>
```

**QUESTION 193**

Refer to the exhibit.

**General Security QoS Policy-Mapping Advanced**

**Layer 2 Layer 3 AAA Servers**

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

**Radius Servers**

Radius Server Overwrite interface  Enabled

Interface Priority **WLAN**

<b>Authentication Servers</b>		<b>Accounting Servers</b>	
<input checked="" type="checkbox"/> Enabled		<input checked="" type="checkbox"/> Enabled	
Server 1	None	None	
Server 2	None	None	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	

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

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

**Correct Answer: B**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

The controller sources RADIUS traffic from the IP address of its management interface unless the configured RADIUS server exists on a VLAN accessible via one of the controller Dynamic interfaces. If a RADIUS server is reachable via a controller Dynamic interface, RADIUS requests to this specific RADIUS server will be sourced from the controller via the corresponding Dynamic interface.

By default, RADIUS packets sourced from the controller will set the NAS-IP-Address attribute to that of the management interface's IP Address, regardless of the packet's source IP Address (Management or Dynamic, depending on topology).

When you enable per-WLAN RADIUS source support (Radius Server Overwrite interface as shown in the diagram) the NAS-IP-Address attribute is overwritten by the controller to reflect the sourced interface. Also, RADIUS attributes are modified accordingly to match the identity. This feature virtualizes the controller on the per-WLAN RADIUS traffic, where each WLAN can have a separate layer 3 identity.

**QUESTION 194**

Refer to this output.

```
R1# *Feb 14 37:09:53.129: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

What is the logging severity level?

- A. notification
- B. error
- C. informational
- D. warnings

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Severity Level	Level Name	Description
0	Emergencies	System unusable
1	Alerts	Immediate action needed
2	Critical	Critical conditions
3	Errors	Error conditions
4	Warnings	Warning conditions
5	Notifications	Normal but significant conditions
6	Informational	Informational messages only
7	Debugging	Debugging messages

**QUESTION 195**

Refer to the exhibit.

```

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

```

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

By default, GRE is the tunnel mode and the keepalive is not set.

However if you enable keepalive by the command "keepalive" without specifying period, the default value is 10 seconds. Therefore the keepalive value in the above tunnel has not been changed.

The following lines are normal and will be shown if you configure an interface as the tunnel source:

```

Tunnel Subblocks:
src-track:
.....

```

**QUESTION 196**

Refer to the exhibit.

```

!
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
!
```

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

- A. ip nat outside source static 192.168.0.1 10.0.0.0 overload
- B. ip nat inside source list 10 interface FastEthernet0/1 overload
- C. ip nat outside source list 10 interface FastEthernet0/2 overload
- D. ip nat inside source list 10 interface FastEthernet0/2 overload

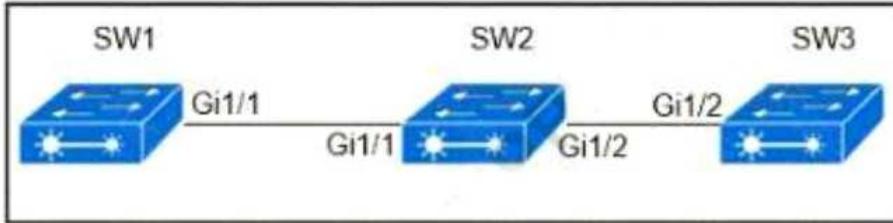
**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 197**



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

- A. Sw1:  
int g1/1  
switchport trunk allowed vlan 1-9,11-4094
- B. Sw2:  
int g1/2  
switchport trunk allowed vlan 10
- C. Sw2:  
int g1/2  
switchport trunk allowed vlan 1-9,11-4094
- D. Sw1:  
int g1/1  
switchport trunk allowed vlan 10

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 198**

Which of the followings are the characteristics of OSPF? (Choose 3)

- A. maintains alternative loop-free backup path if available
- B. Link State Protocol
- C. selects routes using the DUAL algorithm
- D. supports only equal multipath load balancing
- E. Advanced Distance Vector Protocol
- F. quickly computes new path upon link failure

**Correct Answer:** BDF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The remainings are the characteristics of EIGRP. Since EIGRP has feasible successor, there is no need to compute the backup path.

**QUESTION 199**

A client with IP address 209.165.201.25 must access a web server on port 8080 at 209.165.200.225. To allow this traffic, an engineer must add a statement to an access control list that is applied in the inbound direction on the port connecting to the web server.

Which statement allows this traffic?

- A. permit tcp host 209.165.200.225 lt 8080 host 209.165.201.25
- B. permit tcp host 209.165.201.25 host 209.165.200.225 eq 8080
- C. permit tcp host 209.165.200.225 eq 8080 host 209.165.201.25
- D. permit tcp host 209.165.200.225 host 209.165.201.25 eq 8080

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 200**

An engineer must configure interface GigabitEthernet0/0 for VRRP group 10. When the router has the highest priority in the group, it must assume the master role. Which command set must be added if the interface must be added to the initial configuration to accomplish this task?

## Initial Configuration

```
interface GigabitEthernet0/0
description to IDF
ip address 172.16.13.2 255.255.255.0
```

- A. vrrp 10 ip 172.16.13.254  
vrrp 10 preempt
- B. standby 10 ip 172.16.13.254  
standby 10 priority 120
- C. vrrp group 10 ip 172.16.13.254 255.255.255.0  
vrrp group 10 priority 120
- D. standby 10 ip 172.16.13.254 255.255.255.0  
standby 10 preempt

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Only A is valid configuration for VRRP (although preempt is actually enabled by default)  
C is wrong since the word "group" is not accepted.

## QUESTION 201

Refer to the exhibit:

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

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

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Only D seems reasonable. However since it is missing the details about access list 120, it should be written as:  
all traffic matching access-list 120 will be policed based on the rate configured.

## QUESTION 202

Which deployment option of Cisco NGFW provides scalability?

- A. clustering
- B. inline tap
- C. tap

D. high availability

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Firepower Threat Defense (FTD) is a unified software image that can be installed on Cisco NGFW or VMs.:.

## FTD Clustering Basics

- Designed to solve two critical issues with firewall HA:
  - Aggregates firewall capacities for DC environments (bandwidth, connections/sec, etc.)
  - Provides dynamic N+1 stateful redundancy with zero packet loss
- Two types of clustering:
  - Intra-chassis clustering – Supported (9300 only)
  - Inter-chassis clustering – Supported (4100 or 9300)

Highly Reliable  
Scalable  
Available

### QUESTION 203

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

EID-to-RLOC mapping is a single entry.

### QUESTION 204

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

- A. class-map match-all CoPP\_SSH  
match access-group name CoPP\_SSH  
!  
policy-map CoPP\_SSH  
class CoPP\_SSH  
police cir 100000  
exceed-action drop  
!  
!  
interface GigabitEthernet0/1  
ip address 209.165.200.225 255.255.255.0  
ip access-group EGRESS out  
duplex auto  
speed auto  
media-type rj45  
service-policy input CoPP\_SSH  
!  
ip access-list extended CoPP\_SSH  
permit tcp any any eq 22  
!
- B. class-map match-all CoPP\_SSH  
match access-group name CoPP\_SSH  
!  
policy-map CoPP\_SSH  
class CoPP\_SSH  
police cir CoPP\_SSH  
exceed-action drop  
!  
!  
interface GigabitEthernet0/1  
ip address 209.165.200.225 255.255.255.0  
ip access-group EGRESS out  
duplex auto  
speed auto  
media-type rj45  
service-policy input CoPP\_SSH  
!  
ip access-list extended CoPP\_SSH  
deny tcp any any eq 22  
!
- C. class-map match-all CoPP\_SSH

```

match access-group name CoPP_SSH
!
policy-map CoPP_SSH
class CoPP_SSH
police cir 100000
exceed-action drop
!
!
control-plane
service-policy input CoPP_SSH
!
ip access-list extended CoPP_SSH
deny tcp any any eq 22
!
D. class-map match-all CoPP_SSH
match access-group name CoPP_SSH
!
policy-map CoPP_SSH
class CoPP_SSH
police cir 100000
exceed-action drop
!
!
control-plane transit
service-policy input CoPP_SSH
!
ip access-list extended CoPP_SSH
permit tcp any any eq 22
!

```

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

B and C are NOT correct since the rule in the Access List denies port 22 traffic.

D is NOT correct since Control plane transit does not apply to packets sending to the router.

A is the only answer that can match SSH traffic for policing.

However since A is a service policy applied to an interface, it will also police other SSH traffic passing through the router.

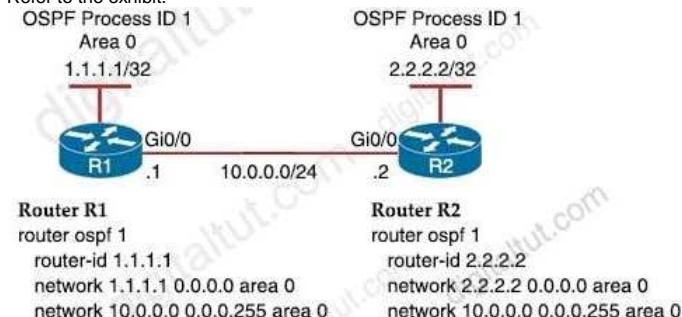
If the action in the rule of the access list in choice C is permit instead of deny, then C is the best answer. A better answer for this question should be a CoPP policy with permit rule for matching SSH traffic but this choice is not available in this question. The choice C of this question is changed in Question 667 (the deny rule is changed to permit rule in the ACL "CoPP\_SSH"). Therefore, C is the best answer in Question 667.

**Remarks :**

**Control plane transit** subinterface: This subinterface receives all control plane IP traffic that is software switched by the route processor. This traffic consists of packets that are not directly destined to the router itself but rather are traffic traversing through the router. Nonterminating tunnels handled by the router are an example of this type of control plane traffic. Control Plane Protection allows specific aggregate policing of all traffic received at this subinterface.

## QUESTION 205

Refer to the exhibit.



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

Which configuration set accomplishes this goal?

- A. R1(config-if)#interface Gi0/0
 R1(config-if)#ip ospf network point-to-point
 R2(config-if)#interface Gi0/0
 R2(config-if)#ip ospf network point-to-point
- B. R1(config-if)#interface Gi0/0
 R1(config-if)#ip ospf network broadcast
 R2(config-if)#interface Gi0/0
 R2(config-if)#ip ospf network broadcast
- C. 1(config-if)#interface Gi0/0
 R1(config-if)#ip ospf database-filter all out
 R2(config-if)#interface Gi0/0
 R2(config-if)#ip ospf database-filter all out
- D. R1(config-if)#interface Gi0/0
 R1(config-if)#ip ospf priority 1
 R2(config-if)#interface Gi0/0
 R2(config-if)#ip ospf priority 1

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 206**

Which statement about a Cisco APIC controller versus a more traditional SDN controller is true?

- A. APIC does support a Southbound REST API
- B. APIC supports OpFlex as a Northbound protocol
- C. APIC uses a policy agent to translate policies into instructions
- D. APIC uses an imperative model

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 207**

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

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

- A. 

```
router eigrp 1
network 10.0.0.0 255.255.255.0
network 172.16.0.0 255.255.255.0
network 192.168.1.0 255.255.255.0
```
- B. 

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

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

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

Correct Answer: C

Section: (none)

Explanation

**Explanation/Reference:**

Packets cannot be routed between different VRFs unless inter-VRF routing (e.g. route target and MP-BGP) is configured. If VRFs is not required, you can remove them. However after VRF settings are configured / changed, you need to reconfigure IP addresses.

**QUESTION 208**

What is used to measure the total output energy of a Wi-Fi device?

- A. dBi
- B. EIGRP
- C. mW
- D. dBm

**Correct Answer:** C

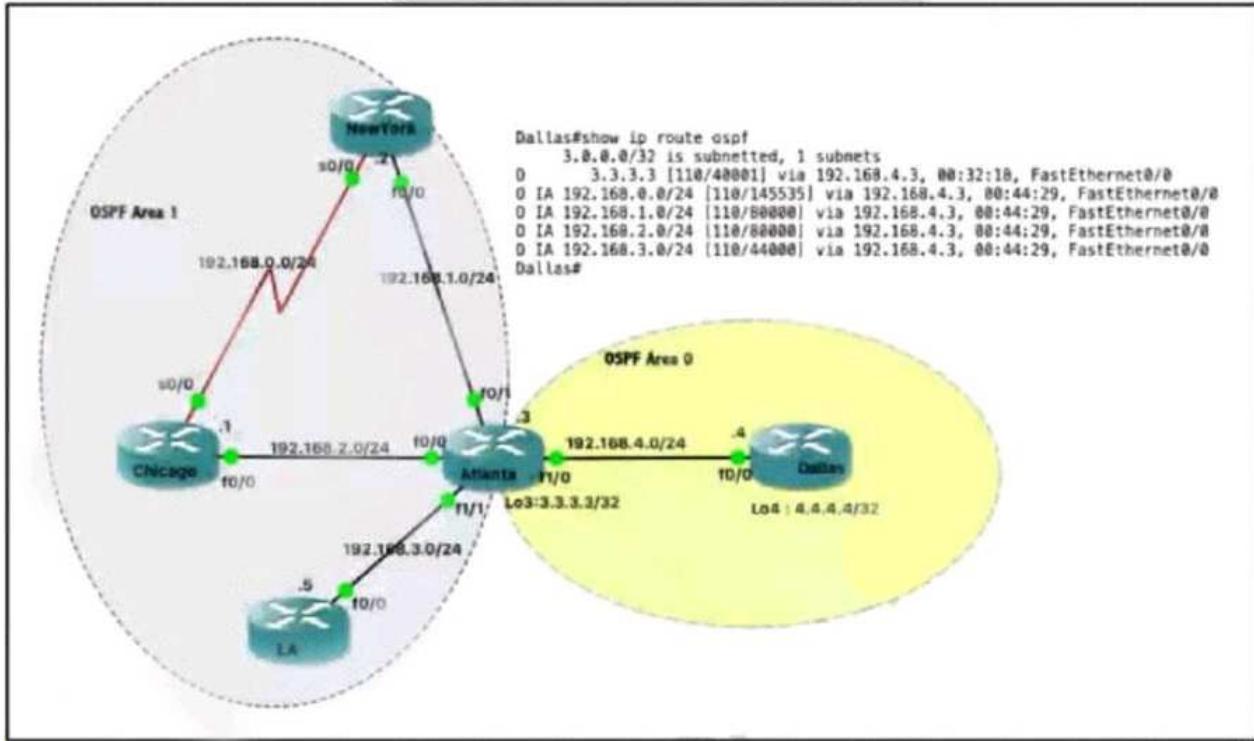
**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 209**

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



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

**Correct Answer:** C

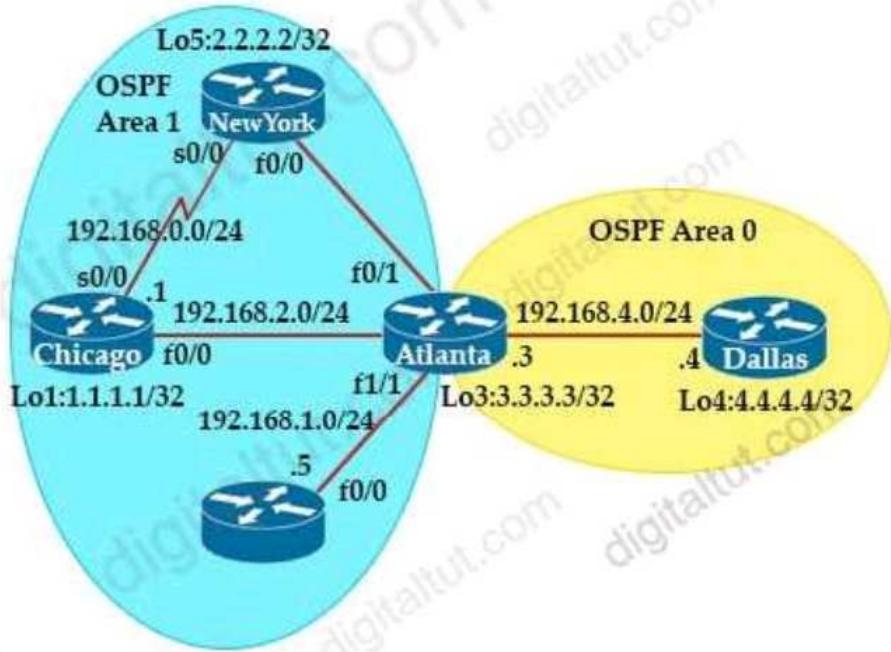
**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 210**

Refer to the exhibit.



Chicago#show ip ospf nei

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	FULL/BDR	00:00:35	192.168.2.3	FastEthernet0/0
2.2.2.2	0	FULL/ -	00:00:35	192.168.0.2	Serial0/0

Chicago#show ip ospf int bri

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Fa0/0	1	1	192.168.2.1/24	40444	DR	1/1	
Se0/0	1	1	192.168.0.1/24	65535	P2P	1/1	

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

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

**Correct Answer:** B

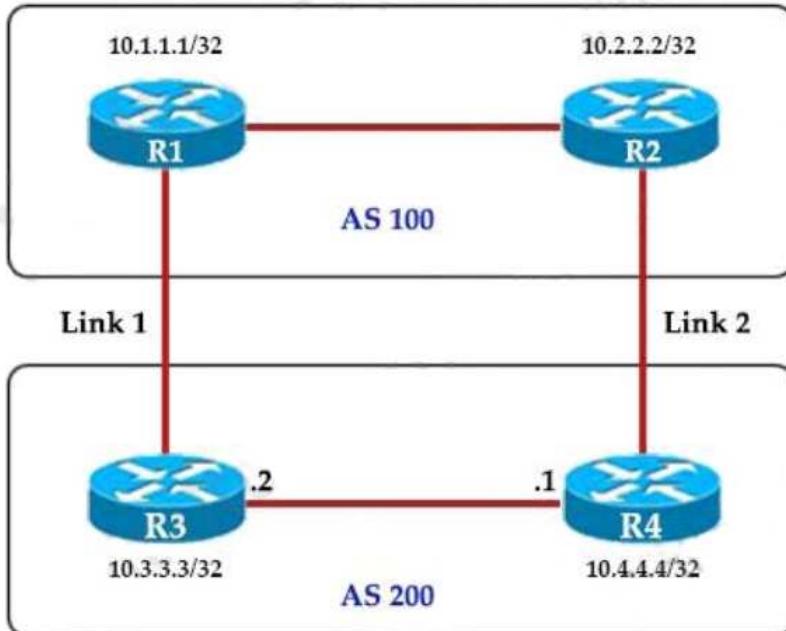
**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 211

Refer to the exhibit.



An engineer must ensure that all traffic entering AS 200 from AS 100 chooses Link 2 as the entry point. Assuming that all BGP neighbor relationships have been formed and that the attributes have not been changed on any of the routers, which configuration accomplish task?

- A. R3(config)# route-map PREPEND permit 10  
R3(config-route-map)# set as-path prepend 100 100 100  
  
R3(config)# router bgp 200  
R3(config-router)# neighbor 10.1.1.1 route-map PREPEND in
- B. R4(config)# route-map PREPEND permit 10  
R4(config-route-map)# set as-path prepend 100 100 100  
  
R4(config)# router bgp 200  
R4(config-router)# neighbor 10.2.2.2 route-map PREPEND in
- C. R3(config)# route-map PREPEND permit 10  
R3(config-route-map)# set as-path prepend 200 200 200  
  
R3(config)# router bgp 200  
R3(config-router)# neighbor 10.1.1.1 route-map PREPEND out
- D. R4(config)# route-map PREPEND permit 10  
R4(config-route-map)# set as-path prepend 200 200 200  
  
R4(config)# router bgp 200  
R4(config-router)# neighbor 10.2.2.2 route-map PREPEND out

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

After R3 sending BGP routes with prepended AS to AS 100, the AS path list will be longer than those received from R4. Hence BGP routers in AS 100 will prefer R4 i.e. Link 2.

Remarks : Other ways to prefer Link 2

- Configure R3 to send BGP routes with MED value. OR
- Configure R2 to add Local Preference value > 100 to routes received from R4.

**QUESTION 212**

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

R1	R2
key chain cisco123	key chain cisco123
key 1	key 1
key-string Cisco123!	key-string Cisco123!
Ethernet0/0 - Group 10	Ethernet0/0 - Group 10
State is Active	State is Active
8 state changes, last state change 00:03:33	17 state changes, last state change 00:03:33
Virtual IP address is 192.168.0.1	Virtual IP address is 192.168.0.1
Active virtual MAC address is 0000.0c07.ac0a	Active virtual MAC address is 0000.0c07.ac0a

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

**Correct Answer:** A  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**  
From the virtual MAC address, the FHRP being implemented is HSRPv1.

**QUESTION 213**  
Which two statements about VRRP are true? (Choose two)

- A. It supports both MD5 and SHA1 authentication
- B. It is assigned multicast address 224.0.0.9.
- C. Three versions of the VRRP protocol have been defined.
- D. It is assigned multicast address 224.0.0.8.
- E. The TTL for VRRP packets must be 255.
- F. Its IP address number is 115.

**Correct Answer:** CE  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

Router(config)#fhrp version vrrp ?  
v2 Legacy VRRP - VRRPv2 for IPv4  
v3 Unified VRRP - VRRPv3 for IPv4 and IPv6

Both versions uses the same multicast address 224.0.0.18 and the same range of virtual MAC address i.e. 0000.5E00.01xx

For VRRP, the TTL MUST be set to 255. A VRRP router receiving a packet with the TTL not equal to 255 MUST discard the packet.

**QUESTION 214**  
In a Cisco SD-WAN solution, how is the health of a data plane tunnel monitored?

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

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

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

**QUESTION 215**  
Which two statements about IP SLA are true? (Choose two)

- A. It uses NetFlow for passive traffic monitoring
- B. It can measure MOS
- C. The IP SLA responder is a component in the source Cisco device
- D. It is Layer 2 transport-independent
- E. It uses active traffic monitoring
- F. SNMP access is not supported

**Correct Answer:** DE  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

B can also be true but Voice MOS measurement can only be obtained by using UDP jitter operation.  
Therefore D and E are best answers.

**QUESTION 216**  
Refer to the exhibit. Which network script automation option or tool is used in the exhibit?

<https://mydevice.mycompany.com/getstuff?queryName=errors&queryResults=yes>

- A. EEM
- B. Bash script
- C. REST
- D. NETCONF
- E. Python

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 217**  
An engineer uses the Design workflow to create a new network infrastructure in Cisco DNA Center. How is the physical network device hierarchy structured?

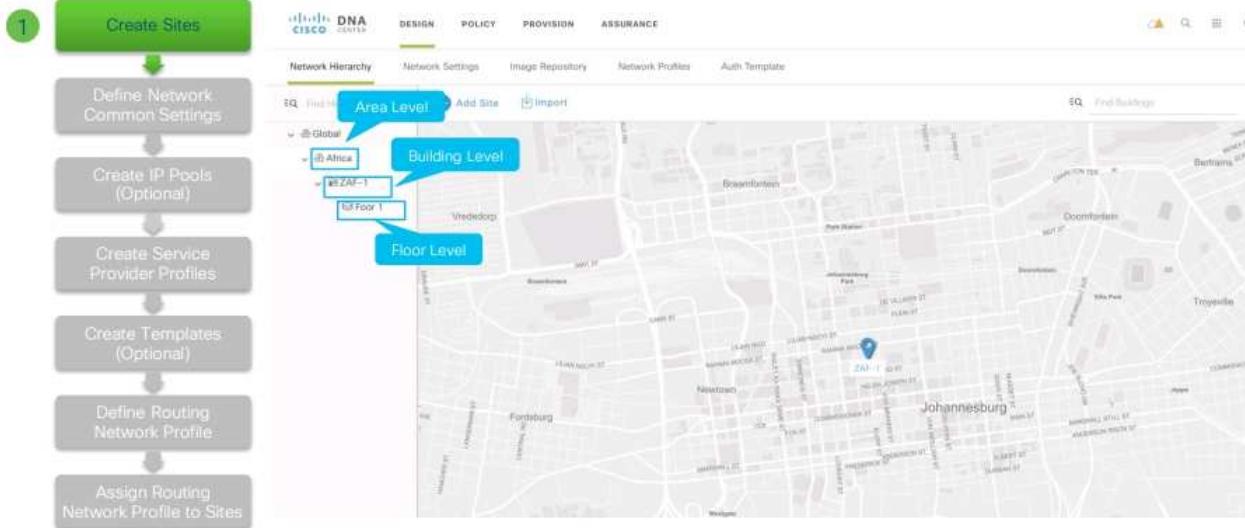
- A. by location
- B. by role
- C. by organization
- D. by hostname naming convention

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 218

What function does vxlan perform in an SD-Access deployment?

- A. policy plane forwarding
- B. control plane forwarding
- C. data plane forwarding
- D. systems management and orchestration

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 219

Into which two pieces of information does the LISP protocol split the device identity? (Choose two)

- A. Device ID
- B. Enterprise Identifier
- C. LISP ID
- D. Routing Locator
- E. Resource Location
- F. Endpoint Identifier

**Correct Answer:** DF

**Section:** (none)

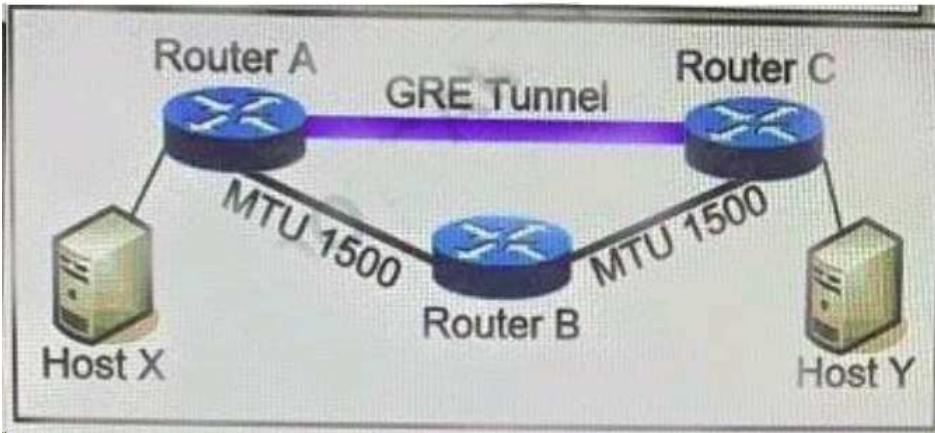
**Explanation**

**Explanation/Reference:**

They are EID and RLOC

#### QUESTION 220

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



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

**Correct Answer:** D

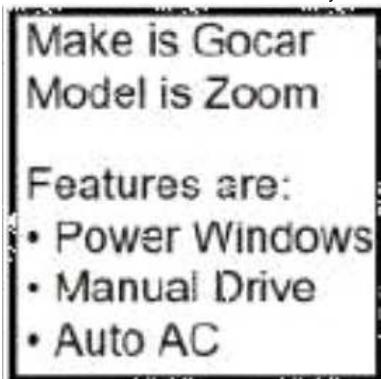
**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 221

Refer to the exhibit. What is the JSON syntax that is formed from the data?



- A. {"Make": "Gocar", "Model": "Zoom", "Features": ["Power Windows", "Manual Drive", "Auto AC"]}
- B. "Make": "Gocar", "Model": "Zoom", "Features": ["Power Windows", "Manual Drive", "Auto AC"]
- C. {"Make": Gocar, "Model": Zoom, "Features": Power Windows, Manual Drive, Auto AC}
- D. {"Make": ["Gocar", "Model": "Zoom"], "Features": ["Power Windows", "Manual Drive", "Auto AC"]}

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 222

How does a fabric access point fit in the network?

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

**Correct Answer:** C

**Section:** (none)

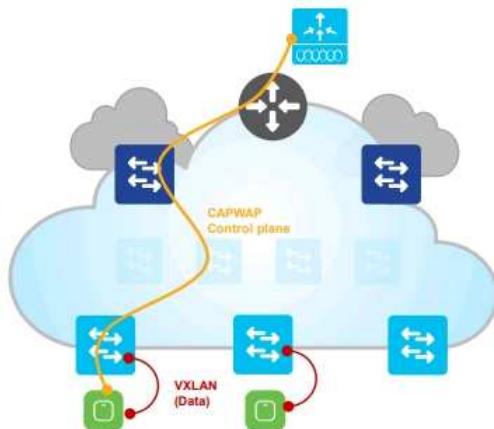
**Explanation**

**Explanation/Reference:**

## Fabric Mode AP integrates with the VXLAN Data Plane

Wireless Data Plane is distributed across APs

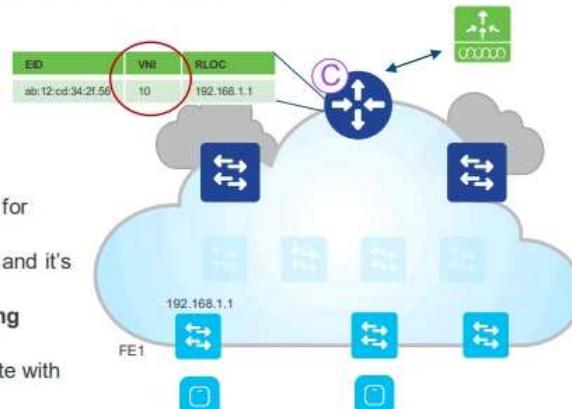
- Fabric mode AP is a local mode AP and needs to be directly connected to FE
- CAPWAP control plane goes to the WLC using Fabric
- **Fabric is enabled per SSID:**
  - For Fabric enabled SSID, AP converts 802.11 traffic to 802.3 and encapsulates it into VXLAN encoding VNI and SGT info of the client
  - Forwards client traffic based on forwarding table as programmed by the WLC. Usually VXLAN DST is first hop switch.
- AP applies all wireless specific feature like SSID policies, AVC, QoS, etc.



## Fabric Mode WLC integrates with the LISP Control Plane

Control Plane is centralized at the WLC for all Wireless functions

- WLC is still responsible for: AP image/config, Radio Resource Management (RRM) and client session management and roaming
- For Fabric integration:
  - For wireless, client **MAC address is used as EID**.
  - Interacts with the Host Tracking DB on Control-Plane node for **Client MAC address registration** with SGT and L2 VNI
  - The VN information is a **Layer 2 VN (L2 VNID)** information and it's mapped to a VLAN on the FEs
  - Responsible for updating the Host Tracking DB with **roaming** information for wireless clients
  - Fabric enabled WLC needs to be co-located at the same site with APs (latency between AP and WLC needs to be < 20 ms)



### QUESTION 223

Which encryption hashing algorithm does NTP use for authentication?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 224

Drag and drop the virtual component from the left onto their descriptions on the right.

**Select and Place:**

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

**Correct Answer:**

	VMX
	vNIC
	OVA
	VMDK

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 225**

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 226**

Refer to the exhibit.

```
No Hellos (Passive interface)
Supports Link-local Signaling (LLS)
! lines omitted for brevity
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 72.16.30.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 72.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown    Topology Name
    0          1        no        no           Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 172.16.11.29, Interface address 172.16.30.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  cobb-resync timeout 40
  No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 72.16.11.29/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 72.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown    Topology Name
    0          1        no        no           Base
Transmit Delay is 1 sec, State DROTHER, Priority 1
Designated Router (ID) 172.16.11.27, Interface address 172.16.11.27
> Backup Designated router (ID) 172.16.11.30, Interface address 172.16.11.30
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  cobb-resync timeout 40
  Hello due in 00:00:07
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
```

A network engineer configures OSPF and reviews the router configuration.

Which interface or interfaces are able to establish OSPF adjacency?

- A. GigabitEthernet0/1 and GigabitEthernet0/1.40
- B. Gigabit Ethernet0/0 and GigabitEthernet0/1
- C. only GigabitEthernet0/0
- D. only GigabitEthernet0/1

Correct Answer: C

Section: (none)

## Explanation

### Explanation/Reference:

Since g0/1 shows No Hellos (Passive Interface), therefore only g0/0 can form neighbor.

## QUESTION 227

Refer to the exhibit.



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

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

```
London(config-if)#end
NewYork#show dtp interface fa0/1
DTP information for FastEthernet0/1:
  TOS/TAS/TNS:      ACCESS/AUTO/ACCESS
  TOT/TAT/TNT:      NATIVE/ISL/NATIVE
```

Communication between London and New York is down.

Which command set must be applied to resolve this issue?

- A. 

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

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

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

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

Correct Answer: B

Section: (none)

Explanation

### Explanation/Reference:

TOS = Trunk Operational Status

TAS = Trunk Administrative Status

TNS = Trunk Negotiation Status

TOT = Trunk Operational (encapsulation) Type

TAT = Trunk Adminstrative (encapsulation) Type

TNT = Trunk Negotiation (encapsulation) Type

From the output:

NewYork f0/1 is configured as auto mode and the operational/negotiation result is Access Port.

NewYork f0/1 is configured to use ISL and the operational/negotiation result is shown as NATIVE (this is shown if the port is not trunk)

As London is configured with on mode which can form trunk with auto mode, you only need to change NewYork to use the same encapsulation as London i.e. dot1q.

## QUESTION 228

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

- A. An NSF-aware device immediately updates the standby route processor RIB without churning the network

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

SSO establishes one of the supervisor engines as active while the other supervisor engine is designated as standby, and then SSO synchronizes information between them. A switchover from the active to the redundant supervisor engine occurs when the active supervisor engine fails, or is removed from the switch, or is manually shut down for maintenance. This type of switchover ensures that Layer 2 traffic is not interrupted.

Cisco NSF always runs with SSO and provides redundancy for Layer 3 traffic. NSF works with SSO to minimize the amount of time that a network is unavailable to its users following a switchover. The main purpose of NSF is to continue forwarding IP packets following a supervisor engine switchover.

During switchover, CEF can be used the synchronized FIB to continue forwarding packets. At the same time, route information can be obtained from the peer NSF capable devices for rebuilding the Routing Information Base (RIB) tables. After route convergence is achieved, the RIB will be used for updating any stale entry in the CEF's FIB table.

**QUESTION 229**

In a Cisco Catalyst switch equipped with two supervisor modules an administrator must temporally remove the active supervisor from the chassis to perform hardware maintenance on it.

Which mechanism ensure that the active supervisor removal is not disruptive to the network operation?

- A. NSF/NSR
- B. SSO
- C. HSRP
- D. VRRP

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 230**

What is the wireless received signal strength indicator?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 231**

What is a characteristic of MACsec?

- A. 802.1AE provides encryption and authentication services
- B. 802.1AE is built between the host and switch using the MKA protocol, which negotiates encryption keys based on the master session key from a successful 802.1X session
- C. 802.1AE is built between the host and switch using the MKA protocol using keys generated via the Diffie-Hellman algorithm (anonymous encryption mode)
- D. 802.1AE is negotiated using Cisco AnyConnect NAM and the SAP protocol

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

The MACsec Key Agreement (MKA) is included as part of the IEEE 802.1XREV-2010 Port-Based Network Access Control Standard. The purpose of MKA is to provide a method for discovering MACsec peers and negotiating the security keys needed to secure the link. There are three ways defined within the 802.1 standard for the generation of keying material for use with MKA:

- Pre-shared Keys (PSK)
- The master session key which is a product of a successful Extensible Authentication Protocol (EAP) authentication
- Key distributed from an MKA key server

**QUESTION 232**

An engineer creates the configuration below.

```
R1#sh run | i aaa
aaa new-model
aaa authentication login default group ACE group AAA_RADIUS local-case
aaa session-id common
R1#
```

Drag and drop the authentication methods from the left into the order of priority on the right. Not all options are used.

Select and Place:

AAA servers of AAA_RADIUS group	Step 1
tacacs servers of group ACE	Step 2
AAA servers of ACE group	Step 3
local configured username in non-case-sensitive format	Step 4
local configured username in case-sensitive format	
If no method works, then deny login	

Correct Answer:

	AAA servers of ACE group
tacacs servers of group ACE	AAA servers of AAA_RADIUS group
	local configured username in case-sensitive format
local configured username in non-case-sensitive format	If no method works, then deny login

Section: (none)

Explanation

Explanation/Reference:

The above uses two custom server groups in which you can configure different combinations of RADIUS / TACACS+ server:  
Router(config)#aaa group server radius ?  
WORD Server-group name

local-case is the same as local except that the username is case-sensitive i.e. login user must type the exact case as the command e.g. "username Peter password pass".

QUESTION 233

The following system log message is presented after a network administrator configures a GRE tunnel:

%TUN-RECURDOWN: Interface Tunnel 0 temporarily disabled due to recursive routing.

Why is Tunnel 0 disabled?

- A. Because the tunnel cannot reach its tunnel destination
- B. Because the best path to the tunnel destination is through the tunnel itself
- C. Because dynamic routing is not enabled
- D. Because the router cannot recursively identify its egress forwarding interface

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

This may occur when routing protocol is running over the tunnel.

```
interface Tunnel0
ip address 192.168.1.1 255.255.255.0
tunnel source Loopback0
tunnel destination 10.3.3.3
```

Assume a static route is configured for forming the tunnel successfully (i.e. the router is reaching 10.3.3.3 using the following static default route).

```
ip route 0.0.0.0 0.0.0.0 172.16.25.2
```

However a new routing entry for the tunnel destination is then learnt through routing protocol to use the remote tunnel IP address as next hop address. (For example, the router now uses the tunnel to reach 10.3.3.3 i.e. the router is now using the tunnel itself to form tunnel).

```
D      10.3.3.0 [90/297372416] via 192.168.1.3, 00:00:00, Tunnel0
```

**QUESTION 234**

Which marking field is used only as an internal marking within a router?

- A. QOS Group
- B. Discard Eligibility
- C. IP Precedence
- D. MPLS Experimental

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

A policy map containing the set qos-group command can only be attached as an input traffic policy. QoS group values are not usable for traffic leaving a device. It can be used for classification traffic internally in output traffic policy of another interface in the same router.

**QUESTION 235**

Drag and drop the characteristics from the left onto the QoS components they describe on the right.

**Select and Place:**

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

**Correct Answer:**

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 236**

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.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 237**

Refer to the exhibit.

```

flow monitor FLOW-MONITOR-1
record netflow ipv6 original-input
exit
!
sampler SAMPLER-1
mode deterministic 1 out-of 2
exit
!
ip cef
ipv6 cef
!
interface GigabitEthernet0/0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
; ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input

```

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

A is incorrect since for a single flow within a time period, only one entry is sent to the collector regardless of the number of packets used for gathering data (e.g. 100 packets OR 50 packets due to 1 out of 2)

#### QUESTION 238

Which outcome is achieved with this Python code?

```

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

```

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since the command is "show ip bgp 192.168.101.0 bestpath", the output is the BGP table.

**Important:** In the above, only "print()" is used for displaying data in exact presentation of that output by "show" command i.e. no formatting is performed Python. Therefore, if this is a "choose two" questions, another correct answer is the show command output is displayed in unformatted way.

#### QUESTION 239

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

A Virtual Network Instance (VNI) is a virtual network instance for individual network segments.

The 24-bit Virtual Network Identifier (VNID) is used to identify a Virtual Network Instance (VNI) for layer 2 segment isolation and is included in a VXLAN header.

Note that some documentation uses VNI to represent Virtual Network Identifier.

#### QUESTION 240

What is the recommended MTU size for a Cisco SD-Access Fabric?

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

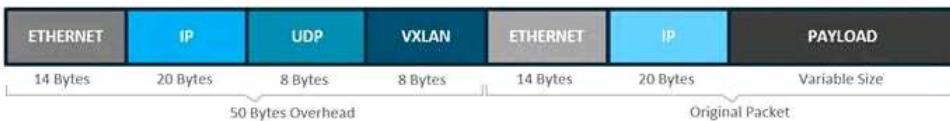
**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

VXLAN encapsulation uses a UDP transport. Along with the VXLAN and UDP headers used to encapsulate the original packet, an outer IP and Ethernet header are necessary to forward the packet across the wire. At minimum, these extra headers add 50 bytes of overhead to the original packet.



Actually, the common denominator and recommended MTU value available on devices operating in a fabric role is 9100.

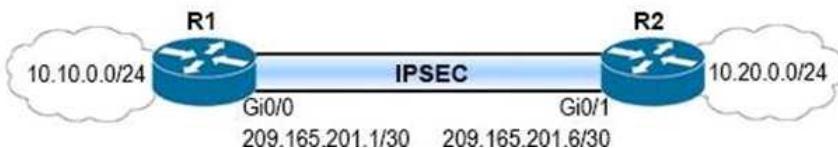
Network should have a minimum starting MTU of at least 1550 bytes to support the fabric overlay. MTU values between 1550 and 9100 are supported along with MTU values larger than 9100 though there may be additional configuration and limitations based on the original packet size.

MTU 9100 is provisioned as part of LAN Automation.

**QUESTION 241**

Refer to the exhibit.

access-list 100 permit gre host 209.165.201.1 host 209.165.201.6	access-list 100 permit gre host 209.165.201.6 host 209.165.201.1
crypto isakmp policy 5	crypto isakmp policy 5
authentication pre-share	authentication pre-share
hash sha256	hash sha256
encryption aes	encryption aes
group 14	group 14
crypto isakmp key D@t@c3nt3r address 209.165.201.6	crypto isakmp key D@t@c3nt3r address 209.165.201.1
crypto ipsec transform-set My_Set esp-aes esp-sha-hmac mode transport	crypto ipsec transform-set My_Set esp-aes esp-sha-hmac mode transport
crypto map MAP 10 ipsec-isakmp set peer 209.165.201.6 set transform-set My_Set match address 100	crypto map MAP 10 ipsec-isakmp set peer 209.165.201.1 set transform-set My_Set match address 100
interface GigabitEthernet0/0 description outside_interface no switchport ip address 209.165.201.1 255.255.255.252 crypto map MAP	interface GigabitEthernet0/1 description outside_interface no switchport ip address 209.165.201.6 255.255.255.252 crypto map MAP
interface Tunnel 100 ip address 192.168.100.1 255.255.255.0 ip mtu 1400 tunnel source GigabitEthernet0/0 tunnel destination 209.165.201.6 ip route 10.20.0.0 255.255.255.0 192.168.100.2 Tunnel100	interface Tunnel 100 ip address 192.168.100.2 255.255.255.0 ip mtu 1400 tunnel source GigabitEthernet0/1 tunnel destination 209.165.201.1 ip route 10.10.0.0 255.255.255.0 192.168.100.1 Tunnel100



A network engineer must simplify the IPsec configuration by enabling IPsec over GRE using IPsec profiles.

Which two configuration changes accomplish this? (Choose two)

- A. Apply the crypto map to the tunnel interface and change the tunnel mode to tunnel mode ipsec ipv4
- B. Remove all configuration related to crypto map from R1 and R2 and eliminate the ACL 100
- C. Remove the crypto map and modify the ACL to allow traffic between 10.10.0.0/24 to 10.20.0.0/24
- D. Create an IPsec profile, associate the transform-set, and apply the profile to the tunnel interface

**Correct Answer: BD**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

A is wrong since it disables the use of GRE and therefore is not IPsec over GRE.

When using IPsec over GRE using tunnel interface, the existing static route (last line in the exhibit) with next hop interface is enough for identifying traffic that requires protection.

**QUESTION 242**

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

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

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 243**

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

**Correct Answer:** BE

**Section:** Selected

**Explanation**

**Explanation/Reference:**

After the LAP gets an IP address from the DHCP server, the LAP broadcasts a Layer 3 CAPWAP discovery message on to its local subnet. Normally these broadcasts are limited to local subnet as it will not cross layer 3 boundaries. If you want to forward these to a particular WLC you have to configure WLC IP address in "ip helper-address" on layer 3 interface where LAP is associated with. Then L3 device forwards these broadcasts to the IP addresses configured with the ip-helper command on the interface on which the broadcast is heard.

You can configure the IP Helper feature in a router to direct the broadcast packet with UDP port 5246 received by e.g. f1/0/3 from the AP to the WLC e.g. 192.168.200.1. (similar to the actions performed as a DHCP relay agent).

```
ip forward-protocol udp 5246
interface FastEthernet1/0/3
 ip helper-address 192.168.200.1
```

**QUESTION 244**

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

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

**Correct Answer:** D

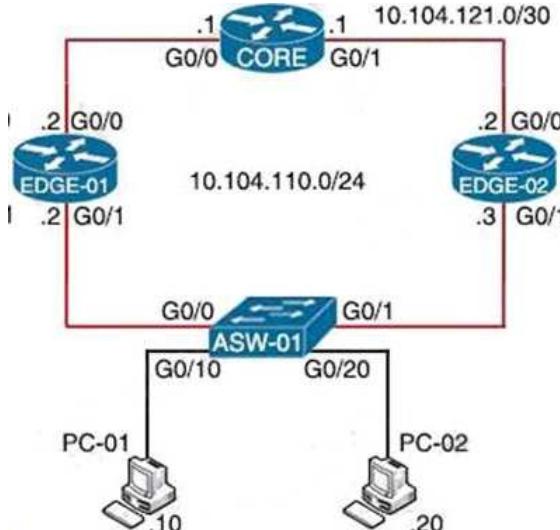
**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 245**

Refer to the exhibit.



Edge-01

```
track 10 interface GigabitEthernet0/0 line-protocol
```

```
!
interface GigabitEthernet0/1
  ip address 10.104.110.2 255.255.255.0
  vrrp 10 ip 10.104.110.100
  vrrp 10 priority 120
```

#### Edge-02

```
interface GigabitEthernet0/1
  ip address 10.104.110.3 255.255.255.0
  vrrp 10 ip 10.104.110.100
```

Object tracking has been configured for VRRP enabled routers Edge-01 and Edge-02.

Which commands cause Edge-02 to preempt Edge-01 in the event that interface G0/0 goes down on Edge-01?

- A. Edge-01(config)#interface G0/1  
Edge-01(config-if)#vrrp 10 track 10 decrement 10
- B. Edge-02(config)#interface G0/1  
Edge-02(config-if)#vrrp 10 track 10 decrement 30
- C. Edge-02(config)#interface G0/1  
Edge-02(config-if)#vrrp 10 track 10 decrement 10
- D. Edge-01(config)#interface G0/1  
Edge-01(config-if)#vrrp 10 track 10 decrement 30

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 246

Which data is properly formatted with JSON?

- A. {  
 "name": "Peter"  
 "age": "25"  
 "likesJson": true  
 "characteristics": ["small", "strong", 18],  
}  
B. {  
 "name": Peter,  
 "age": 25,  
 "likesJson": true,  
 "characteristics": ["small", "strong", "18"],  
}  
C. {  
 "name": "Peter",  
 "age": "25",  
 "likesJson": true,  
 "characteristics": ["small", "strong", 18],  
}  
D. {  
 "name": "Peter".  
 "age": "25",  
 "likesJson": true,  
 "characteristics": ["small", "strong", 18]  
}

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

An array can contain value of different types e.g. string and integer.

D is correct since there are "," between the fields and there is no "," in the last field.

#### QUESTION 247

How does Protocol Independent Multicast function?

- A. It uses unicast routing information to perform the multicast forwarding function.
- B. It uses the multicast routing table to perform the multicast forwarding function.
- C. In sparse mode it establishes neighbor adjacencies and sends hello messages at 5 second intervals.
- D. It uses broadcast routing information to perform the multicast forwarding function.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

PIM's Hello messages are sent periodically at the interval of 30 seconds.

**QUESTION 248**

A customer has recently implemented a new wireless infrastructure using WLC -5520S at a site directly next to a large commercial airport. Users report that they intermittently lose Wi-Fi connectivity, and troubleshooting reveals it is due to frequent channel changes.

Which two actions fix this issue? (Choose two)

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

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The Unlicensed National Information Infrastructure (U-NII) radio band, as defined by the United States Federal Communications Commission, is part of the radio frequency spectrum used by WLAN devices and by many wireless ISPs e.g.

- UNII-1/Lower Band (5.150 to 5.250 GHz) Non-overlapping channels 36, 40, 44, 48
- UNII-2/Middle Band (5.250 to 5.350 GHz) Non-overlapping channels 52, 56, 60, 64
- UNII-2 Extended (5.470 to 5.725 GHz) Non-overlapping channels 100, 104, 108, 112, 120, 124, 128, 136, 140
- UNII-3/Upper Band (5.725 to 5.825 GHz) on-overlapping channels 149, 153, 157, 161, 165

Depending on the country, some of them may be used by radar system (e.g. airport). Although these channels are still allowed for use in WLAN, in order to prevent interference, the country may have regulation to require a wireless device perform scanning before using those channels. This process is known as Dynamic Frequency Selection (DFS).

In US (and most other countries), UNII-2 and Extended UNII-2 are used by radar system and requires DFS. Hence, a simple way is to remove the use of those channels. In US, the removal of DFS channel is the same as removing UNII-2 and UNII-2 Extended channels.

Note that in Bahrain, DFS channels include UNII-2, Extended UNII-2 and UNII-3.

**QUESTION 249**

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

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

**Correct Answer:** AD

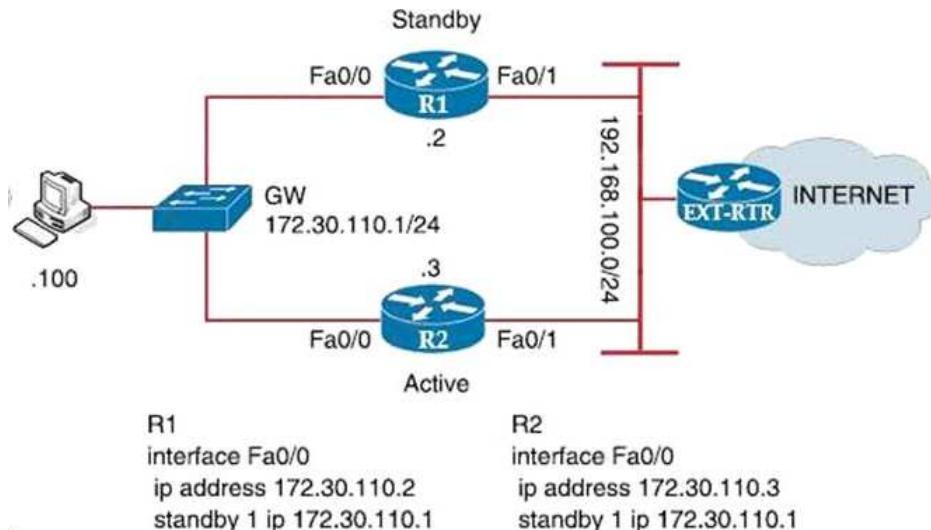
**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 250**

Refer to the exhibit.



Which configuration change ensures that R1 is the active gateway whenever it is in a functional state for the 172.30.110.0/24 network?

- A. R1  
standby 1 preempt  
R2  
standby 1 priority 90
- B. R1  
standby 1 preempt  
R2  
standby 1 priority 100
- C. R2  
standby 1 priority 100  
standby 1 preempt
- D. R2  
standby 1 priority 110  
standby 1 preempt

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 251**

What are two features of NetFlow flow monitoring? (Choose two)

- A. Can track ingress and egress information
- B. Include the flow record and the flow importer
- C. Copies all ingress flow information to an interface
- D. Does not support packet sampling on interfaces
- E. Can be used to track multicast, MPLS, or bridged traffic

**Correct Answer:** AE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 252**

Drag and drop the characteristics from the left onto the QoS components they describe on the right.

**Select and Place:**

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

**Correct Answer:**

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Duplicate question. Same as 235.

**QUESTION 253**

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

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

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The above settings are useful to trigger the client to roam to another AP.

**QUESTION 254**

Refer to the exhibit.

DSW2#sh spanning-tree vlan 20

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

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

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

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 255**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 256**

Drag and drop the descriptions of the VSS technology from the left to the right. Not all options are used.

Which of the followings are the characteristics of VSS (Choose three)?

- A. supported on the Cisco 4500  
and 6500 series

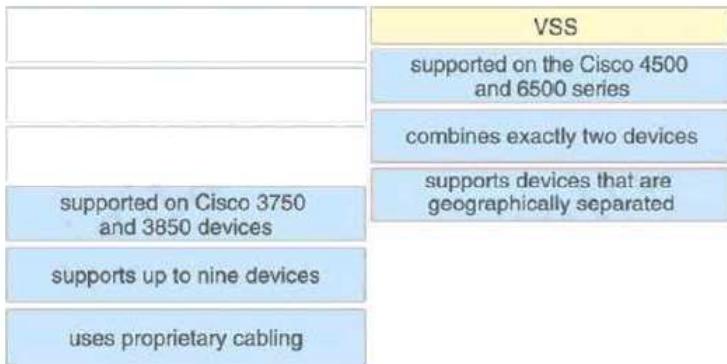
- B. combines exactly two devices
- C. supports devices that are geographically separated
- D. supported on Cisco 3750 and 3850 devices
- E. supports up to nine devices
- F. uses proprietary cabling

Correct Answer: ABC

Section: (none)

Explanation

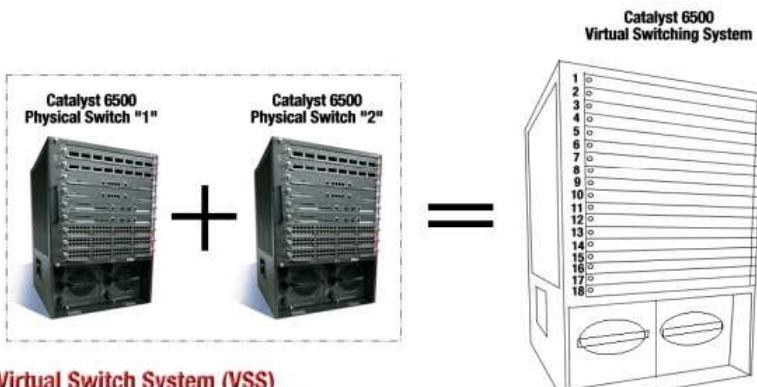
Explanation/Reference:



VSS combines a pair of switches (exactly two switches) into a single network element. It is supported in switch models such as 4500 and 6500.

## Virtual Switching System

Virtual Switch System is a new technology break through for the Catalyst 6500 family...



### Virtual Switch System (VSS)

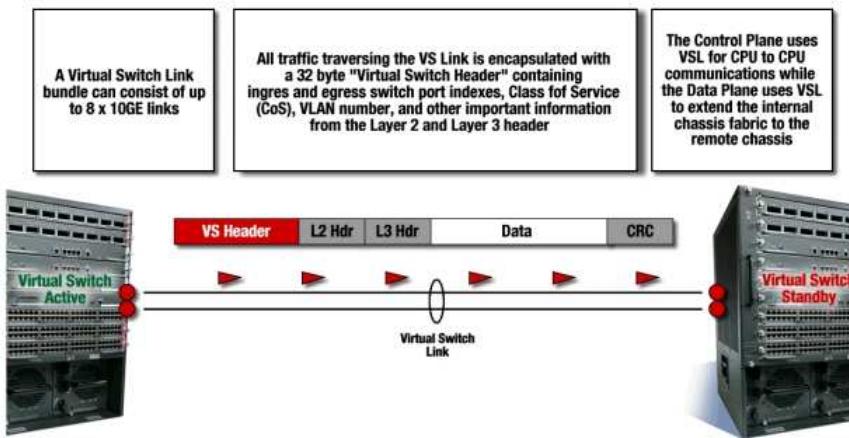
defines two physical Catalyst 6500 switches joined via a special link called a Virtual Switch Link (VSL) running special hardware and software that allows them to operate as a single logical switch

For the two chassis of the VSS to act as one network element, they need to share control information and data traffic. The virtual switch link (VSL) is a special link consisting of two or more 10G links that carries control and data traffic between the two chassis of a VSS.

# Virtual Switch Architecture

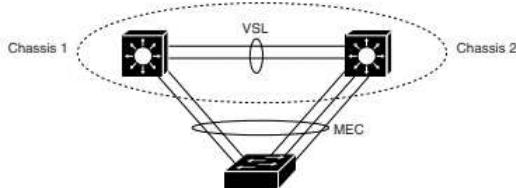
## Virtual Switch Link

The Virtual Switch Link is a special link joining each physical switch together - it extends the out of band channel allowing the active control plane to manage the hardware in the second chassis...



In VSS mode, supervisor engine redundancy operates between the active and standby chassis, using stateful switchover (SSO) and nonstop forwarding (NSF). The peer chassis exchange configuration and state information across the VSL and the standby supervisor engine runs in hot standby mode. The standby chassis monitors the active chassis using the VSL. If it detects failure, the standby chassis initiates a switchover and takes on the active role. When the failed chassis recovers, it takes on the standby role.

VSS mode can manage the redundant links in different chassis for forming a single port channel with another switch and this is known as Multichassis EtherChannel MEC.



Remarks : Unlike switch stacking which requires special stack cable which is usually short, VSS uses standard 10 G Ethernet interfaces and therefore the two chassis may be separated e.g. in different rooms.

### QUESTION 257

Based on the output below, which Python code shows the value of the "upTime" key?

```
{  
    "response": [ {  
        "family": "Routers",  
        "type": "Cisco ASR 1001-X Router",  
        "errorCode": null,  
        "location": null,  
        "macAddress": "00:c8:8b:80:bb:00",  
        "hostname": "asr1001-x.abc.inc",  
        "role": "BORDER ROUTER",  
        "lastUpdateTime": 1577391299537,  
        "serialNumber": "FXS1932Q1SE",  
        "softwareVersion": "16.3.2",  
        "locationName": null,  
        "upTime": "49 days, 13:43:44:13",  
        "lastUpdated": "2019-12-22 16:35:21"  
    }]  
}
```

- A. 

```
json_data = response.json()  
print(json_data[response][0][upTime])
```
- B. 

```
json_data = response_json()  
print(json_data['response'][family][upTime])
```
- C. 

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

D. 

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

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 258**

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

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

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 259**

Refer to the exhibit.

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

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

Which JSON syntax is derived from this data?

- A. 

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

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

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

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

**Correct Answer:** A  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

Since all choices are using single quotes, we assume that they are actually in double quotes.

**QUESTION 260**

Refer to the exhibit.

```

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 (SD)      PAgP    Gi0/0(I) Gi0/1(I)

```

```

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

Group Port-channel Protocol Ports
-----+-----+-----+
1     Po1 (SD)      LACP    Gi0/0(I) Gi0/1(I)

```

Which action resolves the EtherChannel issue between SW2 and SW3?

- A. Configure switchport mode trunk on SW2
- B. Configure switchport nonegotiate on SW3
- C. Configure channel-group 1 mode desirable on both interfaces
- D. Configure channel-group 5 mode active on both interfaces

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 261

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

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

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

#### QUESTION 262

Drag and drop the solutions that comprise Cisco Cyber Threat Defense from the left onto the objectives they accomplish on the right.

**Select and Place:**

StealthWatch	detects suspicious web activity
Web Security Appliance	analyzes network behavior and detects anomalies
Identity Services Engine	uses pxGrid to remediate security threats

**Correct Answer:**

	Web Security Appliance
	StealthWatch
	Identity Services Engine

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Cisco Platform Exchange Grid (pxGrid) enables multivendor, cross-platform network system collaboration among parts of the IT infrastructure such as security monitoring and detection systems, network policy platforms, asset and configuration management, identity and access management platforms, and virtually any other IT operations platform.



#### QUESTION 263

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

A STUN (Session Traversal of User Datagram Protocol [UDP] Through Network Address Translators [NATs]) server allows NAT clients (i.e. IP Phones behind a firewall) to set up phone calls to a VoIP provider hosted outside of the local network.

Similarly, in SD-WAN, vBond acts as a STUN server for all other SD-WAN devices for NAT Traversal..

#### QUESTION 264

A company has an existing Cisco 5520 HA cluster using SSO. An engineer deploys a new single Cisco Catalyst 9800 WLC to test new features. The engineer successfully configures a mobility tunnel between the 5520 cluster and 9800 WLC. Clients connected to the corporate WLAN roam seamlessly between access points on the 5520 and 9800 WLC. After a failure on the primary 5520 WLC, all WLAN services remain functional; however clients cannot roam between the 5520 and 9800 controllers without dropping their connection.

Which feature must be configured to remedy the issue?

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

**Correct Answer: A**

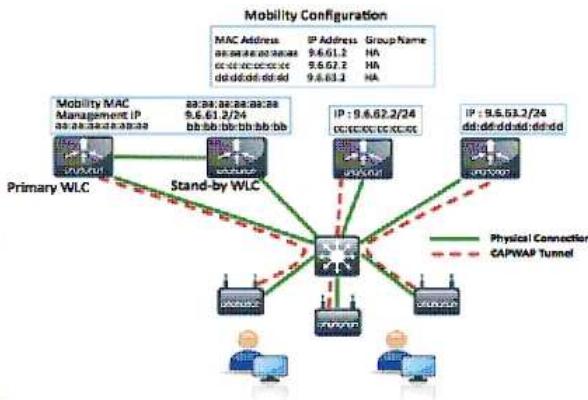
**Section: (none)**

**Explanation**

**Explanation/Reference:**

A Mobility MAC address (e.g. aaaa.aaaa.aaaa) has to be configured in the 5520 cluster. The mobility setup in all other mobility peers (i.e. other WLC of any model)

should configured this MAC address for including the cluster in the mobility group.



For mobility group setup, the MAC address of all concerned WLCs has to be configured in the group.

For HA cluster using SSO, each WLC has its own unique MAC address, which is used in mobility configuration. In the event of failure of the primary WLC acting as active, problem in roaming will occur since other controllers are not setup with the standby WLC's MAC address.

Control path and data path will be down. The administrator has to manually change the MAC to Standby MAC address on all other WLC in mobility setup

In order to keep the mobility network stable without any manual intervention and in the event of failure or switchover, Mobility MAC has been introduced. Just like VIP in FHRP, the Mobility MAC address configured can be configured in the primary WLC and this address will be sync to the standby WLC. If failover occurs and the standby WLC takes over, it continues to use the Mobility MAC address so that roaming can continued to be performed with other WLCs.

#### QUESTION 265

What is a characteristic of para-virtualization?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

#### Explanation/Reference:

Paravirtualization (PV) is an enhancement of virtualization technology in which a guest operating system (guest OS) is modified prior to installation inside a virtual machine (VM) in order to allow all guest OS within the system to share resources and successfully collaborate, rather than attempt to emulate an entire hardware environment.

The following shows a simplified illustration

#### Without Paravirtualization:

Guest OS in VM -> Guest normal Network Card Driver -> Software for emulating the virtual network card -> Hypervisor -> Physical Network Dirver / Card.

#### Paravirtualization:

Guest OS in VM -> Speical PV driver that talks to hypervisor directly -> Hypervisor -> Physical Network Dirver / Card.

#### QUESTION 266

What is YANG used for?

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

**Correct Answer:** D

**Section:** Selected

**Explanation**

#### Explanation/Reference:

#### QUESTION 267

What is the calculation that is used to measure the radiated power of a signal after it has gone through the radio, antenna cable, and antenna?

- A. dBi
- B. mW
- C. dBm
- D. EIRP

**Correct Answer:** D

**Section:** Selected

**Explanation**

#### Explanation/Reference:

Effective, or Equivalent, Isotropically Radiated Power (EIRP) is the maximum amount of power that could be radiated from an antenna, given its antenna gain and the transmitter power of the RF system. EIRP is most commonly given in decibels over isotropic, dBi.

For measuring in client device (i.e. after passing through space and obstacles), RSSI with dBm as unit is used.

#### QUESTION 268

Refer to the exhibit.

TYPE	PROT	SYSTEM IP	ID	ID	PRIVATE IP	PORI	
PUBLIC IP				PORT	LOCAL COLOR	PROXY STATE UPTIME	ID
<hr/>							
vsmart	dtls	0.0.0.0	100	1	192.168.100.80		
12346	10.10.20.70			12446	default	No	up
0:02:24:09	0						
vbond	dtls	0.0.0.0	0	0	192.168.100.81		
12346	10.10.20.80			12346	default	-	up
0:02:24:10	0						
vmanage	dtls	4.4.4.90	100	0	192.168.100.82		
12446	10.10.20.90			12446	default		

The screenshot shows the Postman interface with a POST request to `https://192.168.100.80:12442/i_security_check`. The 'Body' tab is selected, showing form-data fields `i_username` and `i_password`, both set to `admin`.

## Could not get any response

There was an error connecting to `https://192.168.100.80:12442/i_security_check`

### Why this might have happened:

- The server couldn't send a response: Ensure that the backend is working properly
- Self-signed SSL certificates are being blocked: Fix this by turning off 'SSL certificate verification' in *Settings > General*
- Proxy configured incorrectly: Ensure that proxy is configured correctly in *Settings > Proxy*
- Request timeout: Change request timeout in *Settings > General*

What step resolves the authentication issue?

- restart the vsmart host
- target 192.168.100.82 in the URI
- change the port to 12446
- use basic authentication

**Correct Answer: B**

**Section: (none)**

**Explanation**

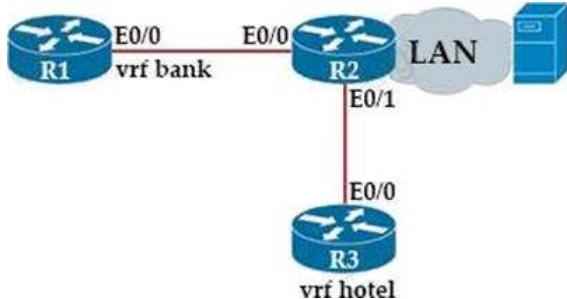
#### Explanation/Reference:

The first diagram shows the control connection ports by the command "show sdwan control connections". Although the port numbers shown are not used for web interface / API, the output can show the IP address of the component nodes.

When you want to authenticate with the SDWAN solution using API, you need to send a POST request to `https://{{vmanage}}:{{port}}/i_security_check`. Hence you should connect to vManage i.e. 192.168.100.82 instead.

#### QUESTION 269

Refer to the exhibit.



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

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

```
interface Ethernet0/0
vrf forwarding bank
ip address 172.16.0.4 255.255.0.0
```

```
interface Ethernet0/1
vrf forwarding hotel
ip address 172.1.0.5 255.255.0.0
```

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

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

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

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

- A. 

```
interface Ethernet0/0
ip address 172.16.0.7 255.255.0.0
!
router ospf 44 vrf hotel
network 172.16.0.0 0.0.255.255
```
- B. 

```
interface Ethernet0/0
vrf forwarding bank
ip address 172.16.0.7 255.255.0.0
!
router ospf 44 vrf bank
network 172.16.0.0 0.0.255.255 area 0
```
- C. 

```
interface Ethernet0/0
vrf forwarding hotel
ip address 172.16.0.7 255.255.0.0
!
router ospf 44 vrf hotel
network 172.16.0.0 0.0.255.255 area 0
```
- D. 

```
interface Ethernet0/0
ip address 172.16.0.7 255.255.0.0
!
router ospf 44 vrf bank
network 172.16.0.0 255.255.0.0
```

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Normally R1 can just configure OSPF. However, all answers include VRF in the OSPF configuration.

Since a VRF "bank" is already configured in R1, you need to find an answer that uses "bank" (i.e. B or D). Then you need to find a configuration settings that also assign the concerned interface in the VRF "bank". Hence the answer is B.

**QUESTION 270**

What does the number in an NTP stratum level represent?

- A. The number of hops it takes to reach the master time server.
- B. The amount of drift between the device clock and true time.
- C. The amount of offset between the device clock and true time.
- D. The number of hops it takes to reach the authoritative time source.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 271**

What is a characteristic of a next-generation firewall?

- A. required in each layer of the network
- B. filters traffic using Layer 3 and Layer 4 information only
- C. only required at the network perimeter
- D. provides intrusion prevention

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 272**

Which unit measures the power of a radio signal with reference to 1 milliwatt?

- A. dBw
- B. dBi
- C. mW
- D. dBm

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 273**

When does a stack master lose its role?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

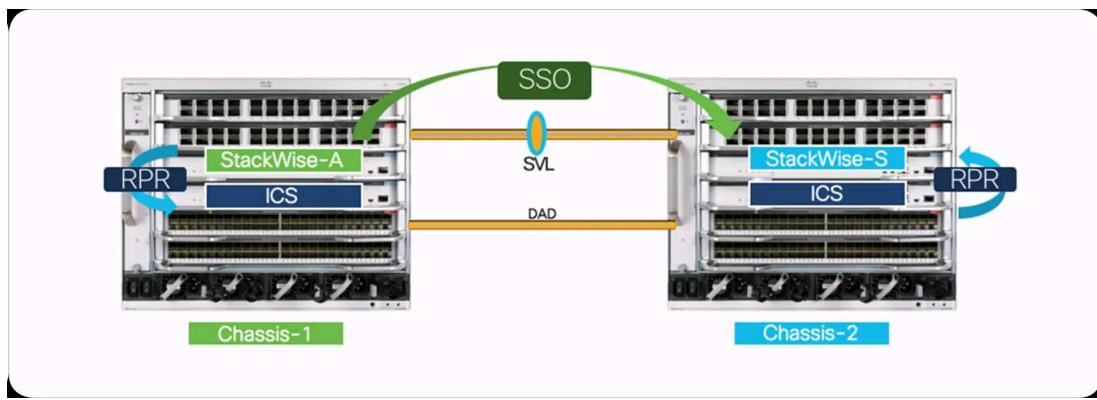
The Switch Stacking is a feature that allows us to configure multiple Cisco switches in a way that they appear as a single switch and act cooperatively.



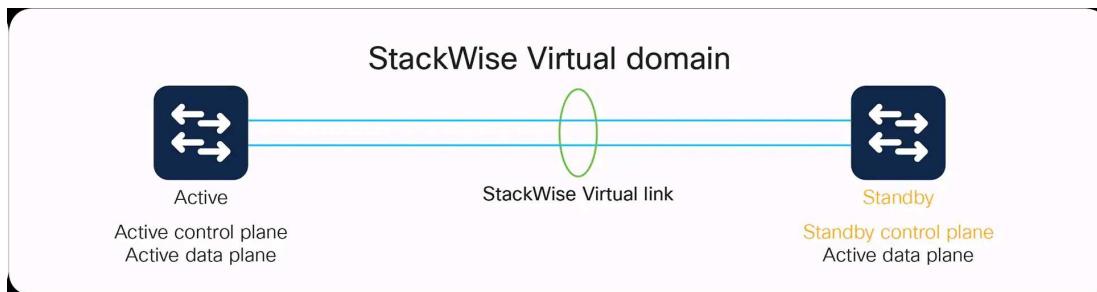
It requires special stacking cable to connect the switch together. Unlike clustering, ports of all other switches are configured as if they are the ports of the stack master switch.

**Important:**

There is also another technique known as "Cisco Stackwise Virtual". It is an advanced technique for high end model e.g. Catalyst 9000. It combines two switches into a single logical network entity from the network control plane and management perspectives. It uses Cisco Stateful Switchover (SSO) technology, as well as Non-Stop Forwarding (NSF) extensions to routing protocols, to provide seamless traffic failover when one of the device fails over.



Remarks : DAD means Dual Active Detection links



The Link Management Protocol (LMP) is activated on each link of the StackWise Virtual link as soon as it is brought up online. The LMP is used for exchanging hello for health monitoring and can rejects any unidirectional links.

#### QUESTION 274

What is the differences between TCAM and the MAC address table? (Choose Two)

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

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 275

Refer to the exhibit.

DSW2#sh spanning-tree vlan 10

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

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

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

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 276**

Refer to the exhibit.

```
Current configuration: 142 bytes
vrf definition STAFF
!
!
interface GigabitEthernet1
    vrf forwarding STAFF
    no ip address
    negotiation auto
    no mop enabled
    no mop sysid
.end
```

An engineer must assign an IP address of 192.168.1.1/24 to the GigabitEthernet1 interface.

Which two commands must be added to the existing configuration to accomplish this task? (Choose two)

- A. Router(config-vrf)#address-family ipv6
- B. Router(config-if)#ip address 192.168.1.1 255.255.255.0
- C. Router(config-vrf)#ip address 192.168.1.1 255.255.255.0
- D. Router(config-if)#address-family ipv4
- E. Router(config-vrf)#address-family ipv4

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 277**

Which two southbound interfaces originate from Cisco DNA Center and terminate at fabric underlay switches? (Choose two)

- A. UDP 67: DHCP
- B. ICMP: Discovery
- C. TCP 23: Telnet
- D. UDP 162: SNMP
- E. UDP 6007: NetFlow

**Correct Answer:** BC

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Answer D is incorrect since it is 162 (port for SNMP Trap) instead of 161.

**Table 6. Cisco DNA Center Traffic**

Source Port <sup>2</sup>	Source	Destination Port	Destination	Description
Any	Cisco DNA Center	UDP 53	DNS Server	From Cisco DNA Center to DNS server
Any	Cisco DNA Center	TCP 22	Fabric underlay	From Cisco DNA Center to fabric switches' loopbacks for SSH
Any	Cisco DNA Center	TCP 23	Fabric underlay	From Cisco DNA Center to fabric switches' loopbacks for TELNET
Any	Cisco DNA Center	UDP 161	Fabric underlay	From Cisco DNA Center to fabric switches' loopbacks for SNMP device discovery
ICMP	Cisco DNA Center	ICMP	Fabric underlay	From Cisco DNA Center to fabric switches' loopbacks for SNMP device discovery
Any	Cisco DNA Center	TCP 443	Fabric underlay	From Cisco DNA Center to fabric switches for software upgrades (also to the Internet if there is no proxy)
Any	Cisco DNA Center	TCP 80	Fabric underlay	From Cisco DNA Center to fabric switches for PnP (also to the Internet if there is no proxy)
Any	Cisco DNA Center	TCP 830	Fabric underlay	From Cisco DNA Center to fabric switches for Netconf (SDA embedded wireless)
UDP 123	Cisco DNA Center	UDP 123	Fabric underlay	From Cisco DNA Center to fabric switches for initial time during LAN automation
Any	Cisco DNA Center	UDP 123	NTP Server	From Cisco DNA Center to NTP server
Any	Cisco DNA Center	TCP 22, UDP 161	WLC	From Cisco DNA Center to WLC
ICMP	Cisco DNA Center	ICMP	WLC	From Cisco DNA Center to WLC

**Important:** The above only shows the standard southbound traffic.

Cisco DNA Center allows customers to manage their non-Cisco devices through the use of a Software Development Kit (SDK) that can be used to create Device Packages for third-party devices. The SDK may generate other traffic not mentioned above in order to communicate with the non-Cisco devices.

**QUESTION 278**

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

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 279**

Which QoS mechanism will prevent a decrease in TCP performance?

- A. Shaper
- B. Policer
- C. WRED
- D. Rate-Limit
- E. LLQ
- F. Fair-Queue

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 280**

Which two results occur if Cisco DNA Center loses connectivity to devices in the SD-Access fabric? (Choose two)

- A. All devices reload after detecting loss of connection to Cisco DNA Center
- B. Already connected users are unaffected, but new users cannot connect
- C. Users lose connectivity
- D. Cisco DNA Center is unable to collect monitoring data in Assurance

E. User connectivity is unaffected

**Correct Answer: DE**

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 281**

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

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

**Correct Answer: D**

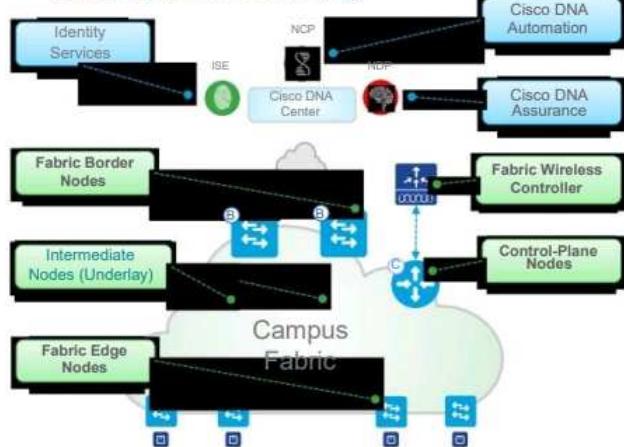
Section: (none)

Explanation

Explanation/Reference:

## Cisco SD-Access

### Fabric Roles & Terminology



- **Cisco DNA Automation** - provides simple GUI management and intent based automation (e.g. NCP) and context sharing
- **Cisco DNA Assurance** - Data Collectors (e.g. NDP) analyze Endpoint to App flows and monitor fabric status
- **Identity Services** - NAC & ID Systems (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition
- **Control-Plane Nodes** - Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** - A Fabric device (e.g. Core) that connects External L3 network(s) to the SDA Fabric
- **Fabric Edge Nodes** - A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric
- **Fabric Wireless Controller** - A Fabric device (WLC) that connects APs and Wireless Endpoints to the SDA Fabric

**QUESTION 282**

Which control plane protocol is used between Cisco SD-WAN routers and vSmart controllers?

- A. BGP
- B. OMP
- C. TCP
- D. UDP

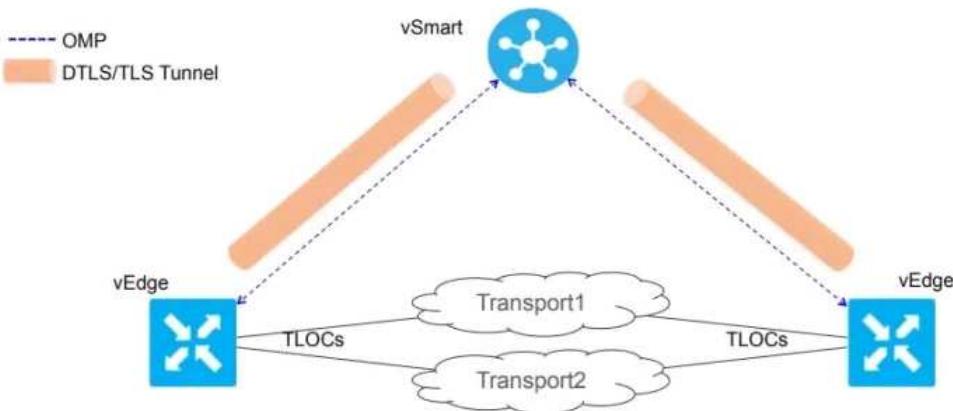
**Correct Answer: B**

Section: (none)

Explanation

Explanation/Reference:

## Fabric Operation Walk-Through



**QUESTION 283**

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

- A. virtual channel used to carry control plane information

- B. attribute to identify a set of services offered in specific places in the SD -WAN fabric
- C. common exchange point between two different services
- D. virtualized environment that provides traffic isolation and segmentation in the SD -WAN fabric

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 284**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 285**

Refer to the exhibit.

**Vlan503 - Group 1**

**State is Active**

1 state change, last state change 32w6d

Virtual IP address is 10.0.3.241

Active virtual MAC address is 0000.0c07.ac01

Local virtual MAC address is 0000.0c07.ac01 (v1 default)

Hello time 3 sec, hold time 10 sec

Next hello sent in 0.064 secs

Preemption enabled

Active router is local

Standby router is 10.0.3.242, priority 100 (expires in 10.624 sec)

Priority 110 (configured 110)

Group name is "hsrp-VI503-1" (default)

Which two facts does the device output confirm? (Choose two)

- A. The device is using the default HSRP hello timer
- B. The standby device is configured with the default HSRP priority
- C. The device's HSRP group uses the virtual IP address 10.0.3.242.
- D. The device is configured with the default HSRP priority
- E. The device sends unicast messages to its peers

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 286**

Drag and drop the characteristic from the left onto the orchestration tools that they describe on the right.

Which of the following are the characteristics of Ansible (Choose two)?

- A. uses playbooks
- B. uses a pull model
- C. procedural
- D. declarative

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



Chef and Ansible encourage a procedural style where you write code that specifies, step-by-step, how to achieve some desired end state.

SaltStack and Puppet encourage a more declarative style where you write code that specifies your desired end state, and the IAC tool itself is responsible for figuring out how to achieve that state.

#### **QUESTION 287**

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 happens to access interfaces where VLAN 222 is assigned?

- A. They are placed into an inactive state
- B. A description "RSPAN" is added
- C. STP BPDU guard is enabled
- D. They cannot provide PoE

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 288**

Which tunneling technique is used when designing a Cisco SD -Access fabric data plane?

- A. VXLAN
- B. VRF Lite
- C. VRF
- D. LISP

**Correct Answer:** A

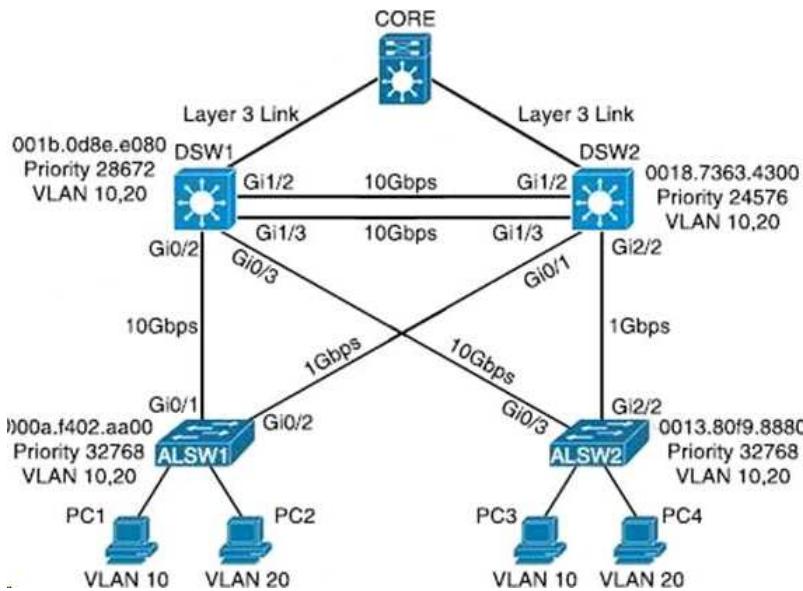
**Section:** Selected

**Explanation**

**Explanation/Reference:**

#### **QUESTION 289**

Refer to the exhibit.



How to make DSW1 g1/3 the root port for VLAN 10? (Choose two)

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

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Note that since no VLAN is specified in the command in B, the port priority is set for both VLAN 10 and 20. Hence DSW1 g1/3 will become root port for both VLANs.

#### QUESTION 290

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

- A. provide QoS prioritization services such as marking, queueing, and classification for critical network traffic
- B. provide advanced network security features such as 802.1X, DHCP snooping, VACLs, and port security
- C. provide redundant Layer 3 point-to-point links between the core devices for more predictable and faster convergence
- D. provide redundant aggregation for access layer devices and first-hop redundancy protocols such as VRRP

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

#### QUESTION 291

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

- A. host
- B. virtual machine
- C. container
- D. mainframe

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Container is a special form of virtualization. For each container in a host, it is sharing the OS kernel from the host machine. Hence if a host running Linux and install containers in it, all containers can only run Linux.

A is NOT correct since it is not an emulated machine.

For VM, although compute resource i.e. CPU in the host are by default shared and assigned dynamically among VMs. Most type-1 hypervisor can allow you to dedicate assign one or more of the CPU cores in the host for a single VM only.

#### QUESTION 292

How are the Cisco Express Forwarding table and the FIB related to each other?

- A. The FIB is used to populate the Cisco Express Forwarding table
- B. The Cisco Express Forwarding table allows route lookups to be forwarded to the route processor for processing before they are sent to the FIB
- C. There can be only one FIB but multiple Cisco Express Forwarding tables on IOS devices
- D. Cisco Express Forwarding uses a FIB to make IP destination prefix-based switching decisions

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 293**

In a Cisco SD-Access wireless architecture, which device manages endpoint ID to Edge Node bindings?

- A. fabric control plane node
- B. fabric wireless controller
- C. fabric border node
- D. fabric edge node

**Correct Answer:** A

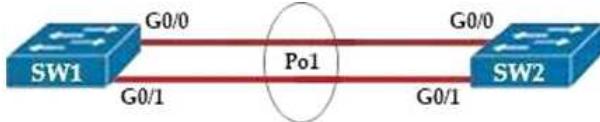
**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 294**

Refer to the exhibit.



SW1# show etherchannel summary

```
! output omitted

> Group      Port-channel      Protocol      Ports
-----+-----+-----+-----+
1       Po1 (SD)           -
```

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

SW2#

```
09:45:32: %PM-4-ERR_DISABLE: channel-misconfig error detected on Gi0/0, putting Gi0/0 in err-disable state
09:45:32: %PM-4-ERR_DISABLE: channel-misconfig error detected on Gi0/1, putting Gi0/1 in err-disable state
```

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.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

No member port is shown in the output.

**Important:** If this is a "choose two" questions, you should also choose the answer that mention about shut and no shut the error-disabled ports in order to recovery all the disabled ports.

**QUESTION 295**

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Unlike HSRP or GLBP, VRPP is an open standard. Only VRRPv3 supports both IPv4 and IPv6.

**QUESTION 296**

In a Cisco SD-Access fabric, which control plane protocol is used for mapping and resolving endpoints?

- A. LISP
- B. DHCP

- C. SXP
- D. VXLAN

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 297**

What are two characteristics of Cisco SD-Access elements? (Choose two)

- A. Fabric endpoints are connected directly to the border node
- B. The border node is required for communication between fabric and nonfabric devices
- C. The control plane node has the full RLOC-to-EID mapping database
- D. Traffic within the fabric always goes through the control plane node
- E. The border node has the full RLOC-to-EID mapping database

**Correct Answer:** BC  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

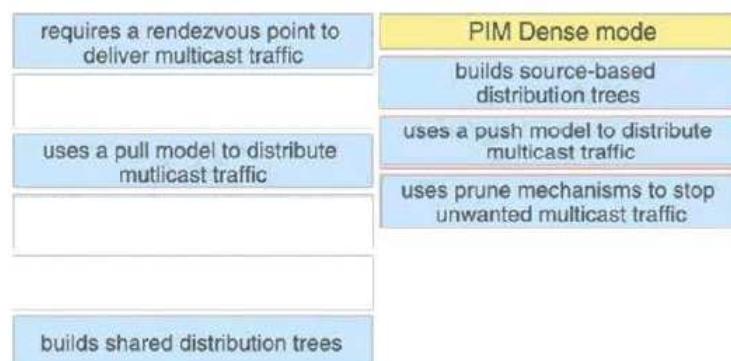
**QUESTION 298**

Drag and drop characteristics of PIM dense mode from the left to the right. (Choose three)?

- A. requires a rendezvous point to deliver multicast traffic
- B. builds source-based distribution trees
- C. uses a pull model to distribute multicast traffic
- D. uses a push model to distribute multicast traffic
- E. uses prune mechanisms to stop unwanted multicast traffic
- F. builds shared distribution trees

**Correct Answer:** BDE  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**



**QUESTION 299**

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

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

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

The BFD protocol detects link failures between routers. It measures data loss and latency on the data tunnel to determine the status of the devices at either end of the connection.

BFD is enabled by default on all connections between Cisco vEdge devices. You cannot disable BFD.

**QUESTION 300**

When a wired client connects to an edge switch in an SDA fabric, which component decides whether the client has access to the network?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 301**

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

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

**Correct Answer:** B

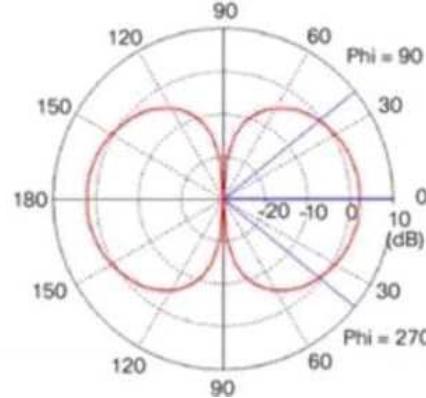
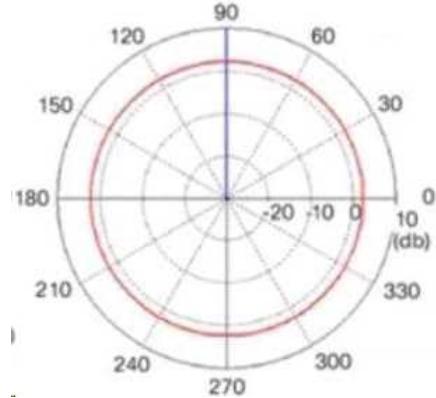
**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 302**

Refer to the exhibit.



Which type of antenna is shown on the radiation patterns?

- A. Dipole
- B. Yagi
- C. Patch
- D. Omnidirectional

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 303**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 304**

Drag and drop the LISP components on the left to the correct description on the right.

**Select and Place:**

map server	IPv4 or IPv6 address of an endpoint within a LISP site
ETR	network infrastructure component that learns of EID-prefix mapping entries from an ETR
EID	de-encapsulates LISP packets coming from outside of the LISP site to destinations inside of the site

Correct Answer:



Section: (none)

Explanation

Explanation/Reference:

#### QUESTION 305

An engineer must configure a GRE tunnel interface in the default mode. The engineer has assigned an IPv4 address on the tunnel and sourced the tunnel from an ethernet interface. Which additional configuration must be made on the tunnel interface?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

#### QUESTION 306

```

#!/usr/bin/env python3

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

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

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

def network_device_list(dnac, token):
    url = "https://{}api/v1/network-device".format(dnac["host"])
    headers["x-auth-token"] = token
    response = requests.get(url, headers=headers, verify=False)
    data = response.json()
    for item in data["response"]:
        dnac_devices.add_row([item["hostname"],item["platformId"],item["softwareType"],item["softwareVersion"],item["upTime"]])

```

Refer to the exhibit. Which code results in the working python script displaying a list of network devices from the Cisco DNA center?

- A. 

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

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

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

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 307

What is a type 2 hypervisor?

- A. Installed as an application on an already installed operating system.
- B. Runs directly on a physical server and includes its own operating system.
- C. Supports over-allocation of physical resources.
- D. Also referred to as a “bare metal hypervisor” because it sits directly on the physical server.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 308

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

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

Location D: -80 dBm

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

- A. The signal strength at location B is 10 dB better than location C.
- B. Location D has the strongest RF signal strength.
- C. The signal strength at location C is too weak to support web surfing.
- D. The RF signal strength at location B is 50% weaker than location A
- E. The RF signal strength at location C is 10 times stronger than location B

**Correct Answer:** DE

**Section:** Selected

**Explanation**

**Explanation/Reference:**

A, B and C are wrong since e.g. -75 dBm is a weaker signal string than -65 dBm

Since ratio[in dB] =  $10 \log_{10} (a/b)$ , the scale are therefore:

+10 dB = 10 times the power

-10 dB = one tenth power

+3 dB = double power

-3 dB = half the power

#### QUESTION 309

Which unit is used to express the signal-to-noise ratio?

- A. mW
- B. db
- C. amp
- D. dbm

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

#### QUESTION 310

Which design principle should be followed in a Cisco SD-Access wireless network deployment?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**SD-Access Wireless Network deployment:**

Access point:

AP will be directly connected to Fabric Edge Switch or to an external node switch

AP is part of fabric Overlay

AP will be part of INFRA-VN which will be further mapped to Global routing table

AP will join to WLC in Local Mode.

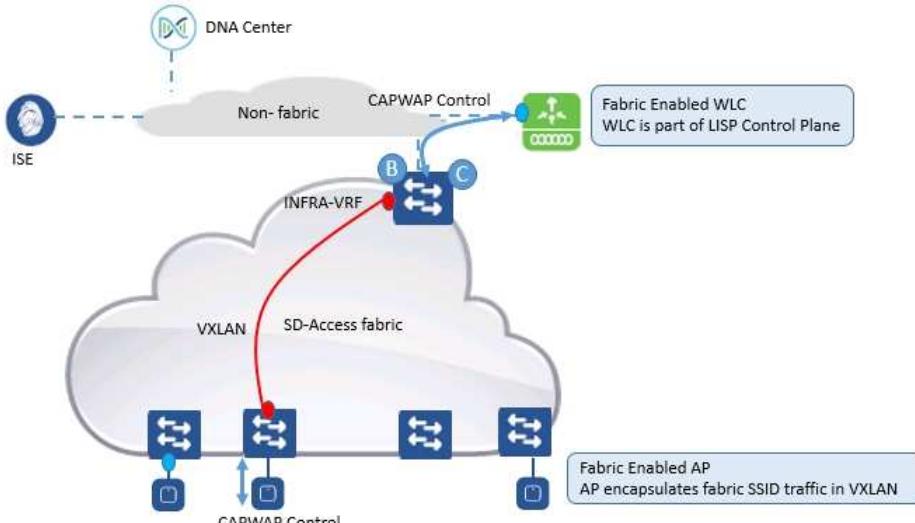
For Wireless LAN Controller:

WLC is connected to outside fabric or can also be connected directly to Border switch

WLC should be routed and reachable via Global Routing table.

There is no need for inter-VRF leaking for AP to join WLC

WLC can only communicate to one Control Plane Node (two for redundancy) and only one WLC can always be part of only one fabric Domain.



**QUESTION 311**

Which function does a fabric AP perform in a Cisco SD-Access deployment?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 312**

What is an advantage of using BFD?

- A. It detects link failure at layer 1 and updates routing table
- B. It detects local link failure at layer 3 and updates routing protocols
- C. It has sub-second failure detection for layer 1 and layer 3 problems.
- D. It has sub-second failure detection for layer 1 and layer 2 problems.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 313**

Refer to the exhibit.

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 314**

What is the function of vBond in a Cisco SDWAN deployment?

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

**Correct Answer:** C

**Section:** (none)

## Explanation

### Explanation/Reference:

vBond tells our vEdges where and how to connect to our organizations vManage and vSmart controllers, while also advising our vSmart controllers as new vEdges join the SD-WAN fabric.

vBond is the first point of contact and thus our first point of authentication for all SD-WAN components as they boot up and join the SD-WAN fabric. Each vBond requires a dedicated public IP address so that all other components can initiate connections to it.

Remarks : For the choice D, vManage is responsible for collecting network telemetry from our vEdge devices and alerting on events and outages in the SD-WAN environment

### QUESTION 315

Which three resources must the hypervisor make available to the virtual machines? (Choose three)

- A. memory
- B. bandwidth
- C. IP address
- D. processor
- E. storage
- F. secure access

**Correct Answer:** ADE

**Section:** (none)

**Explanation**

### Explanation/Reference:

### QUESTION 316

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"]:
    print(interface["enabled"])
    print(interface["description"])
```
- B. 

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

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

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

**Correct Answer:** C

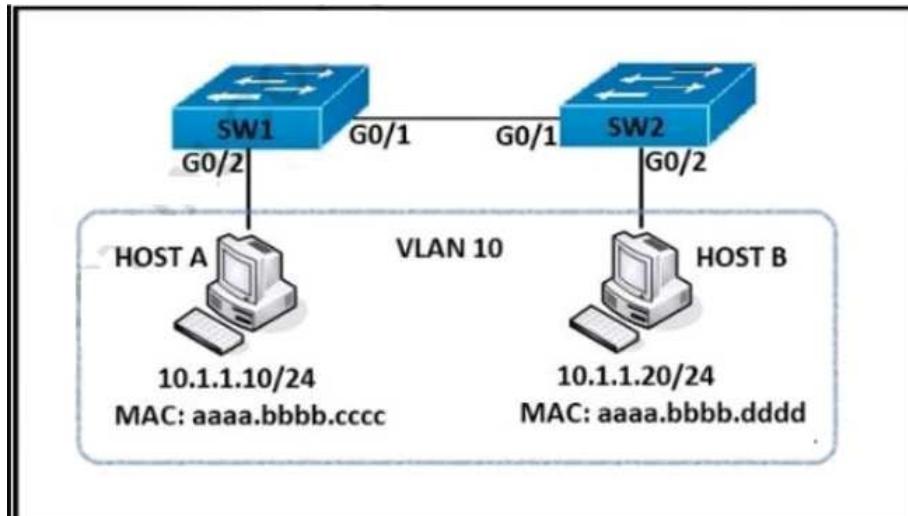
**Section:** Selected

**Explanation**

### Explanation/Reference:

### QUESTION 317

Refer to the exhibit.



An engineer must deny HTTP traffic from host A to host B while allowing all other communication between the hosts. Which command set accomplishes this task?

- A. 

```
SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)#permit tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# ip access-list extended MATCH_ALL
SW1(config-ext-nacl)# permit ip any any

SW1(config)# vlan access-map HOST-A-B 10
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# action drop
SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address MATCH_ALL
SW1(config-access-map)# action forward

SW1(config)# vlan filter HOST-A-B vlan 10
```
- B. 

```
SW1(config)# mac access-list extended HOST-A-B
SW1(config-ext-macl)# permit host aaaa.bbbb.cccc aaaa.bbbb.dddd

SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)#deny tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# vlan access-map DROP-MAC 10
SW1(config-access-map)# match mac address HOST-A-B
SW1(config-access-map)# action drop
SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# action drop
```
- C. 

```
SW1(config)# mac access-list extended HOST-A-B
SW1(config-ext-macl)# permit host aaaa.bbbb.cccc aaaa.bbbb.dddd

SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)#permit tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# vlan access-map DROP-MAC 10
SW1(config-access-map)# match mac address HOST-A-B
SW1(config-access-map)# action forward
SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# action drop

SW1(config)# vlan filter HOST-A-B vlan 10
```

D. SW1(config)# ip access-list extended DENY-HTTP  
 SW1(config-ext-nacl)#deny tcp host 10.1.1.10 host 10.1.1.20 eq www  
 SW1(config)# ip access-list extended MATCH\_ALL  
 SW1(config-ext-nacl)# permit ip any any  
 SW1(config)# vlan access-map HOST-A-B 10  
 SW1(config-access-map)# match ip address DENY-HTTP  
 SW1(config-access-map)# action drop

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

To define a VLAN access map, perform this task:

Command	Purpose
Router(config)# <b>vlan access-map map_name [0-65535]</b>	Defines the VLAN access map. Optionally, you can specify the VLAN access map sequence number.

To configure a match clause in a VLAN access map sequence, perform this task:

Command	Purpose
Router(config-access-map)# <b>match {[ip   ipv6] address [1-199   1300-2699   acl_name]   [mac address acl_name]}</b>	Configures the match clause in a VLAN access map sequence.

To configure an action clause in a VLAN access map sequence, perform this task:

Command	Purpose
Router(config-access-map)# <b>action {drop [log]   [forward {capture   vlan vlan_ID}]   [redirect {[fastethernet   gigabitethernet   tengigabitethernet] slot/port}   [port-channel channel_id]}</b>	Configures the action clause in a VLAN access map sequence.

To apply a VLAN access map, perform this task:

Command	Purpose
Router(config)# <b>vlan filter map_name vlan-list</b>	Applies the VLAN access map to the specified VLANs.

**QUESTION 318**

Refer to the exhibit.

```
event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.3 get-type next entry-op gt entry-val 80 poll-interval 5
!
action 1.0 cli command "enable"
action 2.0 syslog msg "high cpu"
action 3.0 cli command "term length 0"
```

An engineer must create a script that appends the output of the show process cpu sorted command to a file. Which action completes the configuration?

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

**Correct Answer:** B  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

**QUESTION 319**

Refer to the exhibit.

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

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

A network administrator configured RSPAN to troubleshoot an issue between switch1 and switch2. The switches are connected using interface GigabitEthernet 1/1 An external packet capture device is connected to switch2 interface GigabitEthernet1/2 Which two commands must be added to complete this configuration? (Choose two)

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

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

There are problems in Switch2 settings shown in the exhibit:

- RSPAN VLAN i.e. 70 is not allowed in trunk
- Destination interface is incorrect.

Remarks : E is correct due to the settings about destination interface. The number being used in monitor session is not important since there is no need to match session number in different switches.

#### QUESTION 320

Which function is handled by vManage in the Cisco SD-WAN fabric?

- A. Establishes BFD sessions to test liveness of links and nodes
- B. Distributes policies that govern data forwarding
- C. Performs remote software upgrades for WAN Edge, vSmart and vBond
- D. Establishes IPsec tunnels with nodes.

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

#### QUESTION 321

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 322

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

action should the engineer use?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 323

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 324

An engineer runs the sample code, and the terminal returns this output.

**Sample Code**

```
#!/usr/bin/env python
```

```
import json
import sys

test_json = """
{
    "type": "Cisco ASR 1001-X Router",
    "lastUpdateTime": 1552394222783,
    "macAddress": "00:c8:8b:80:bb:00",
    "serialNumber": "FXS1932Q1SE"
}
"""

print(json.load(test_json))
```

**Output**

```
$ python print_json.py
```

```
Traceback (most recent call last):
```

```
  File "question_3.py", line 15, in <module>
    Print(json.load(test_json))
  File
  "/System/Library/Framework/Python.framework/Versions/2.7/lib/python2.7/json/_init_.py", line 286 in load
    return loads(fp.read(),
AttributeError: 'str' object has no attribute 'read'
```

Which change to the sample code corrects this issue?

- A. Change the JSON method from load() to loads().
- B. Enclose null in the test\_json string in double quotes
- C. Use a single set of double quotes and condense test\_json to a single line
- D. Call the read() method explicitly on the test\_json string

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 325

Refer to the exhibit.

```

R1#show access-list 100
Extended IP access list 100
 10 deny ip any any
 20 permit ip 192.168.0.0 0.0.255.255 any
 30 permit ip any 192.168.0.0 0.0.255.255

```

Extended access-list 100 is configured on interface GigabitEthernet 0/0 in an inbound direction, but it does not have the expected behavior of allowing only packets to or from 192.168.0.0/16.

Which command set properly configures the access list?

- A. R1(config)#ip access-list extended 100  
R1(config-ext-nacl)#5 permit ip any any
- B. R1(config)#no access-list 100 seq 10  
R1(config)#access-list 100 seq 40 deny ip any any
- C. R1(config)#no access-list 100 deny ip any any
- D. R1(config)#ip access-list extended 100  
R1(config-ext-nacl)#no 10

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

For B, you cannot use sequence number when editing the ACL using the old configuration way.  
C is NOT correct since it will remove the entire ACL.

#### QUESTION 326

Refer to the exhibit.

```

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

Switch1#show etherchannel summary
!output omitted

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

Switch2#show etherchannel summary
!output omitted

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

```

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

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

**Correct Answer:** C

**Section:** (none)

## Explanation

Explanation/Reference:

### QUESTION 327

A customer has 20 stores located throughout a city. Each store has a single Cisco AP managed by a central WLC. The customer wants to gather analytics for users in each store. Which technique supports these requirements?

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

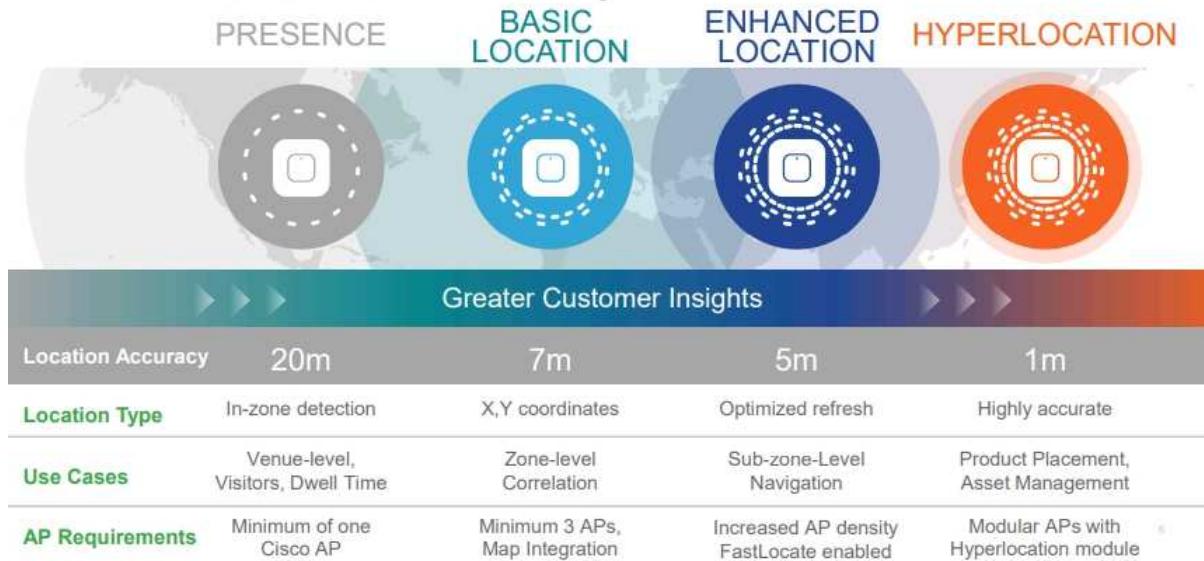
**Correct Answer:** B

Section: (none)

Explanation

Explanation/Reference:

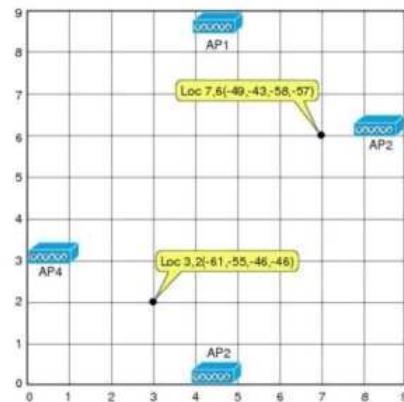
## Different levels of accuracy



Remarks : With three or more AP, more precise location of users can be determined.

## Location Patterning (Fingerprinting)

- Location patterning is based on the sampling and recording of radio signal behavior patterns in specific environments
- Location patterning assumes:
  - That each potential device location ideally possesses a distinctly unique RF "signature"
  - That each floor or subsection possesses unique signal propagation characteristics
- Deployment of patterning-based positioning systems can typically be divided into two phases:
  - Calibration phase
  - Operation phase



### QUESTION 328

Refer to the exhibit.

```

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

```

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

- A. Configure a match-host type NAT pool
- B. Reconfigure the pool to use the 192.168.1.0 address range
- C. Increase the NAT pool size to support 254 usable addresses
- D. Configure a one-to-one type NAT pool

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Without "overload", it is actually a one-to-one NAT and therefore a matching number of public IP addresses is required in order for enough addresses for all users.

#### QUESTION 329

How do 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 have lower upfront costs than on-premises deployments.
- D. Cloud deployments require less frequent upgrades than on-premises deployments.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Both deployments require upgrades from time to time, however, some upgrades for cloud deployments may be performed by service provider.

#### QUESTION 330

Refer to the exhibit.

```

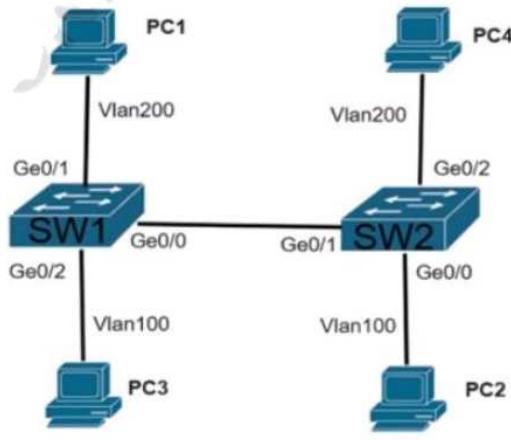
SW1# show interfaces gigabitethernet 0/0 switchport
Name: Gi0/0
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native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

```

```

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

```



The connection between SW1 and SW2 is not operational. Which two actions resolve the issue? (Choose two.)

- A. configure switchport mode access on SW2
- B. configure switchport nonegotiate on SW2
- C. configure switchport mode trunk on SW2
- D. configure switchport nonegotiate on SW1
- E. configure switchport mode dynamic desirable on SW2

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Sw2 has to change according to C or D in order to form trunk with Sw1 (having dynamic auto).

In fact, there are some problems in this question.

- For C, since the "Administrative Trunking Encapsulation" in Sw2 is "negotiate", you should manually configure the trunk encapsulation "dot1q" before you can configure "mode trunk".
- For E, since the "Negotiation of Trunking" in Sw1 is "Off", trunk cannot be formed by negotiation. Hence, you should manually configure "no switchport nonegotiate" in Sw1 before negotiation can occur.

The following shows a better answer which involves performing both tasks for resolving the issue:

- configure **no switchport nonegotiate** on Sw1 (this choice is not available in this question).
- configure **switchport mode dynamic desirable** on SW2 (i.e. E).

**QUESTION 331**

Which of the following statements regarding BFD are correct? (Select 2 choices.)

- A. BFD is supported by OSPF, EIGRP, BGP, and IS-IS.
- B. BFD detects link failures in less than one second.
- C. BFD can bypass a failed peer without relying on a routing protocol.
- D. BFD creates one session per routing protocol per interface.
- E. BFD is supported only on physical interfaces.
- F. BFD consumes more CPU resources than routing protocol timers do.

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 332**

In a Cisco DNA Center Plug and Play environment, why would a device be labeled unclaimed?

- A. The device has not been assigned a workflow.
- B. The device could not be added to the fabric.
- C. The device had an error and could not be provisioned.
- D. The device is from a third-party vendor.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The Network Plug and Play application provides a way to automatically and remotely provision and onboard new network devices with minimal network administrator and field personnel involvement.

To access the Network Plug and Play application after it is installed, from the Cisco DNA Center home page, click the Network Plug and Play tool. In the Pie chart showing the number of devices in each of the following states:

**Error**—Device had an error and could not be provisioned.

**Unclaimed**—Device has not been assigned a workflow.

**Planned**—Device is added to Network Plug and Play and has been assigned a workflow, but has not yet contacted the server.

**Provisioned**—Device is successfully onboarded and added to inventory.

**QUESTION 333**

An engineer is concerned with the deployment of a new application that is sensitive to inter-packet delay variance. Which command configures the router to be the destination of jitter measurements?

- A. Router(config)# ip sla responder udp-connect 172.29.139.134 5000
- B. Router(config)# ip sla responder tcp-connect 172.29.139.134 5000
- C. Router(config)# ip sla responder udp-echo 172.29.139.134 5000
- D. Router(config)# ip sla responder tcp-echo 172.29.139.134 5000

**Correct Answer:** C

**Section:** (none)

**Explanation**

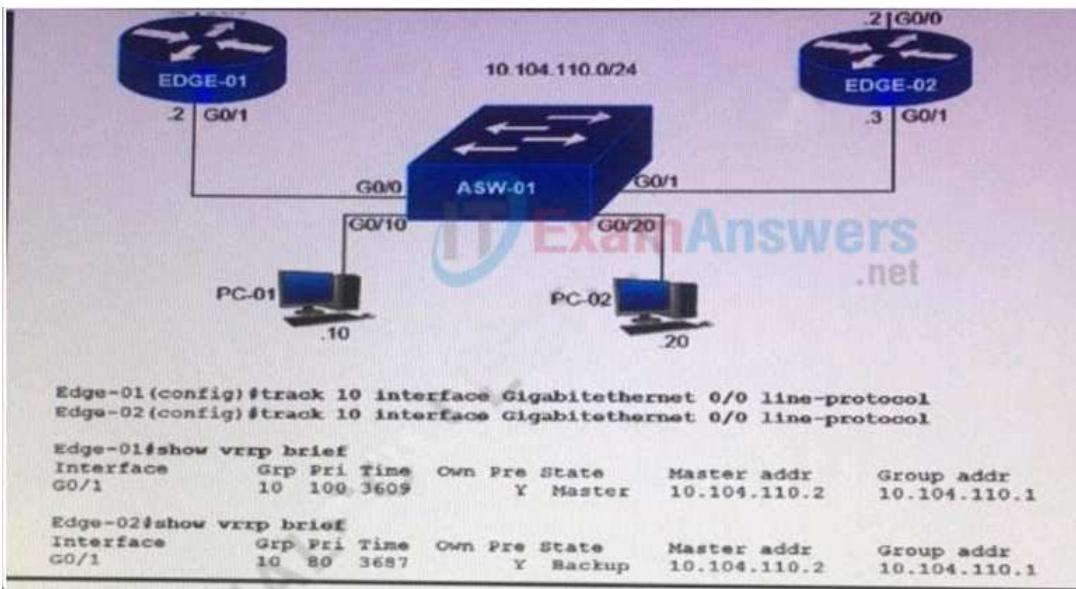
**Explanation/Reference:**

Among the choices, C is the best. There is no tcp-echo operation.

Better choices, if available, are icmp-jitter and udp-jitter.

**QUESTION 334**

Refer to the exhibit.



Object tracking has been configured for VRRP. Enabled routers Edge-01 and Edge-02. Which commands cause Edge-02 to preempt Edge-01 in the event that interface G0/0 goes down on Edge-01?

- A. Edge-01(config)#interface G0/1  
Edge-01(config-if)#vrrp 10 track 10 decrement 30
- B. Edge-02(config)#interface G0/1  
Edge-02(config-if)#vrrp 10 track 10 decrement 30
- C. Edge-02(config)#interface G0/1  
Edge-02(config-if)#vrrp 10 track 10 decrement 10
- D. Edge-01(config)#interface G0/1  
Edge-01(config-if)#vrrp 10 track 10 decrement 10

**Correct Answer: A**

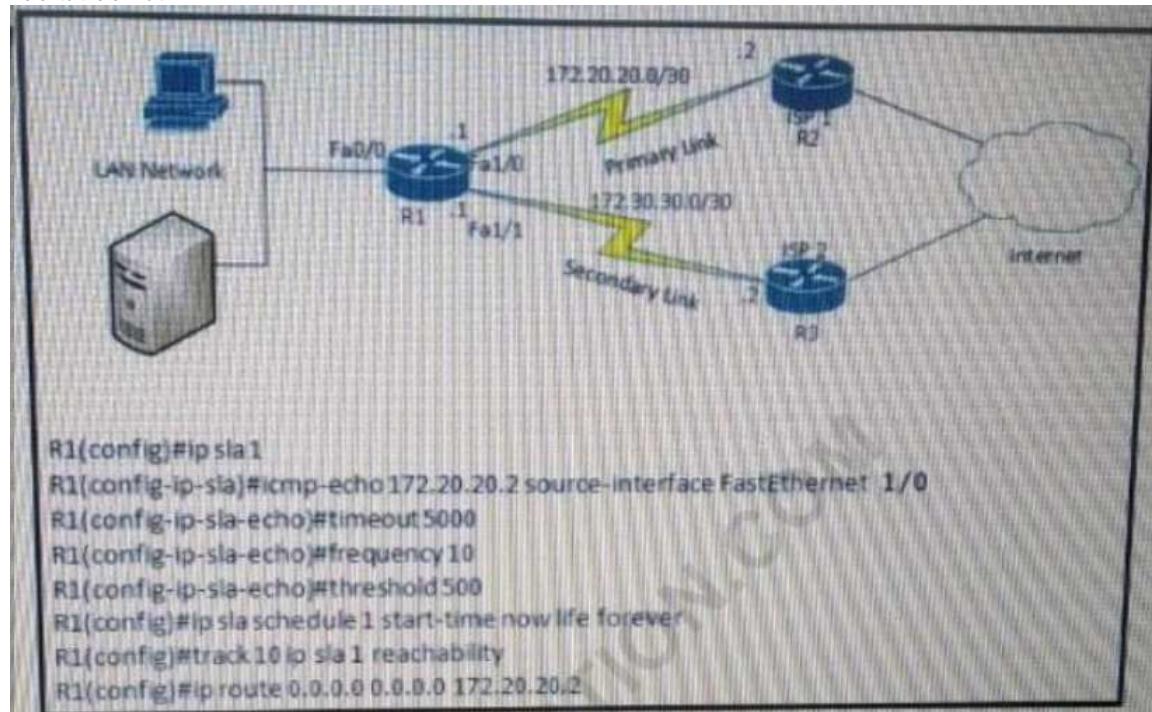
Section: (none)

Explanation

Explanation/Reference:

#### QUESTION 335

Refer to the exhibit.



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

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

**Correct Answer: C**

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 336**

Which protocol is implemented to establish secure control plane adjacencies between Cisco SD-WAN nodes?

- A. IKE
- B. DTLS
- C. IPsec
- D. ESP

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

The foundation of the control plane is one of two security protocols derived from SSL (Secure Sockets Layer)—the Datagram Transport Layer Security (DTLS) protocol and the Transport Layer Security (TLS) protocol. The vSmart controller, which is the centralized brain of the Cisco SD-WAN solution, establishes and maintains DTLS or TLS connections to all Cisco SD-WAN devices in the overlay network: to the routers, the vBond orchestrators, to Cisco vManage, and to other vSmart controllers. These connections carry control plane traffic. DTLS or TLS provides communication privacy between Cisco SD-WAN devices in the network, using the Advanced Encryption Standard (AES-256) encryption algorithm to encrypt all control traffic sent over the connections.



**QUESTION 337**

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Since it is a long-standing issue, the VM should be relocated. Live migrate is the method of moving VM to another hypervisor while it is still running. On the other hand, if the VM does not need to be running all the time, you can simply power it off before moving it.

**QUESTION 338**

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 339**

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 340**

What are two methods of ensuring that the multicast RPF check passes without changing the unicast routing table? (Choose two.)

- A. implementing static mroutes
- B. disabling BGP routing protocol
- C. implementing MBGP
- D. disabling the interface of the router back to the multicast source
- E. implementing OSPF routing protocol

**Correct Answer:** AC

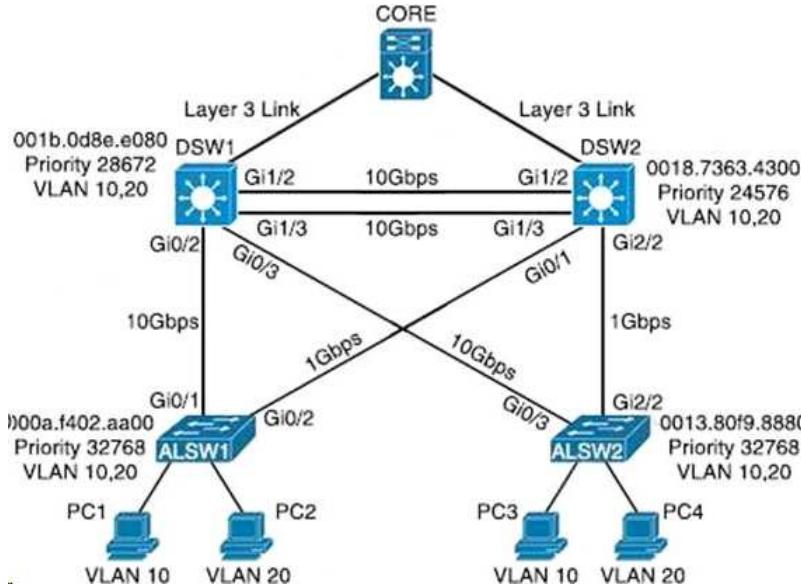
**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 341**

Refer to the exhibit.



Which two commands ensure that traffic from PC1 is forwarded over Gi1/3 trunk port between DWS1 and DSW2? (Choose two)

- A. DWS1(config-if)#spanning-tree port-priority 0
- B. DSW2(config-if)#spanning-tree port-priority 16
- C. DSW1(config-if)#interface gi1/3
- D. DSW2(config-if)#interface gi1/3
- E. DSW2(config-if)#spanning-tree port-priority 128

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 342**

How does EIGRP differ from OSPF?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

EIGRP metric can be based on bandwidth and delay. OSPF metric is based on bandwidth only.

**QUESTION 343**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

On Cisco Nexus devices, you can configure quality of service (QoS) policies for classification and marking on VLANs. The policies that you apply to a VLAN are applied to the traffic on the VLAN's Layer 2 and switch virtual interface (SVI) ports.

The QoS TCAM region is shared by the interface QoS, system QoS, and VLAN QoS policies. You need to limit the number of TCAM entries for the interface QoS policies in order to define VLAN QoS policies. Use the `hardware profile tcam feature interface-qos limit tcam-size` to configure this limit.

#### QUESTION 344

Which level message does the WLC send to the syslog server?

- A. syslog level errors and less severity messages
- B. syslog level errors messages
- C. all syslog levels messages
- D. syslog level errors and greater severity messages

**Correct Answer:** D

**Section:** (none)

**Explanation**

#### Explanation/Reference:

Only D is reasonable (although errors may not be the default severity level).

Note that greater severity means less value in severity level. Hence if the choices include the word "value" or "number", the following should be chosen. syslog level errors and less severity **level value** messages

The following is extracted from the documentation for Wireless LAN Controllers running AireOS 8.8.111.0 Software.

To set the Syslog Level (severity) for filtering syslog messages to the syslog servers, choose one of the following options from the Syslog Level drop-down list:  
Emergencies= Severity level 0  
Alerts= Severity level 1 (default value)  
Critical= Severity level 2  
Errors= Severity level 3  
Warnings= Severity level 4  
Notifications= Severity level 5  
Informational= Severity level 6  
Debugging= Severity level 7

The following shows the GUI for changing the syslog severity level to "Informational":

The screenshot shows the Cisco WLC Management interface. The top navigation bar includes CISCO, MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, and MANAGEMENT. The MANAGEMENT tab is selected. On the left, a sidebar lists various management categories: Summary, SNMP, HTTP-HTTPS, Telnet-SSH, Serial Port, Local Management, Users, User Sessions, Logs (selected), Mgmt Via Wireless, and Tech Support. The 'Logs' section is expanded, showing Config, Message logs, and File Info checkboxes. The main content area is titled 'Syslog Configuration'. It contains fields for 'Syslog Server IP Address' (192.168.100.10) with an 'Add' button, 'Syslog Level' (set to 'Informational'), and 'Syslog Facility' (set to 'Local Use 0'). Below this is the 'Msg Log Configuration' section, which includes 'Buffered Log Level' (Errors), 'Console Log Level' (Disable), and checkboxes for 'File Info' and 'Trace Info'.

#### QUESTION 345

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

**Correct Answer:** B

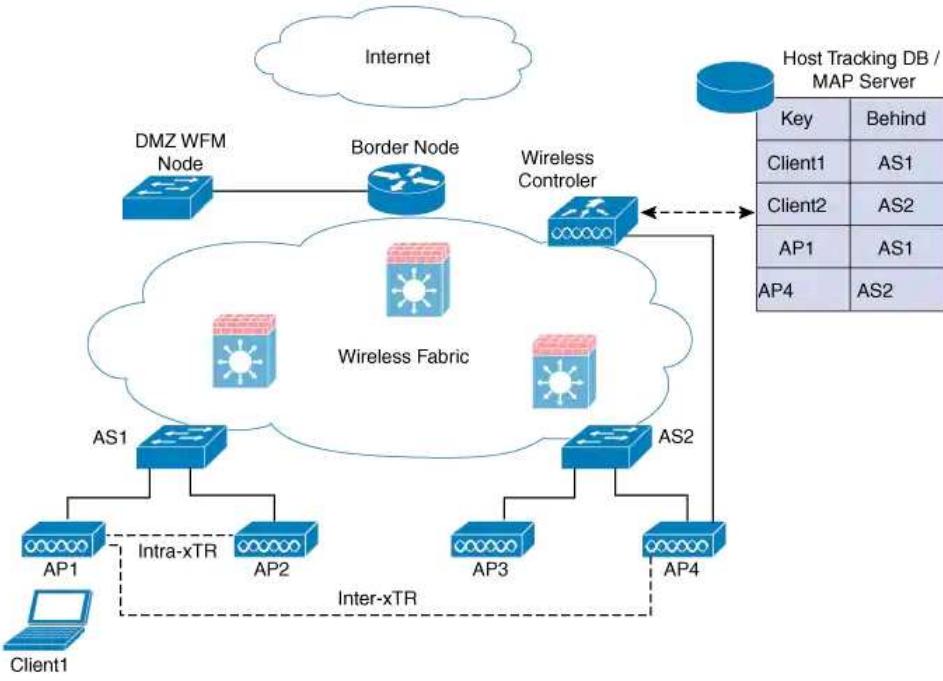
**Section:** Selected

**Explanation**

#### Explanation/Reference:

SDA supports two additional types of roaming, which are Intra-xTR and Inter-xTR. In SDA, xTR stands for an access-switch that is a fabric edge node. It serves both as an ingress tunnel router as well as an egress tunnel router.

The following shows an example of inter-xTR since the access switch connected by the new AP (AP4) is different.



#### QUESTION 346

```

interface Vlan10
ip vrf forwarding Clients
ip address 192.168.1.1 255.255.255.0
!
interface Vlan20
ip vrf forwarding Servers
ip address 172.16.1.1 255.255.255.0
!
interface Vlan30
ip vrf forwarding Printers
ip address 10.1.1.1 255.255.255.0

```

Refer to the exhibit. An engineer attempts to configure a router so that the client 192.168.1.100 connected through vrf Clients can access the servers connected to VRF Servers.

- A. ip route vrf Clients 172.16.1.0 255.255.255.0 172.16.1.1 Servers  
ip route vrf Servers 192.168.1.100 255.255.255.255 192.168.1.1 Clients
- B. ip route vrf Clients 172.16.1.0 255.255.255.0 172.16.1.1 global  
ip route vrf Servers 192.168.1.100 255.255.255.255 192.168.1.1 global
- C. ip route vrf Clients 172.16.1.1 255.255.255.255 172.16.1.1 global  
ip route vrf Servers 192.168.1.100 255.255.255.0 192.168.1.1 global
- D. ip route vrf Clients 172.16.1.0 255.255.255.0 172.16.1.1 Clients  
ip route vrf Server2 192.168.1.100 255.255.255.255 192.168.1.1 Server2

**Correct Answer:** B

**Section:** (none)

**Explanation**

#### Explanation/Reference:

Normally MP-BGP is used for inter VRF forwarding. However static route can also be used but the global routing table (i.e. the default routing table) must be used.

For packets 192.168.1.100 (vrf Clients) --> 172.16.1.x (vrf Servers).

- You need to configure a static route in vrf Clients about the network 172.16.1.0/24 and sent it to Global.
- Then you need to configure a status route in global routing table about network 172.16.1.0/24 and sent it to the interface VLAN 20. (Note that this is needed since int VLAN 20 is a connected network of vrf Servers and therefore not appears in global routing table by default).

For returned packets 172.16.1.x (vrf Servers) --> 192.168.1.100 (vrf Clients)

- You need to configure a static route in vrf Servers about the host 192.168.1.100/32 and sent it to Global.
- Then you need to configure a status route in global routing table about network 192.168.1.0/24 and sent it to the interface VLAN 10. (Note that this is needed since int VLAN 10 is a connected network of vrf Clients and therefore not appears in global routing table by default).

**QUESTION 347**

```
line vty 0 4
<settings omitted>
line vty 5 15
<settings omitted>
```

Which of the following configures the all vty terminal sessions to be terminated in 600 seconds.

- A. line vty 0 4  
exec-timeout 600
- B. line vty 0 15  
exec-timeout 10 0
- C. line vty 0 15  
exec-timeout 600
- D. line vty 0 15  
no exec-timeout

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Note that since 0 - 4 and 5 - 15 are defined, you need to use 0 - 15 to configure all vty terminal lines.

```
Router(config-line)#exec-timeout ?
<0-35791> Timeout in minutes

Router(config-line)#exec-timeout 0 ?
<0-2147483> Timeout in seconds
<cr>
```

Since the configuration is in minutes and seconds, you can either configure:

- exec-timeout 10 OR
- exec-timeout 10 0

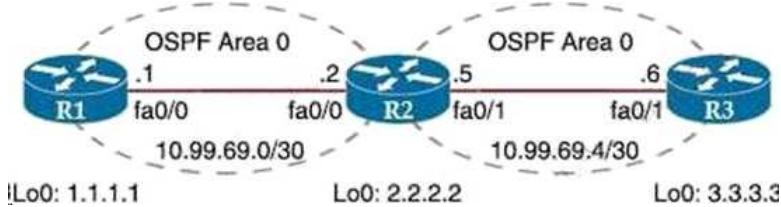
**Important:**

If the question asks you to allow SSH access from 10.10.10.0/24 and disallow all other vty connections, the additional settings will be:

```
access-list 1 permit 10.10.10.0 0.0.0.255
line vty 0 15
access-class 1 in
transport input ssh
```

**QUESTION 348**

Refer to the exhibit.



In R1, issuing traceroute to 3.3.3.3 shows result with symbol !A.

Why do traceroute fail?

- A. The loopback on R3 is in a shutdown state.
- B. OSPF redistribution is not configured.
- C. An ACL applied in fa0/1 inbound
- D. An ACL applied in R2's lo0 inbound

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

If you find "!A" in the output of traceroute, it means that packets have been dropped (usually by access control).

The following shows the output of ping when packets are dropped by access control:  
U.U.U

The following shows the output of traceroute when packets are dropped by access control:  
!A !A \*

**QUESTION 349**

HQ (100.100.100.100) ---- ISP1 ---- IP Network --- ISP2 --- BR (200.200.200.200)

A GRE tunnel is formed between HQ and BR routers.

If a GRE packet captured by a protocol analyser has the following characteristics:

```
Ethernet II, Src: 50:00:00:00:00:01 Dst: 50:00:00:00:00:02
Internet Protocol Version 4, Src 100.100.100.100 Dst : 200.200.200.200
Generic Routing Encapsulation (IP)
```

Internet Protocol Version 4, Src 192.168.100.1 Dst : 192.168.100.2  
Internet Control Message Protocol

What is the tunnel IP of the HQ router?

- A. 100.100.100.100
- B. 200.200.200.200
- C. 192.168.100.1
- D. 192.168.100.2

**Correct Answer:** C

**Section:** (none)

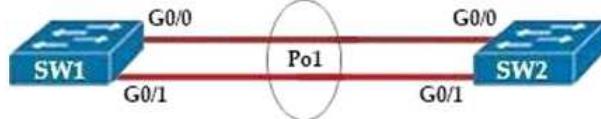
**Explanation**

**Explanation/Reference:**

Since there is no further information, we can only assume the ping packet is sent by HQ to BR. (i.e. someone ping the BR router's tunnel's IP from HQ router)

Since the source 100.100.100.100 of the outer IP header is the IP of HQ router, the source of the inner IP packet i.e. 192.168.100.1 is the tunnel IP of the HQ router.

**QUESTION 350**



```
Sw1(config)#interface range g0/0-1
Sw1(config-if-range)#switchport trunk encapsulation dot1q
Sw1(config-if-range)#switchport mode trunk
Sw1(config-if-range)#channel-group 1 mode active
Sw1(config)#channel-group 1 mode active
```

Connection between the two switches are down. What should be configured in Sw2 if it's Po1 is shown as down with PAgP configured as the link aggregation protocol?

- A. Sw2(config-if-range)#channel-group 1 mode on
- B. Sw2(config-if-range)#channel-group 1 mode passive
- C. Sw2(config-if-range)#channel-group 1 mode auto
- D. Sw2(config-if-range)#channel-group 1 mode negotiate

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since Sw1 is configured with active i.e. LACP, you must also use LACP in Sw2 (i.e. active or passive).

**QUESTION 351**

What is the function of the Cisco DNA Center in a Cisco SD-Access deployment?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In SD-Access, Cisco DNA Center centrally manages major configuration and operations workflow areas.

- Design—Configures device global settings, network site profiles for physical device inventory, DNS, DHCP, IP addressing, SWIM repository, device templates, and telemetry configurations such as Syslog, SNMP, and NetFlow.
- Policy—Defines business intent including creation of virtual networks, assignment of endpoints to virtual networks, policy contract definitions for groups, and configures application policies (QoS).
- Provision—Provisions devices and adds them to inventory for management, supports Cisco Plug and Play, creates fabric sites along with other SD-Access components, and provides service catalogs such as Stealthwatch Security Analytics and Application Hosting on the Cisco Catalyst 9000 Series Switches.
- Assurance—Enables proactive monitoring and insights to confirm user experience meets configured intent, using network, client, and application health dashboards, issue management, sensor-driven testing, and Cisco AI Network Analytics.
- Platform—Allows programmatic access to the network and system integration with third-party systems via APIs by using feature set bundles, configurations, a runtime dashboard, and a developer toolkit.

**QUESTION 352**

Drag and drop the characteristic from the left onto the orchestration tools that they describe on the right.

Which are the characteristics of Ansible (Choose Two)?

- A. Pull Model
- B. Push Model
- C. Multimaster Architecture
- D. Primary / Secondary Architecture

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



Both Ansible and Puppet have backups in case of failure, meaning availability need never be interrupted. Ansible has a secondary node in case the active node fails, and Puppet has more than one master in case the original master fails.

#### QUESTION 353

Which new enhancement was implemented in Wi-Fi 6?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Wi-Fi 6 technology dimensions:

- Denser modulation using 1024 Quadrature Amplitude Modulation (QAM), enabling a more than 35 percent speed burst.
- Orthogonal Frequency Division Multiple Access (OFDMA)-based scheduling to reduce overhead and latency.
- Robust high-efficiency signaling for better operation at a significantly lower Received Signal Strength Indication (RSSI).
- Better scheduling and longer device battery life with Target Wake Time (TWT)

In Wi-Fi 6 i.e. 802.1ax, MU-MIMO is supported in both downlink and uplink. Moreover, multiplexing through frequency domain is also introduced. The techniques of using frequency domain with MU-MIMO is also introduced and is known as Orthogonal Frequency Division Multiple Access (OFDMA)

#### QUESTION 354

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 355

Refer to the exhibit. What does the snippet of code achieve?

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Although "hostkey\_verify" is used for verifying the public key (i.e. identity) of the connected node acting as SSH server. Since "with manager.connect" implies the use of ncclient, the above make a ncclient for NETCONF.

#### QUESTION 356

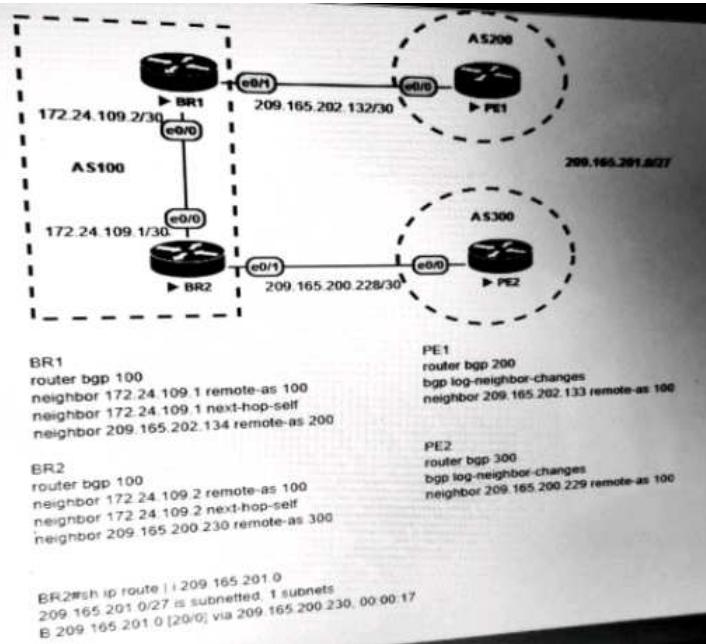
A customer has completed the installation of a Wi-Fi 6 greenfield deployment at their new campus. They want to leverage Wi-Fi 6 enhanced speeds on the trusted employee WLAN. To configure the employee WLAN, which two Layer 2 security policies should be used? (Choose two.)

- A. 802.1X
- B. WPA (AES)
- C. WPA2(AES)+WEP
- D. OPEN
- E. WEP

**Correct Answer: AC**  
Section: (none)  
Explanation

Explanation/Reference:

**QUESTION 357**



Which configuration change will force BR2 to reach 209.165.201.0/27 via BR1.

- A. Set the origin to igr on BR2 toward PE2 inbound
- B. Set the local preference to 150 on PE1 toward BR1 outbound
- C. Set the weight attribute to 65535 on BR1 toward PE1
- D. Set the MED to 1 on PE2 toward BR2 outbound

**Correct Answer: D**  
Section: (none)  
Explanation

Explanation/Reference:

A is wrong since among the origin, "igp" is preferred.  
B is wrong since setting Local Preference in PE1 will not sent to BR1 of another neighbor AS 100.  
C is wrong since it only affects BR1  
D seems correct since BR2 will prefer the BGP route with MED 0 learnt from iBGP neighbor BR1. However, you must configue "bgp always-compare-med" so that MED can be used for selecting BGP routes learnt from different ASes.

**QUESTION 358**

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

```
from json import dumps, loads  
  
Devices=[  
 {  
  'name': 'distsw1',  
  'ip': '192.168.255.1',  
  'type': 'Catalyst C9407R',  
  'user': 'netadmin',  
  'pass': '66674431c3577d398613263c0bf6fe5'  
 }]
```

- A. json.print(Devices)
- B. json.loads(Devices)
- C. json.dumps(Devices)
- D. json.repr(Devices)

**Correct Answer: C**  
Section: (none)  
Explanation

Explanation/Reference:

Since "Devices" is a object. You can export it as JSON format string with "dumps()".

Note that d1 (with quote around {}) stores a string while d2 stores an object.

```
d1 = '{ "person": { "name": "Kenn", "sex": "male", "age": 28}}'  
d2 = { "person": { "name": "Kenn", "sex": "male", "age": 28}}
```

**QUESTION 359**

What device makes the decision for a wireless client to roam?

- A. wireless client
- B. WLC
- C. Access Point
- D. WCS location server

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Roaming is a client side decision in 802.11 WiFi. Client devices listen for beacon frames or send probe requests to discover APs advertising the preferred SSID.

WLC can only attract a client to roam by adjusting the signal strength sent to the client by different APs.

**QUESTION 360**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple PIM-SM domains. The purpose of MSDP is to allow a RP to dynamically discover multicast sources in other PIM domains.

When MSDP is configured in a network, RPs exchange source information with RPs in other domains. An RP can join the interdomain source tree for sources that are sending to groups for which it has receivers.

**QUESTION 361**

What is one benefit in implementing a VSS architecture?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

VSS increases operational efficiency by simplifying the network, reducing switch management overhead by at least 50 percent.

- Single point of management, IP address, and routing instance for the Cisco Catalyst 6500 virtual switch
- Single configuration file and node to manage. Removes the need to configure redundant switches twice with identical policies.
- Removes the need for Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP)

**QUESTION 362**

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

- A. 0000.0c07.ac37
- B. 0000.0c07.ac25
- C. c0:00:00:25:00:00
- D. c0:39:97:655:5

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Note that the MAC address is in Hexidecimal characters and therefore group 37 should be represented as 25.

**QUESTION 363**

A Linux server is providing virtual machine along with DNS and DHCP services. Which technology does this represent?

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

**Correct Answer:** B

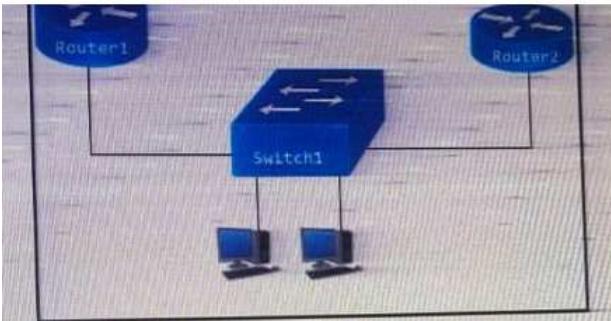
**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since the server is running Linux OS, the hypervisor for providing VM is a type 2 hypervisor.

**QUESTION 364**



Refer to the exhibit. Router1 is currently operating as the HSRP primary with a priority 110. Router1 fails and Router2 takes over the forwarding role. Which command on Router1 causes it to take over the forwarding role when it returns to service.

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 365

Refer to the exhibit. An engineer is installing a new pair of routers in a redundant configuration but they are not functioning as expected. What is the cause?

<b>R1</b>	<b>R2</b>
key chain cisco123	key chain cisco123
key 1	key 1
key-string Cisco123!	key-string cisco123!

Ethernet0/0 - Group 10

State is Active

8 state changes, last state change 00:03:33

Virtual IP address is 192.168.0.1

Active virtual MAC address is 0000.0c07.ac0a

<b>R1</b>	<b>R2</b>
key chain cisco123	key chain cisco123
key 1	key 1
key-string Cisco123!	key-string cisco123!

Ethernet0/0 - Group 10

State is Active

17 state changes, last state change 00:03:33

Virtual IP address is 192.168.0.1

Active virtual MAC address is 0000.0c07.ac0a

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

R1's key-string has an upper case "C" but R2's key-string has a lower case "c".

#### QUESTION 366

"HTTP/1.1 204 No Content" is returned when the `curl -i -X DELETE` command is issued. Which situation 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 is invalid.

**Correct Answer:** B

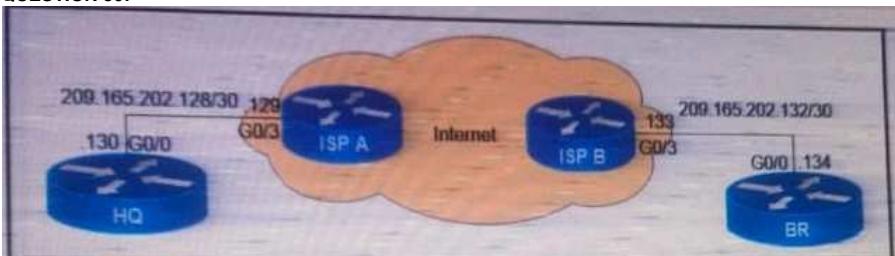
**Section:** (none)

**Explanation**

**Explanation/Reference:**

HTTP Status Code 204: The server has successfully fulfilled the request and that there is no additional content to send in the response payload body.

#### QUESTION 367



Refer to the exhibit. What is the effect of the following command when configured in GRE tunnel interface?

```
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 3 seconds and 5 retries.
- C. The keepalives are sent every 5 seconds and 3 retries.
- D. The tunnel line protocol does down when the keepalive counter reaches 5.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Normally, a GRE Tunnel interface comes up as soon as it is configured and it stays up as long as there is a valid tunnel source address or interface which is up. The tunnel destination IP address must also be routable. This is true even if the other side of the tunnel has not been configured.

The GRE tunnel keepalive mechanism is similar to PPP keepalives in that it gives the ability for one side to originate and receive keepalive packets to and from a remote router.

The remote router does not need to support GRE keepalives. Here is an example of a keepalive packet that originates from Router A and is destined for Router B. The keepalive response that Router B returns to Router A is already inside the Inner IP Header. Router B simply decapsulates the keepalive packet and sends it back out the physical interface (forming the tunnel). It processes the GRE keepalive packet just like any other GRE IP data packet.

**GRE Keepalives:**

GRE IP Header		GRE	IP Header		GRE
Source A	Destination B	PT=IP	Source B	Destination A	PT=0

```
Router# configure terminal
Router(config)#interface tunnel0
Router(config-if)#keepalive 5 4
!---- The syntax of this command is keepalive [seconds [retries]].
!---- Keepalives are sent every 5 seconds and 4 retries.
!---- Keepalives must be missed before the tunnel is shut down.
!---- The default values are 10 seconds for the interval and 3 retries.
```

**QUESTION 368**

Which command allows you to capture outgoing traffic from VLAN 3 on interface g0/3 while ignoring traffic of other VLANs on the same interface.

- A. monitor session 1 source interface g0/3 tx  
monitor session 1 filter vlan 1-2,4-4094
- B. monitor session 1 source interface g0/3 rx  
monitor session 1 filter vlan 1-2,4-4094
- C. monitor session 1 source interface g0/3 tx  
monitor session 1 filter vlan 3
- D. monitor session 1 source interface g0/3 rx  
monitor session 1 filter vlan 3

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

When you monitor a trunk port as a source port, all VLANs active on the trunk are monitored by default. You can use VLAN filtering in order to limit SPAN traffic monitoring on trunk source ports to specific VLANs. VLAN filtering applies only to trunk ports or to voice VLAN ports.

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor **traffic received** on Gigabit Ethernet trunk port 2, and send traffic for **only VLANs 1 through 5 and VLAN 9** to destination Gigabit Ethernet port 1.

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5, 9
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/1
```

**QUESTION 369**

What are the two characteristics of using SSO in network redundancy feature? (Choose two)

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

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 370**

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

- client mode
- SE-connect mode
- sensor mode
- sniffer mode

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Some new Aironet models have a new AP mode called "sensor" mode. Using a supported AP or dedicated sensor the device can actually function much like a WLAN client would associating and identifying client connectivity issues within the network in real time without requiring an IT or technician to be on site.

**QUESTION 371**

Drag and drop the Qos mechanisms from the left to the correct descriptions on the right.

**Select and Place:**

service policy	mechanism to create a scheduler for packets prior to forwarding
shaping	mechanism to apply a Qos policy to an interface
DSCP	portion of the IP header used to classify packets
policy map	bandwidth management technique which delays datagrams
policing	tool to enforce rate limiting on ingress/egress
Cos	portion of the 802.1Q header used to classify packets

**Correct Answer:**

	policy map
	service policy
	DSCP
	shaping
	policing
	Cos

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 372**

Drag and drop the Qos mechanisms from the left to the correct descriptions on the right.

**Select and Place:**

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

**Correct Answer:**

	policy map
	service policy
	DSCP

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 373**

```
Router# traceroute 10.10.10.1
Type escape sequence to abort.
Tracing the route to 10.10.10.1
1  10.0.0.1  5 msec  5 msec  5 msec
2  10.5.0.1  15 msec  17 msec  17 msec
3  10.10.10.1 *      *      *
```

Refer to the exhibit. An engineer is troubleshooting a connectivity issue and executes a traceroute.. What does the result confirm?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since Cisco uses UDP for traceroute, the destination may respond with ICMP port unreachable or protocol unreachable. Traceroute uses the ICMP error messages responded to obtain results e.g. the timing information.

In the above, the cause is probe timed out i.e. the destination did not response with anything or the responses were dropped due to traffic congestion.

**QUESTION 374**

What is the function of the LISP map resolver?

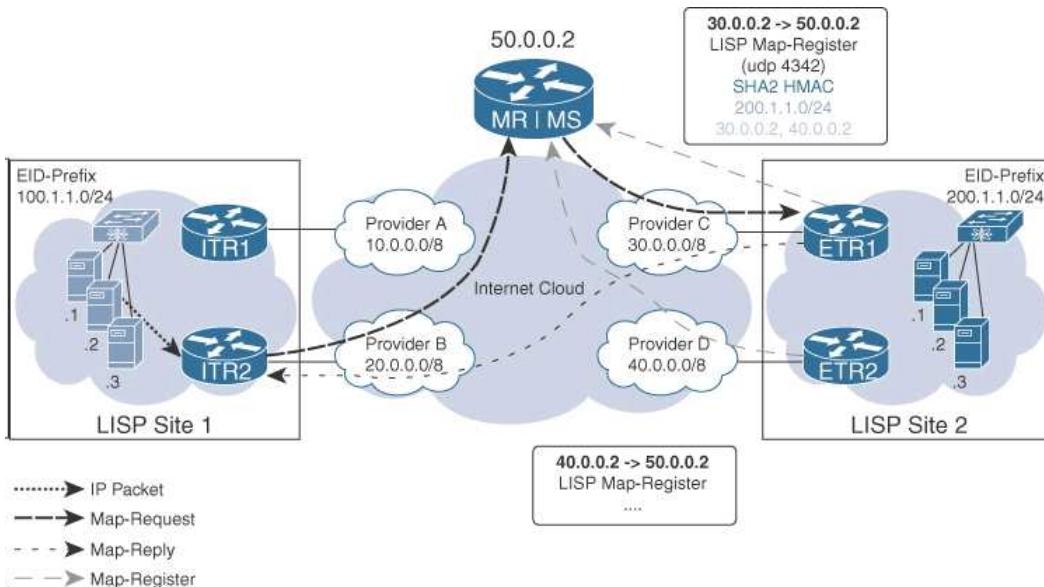
- A. to send traffic to non-LISP sites when connected to a service provider that does not accept nonroutable EIDs as packet sources.
- B. to connect a site to the LISP capable part of a core network, publish the EID-to-RLOC mappings for the site, and respond to the map-request messages.
- C. to decapsulate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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

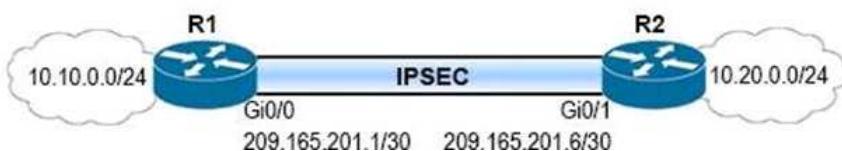


In this topology, when host S1 with IP address 100.1.1.1 tries to reach host D2 with IP address 200.1.1.2, it sends the packet to one of the local ITRs at the site. Then, if the ITR does not have an entry in its map cache table, the **ITR creates a map request** looking for the host 200.1.1.2 and sends it **to the map resolver (MR)**. The **map request is also LISP encapsulated** where the outer header has the source IP address of 200.0.0.2 and destination IP address of 50.0.0.2. Based on the request, the **MR forwards the map request to the map server (MS)**. The **MS redirects the packet to the ETR**, which has the information about the host prefix/subnet. One important thing to notice in this map request/map reply is that the map request comes toward the mapping system, but the mapping system does not send the reply. The **ETR sends the map reply directly to the ITR that raised the map request**. This significantly reduces the load on the MR/MS and at the same time helps validate the path between the ETR and the ITR. The map reply contain the mapping entries of the ETRs that hold the destination EIDs.

#### QUESTION 375

Refer to the exhibit.

<pre> access-list 100 permit gre host 209.165.201.1 host 209.165.201.6 crypto isakmp policy 5 authentication pre-share hash sha256 encryption aes group 14  crypto isakmp key D@t@c3nt3r address 209.165.201.6  crypto ipsec transform-set My_Set esp-aes esp-sha-hmac mode transport  crypto map MAP 10 ipsec-isakmp set peer 209.165.201.6 set transform-set My_Set match address 100  interface GigabitEthernet0/0 description outside_interface no switchport ip address 209.165.201.1 255.255.255.252 crypto map MAP  interface Tunnel 100 ip address 192.168.100.1 255.255.255.0 ip mtu 1400 tunnel source GigabitEthernet0/0 tunnel destination 209.165.201.6  ip route 10.20.0.0 255.255.255.0 192.168.100.2 Tunnel100 </pre>	<pre> access-list 100 permit gre host 209.165.201.6 host 209.165.201.1 crypto isakmp policy 5 authentication pre-share hash sha256 encryption aes group 14  crypto isakmp key D@t@c3nt3r address 209.165.201.1  crypto ipsec transform-set My_Set esp-aes esp-sha-hmac mode transport  crypto map MAP 10 ipsec-isakmp set peer 209.165.201.1 set transform-set My_Set match address 100  interface GigabitEthernet0/1 description outside_interface no switchport ip address 209.165.201.6 255.255.255.252 crypto map MAP  interface Tunnel 100 ip address 192.168.100.2 255.255.255.0 ip mtu 1400 tunnel source GigabitEthernet0/0 tunnel destination 209.165.201.1  ip route 10.10.0.0 255.255.255.0 192.168.100.1 Tunnel100 </pre>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



A network engineer must simplify the IPsec configuration by enabling IPsec over GRE using IPsec profiles.

Which two configuration changes accomplish this? (Choose two)

- A. Apply the crypto map to the tunnel interface and change the tunnel mode to tunnel mode ipsec ipv4
- B. Remove all configuration related to crypto map from R1 and R2 and eliminate the ACL 100
- C. Remove the crypto map and modify the ACL to allow traffic between 10.10.0.0/24 to 10.20.0.0/24
- D. Create an IPsec profile, associate the transform-set, and apply the profile to the tunnel interface
- E. Create an IPsec profile, associate the transform-set ACL, and apply the profile to the tunnel interface.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In IPsec configuration by Crypto Map, you need to setup ACL to determine the traffic that needs to be protected (i.e. sending through the IPsec tunnel).

In IPsec over GRE using IPsec profiles, traffic that needs to be protected should be forwarded through the tunnel interface by matching a routing entries with the remote tunnel interface as next hop in the routing table. Hence no ACL is needed.

#### QUESTION 376

A network administrator is configuring the following prefix list to prevent a route 172.16.0.0/16 from entering as OSPF route in the routing table.  
ip prefix-list OFFICE seq 5 deny 172.16.0.0/16.

Which two additional configuration commands must be required? (Choose Two)

- A. Under OSPF process, distribute-list prefix OFFICE in
- B. ip prefix-list OFFICE seq 10 permit 0.0.0.0/0 ge 32
- C. ip prefix-list OFFICE seq 10 permit 0.0.0.0/0 le 32
- D. Under OSPF process, distribute-list OFFICE out
- E. Under OSPF process, distribute-list OFFICE in

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

You need to use "in" to prevent OSPF route from entering into local routing table.  
To use a prefix list instead of access list, you must specify the keyword "prefix"

#### QUESTION 377

What are the two benefits of YANG? (Choose Two)

- A. It enforces the use of a specific encoding format for NETCONF.
- B. It collects statistical constraint analysis information.
- C. It enables multiple leaf statements to exist within a leaf list.
- D. It enforces configuration constraints.
- E. It enforces configuration semantics.

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Yang model is protocol independent and can be converted into any encoding format, e.g. XML or JSON, for use by the network configuration protocol.

YANG constraints are used to automate the validation of complicated system configuration. All YANG constraints must be validated before a configuration change can take effect.

#### QUESTION 378

Where is radio resource management performed in Cisco SD-Access wireless solution?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

# SD-Access Wireless Architecture

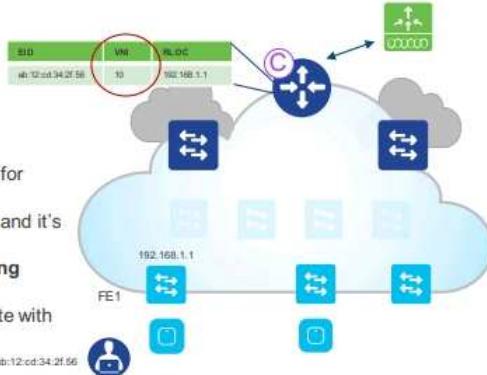
1

## Control Plane Node – A Closer Look

### Fabric Mode WLC integrates with the LISP Control Plane

Control Plane is centralized at the WLC for all Wireless functions

- WLC is still responsible for: AP image/config, Radio Resource Management (RRM) and client session management and roaming
- For Fabric integration:
  - For wireless, client **MAC address is used as EID**.
  - Interacts with the Host Tracking DB on Control-Plane node for **Client MAC address registration** with SGT and L2 VNI
  - The VN information is a **Layer 2 VN (L2 VNI)** information and it's mapped to a VLAN on the FEs
  - Responsible for updating the Host Tracking DB with **roaming** information for wireless clients
  - Fabric enabled WLC needs to be co-located at the same site with APs (latency between AP and WLC needs to be < 20 ms)



#### QUESTION 379

What does the LAP send when multiple WLCs respond to the CISCO\_CAPWAP-CONTROLLER.localdomain hostname during the CAPWAP discovery and join process?

- broadcast discover request
- join request to all the WLCs
- Unicast discovery request to the first WLS that resolves the domain name
- unicast discovery request to each WLC

**Correct Answer:** D

**Section:** Selected

**Explanation**

#### Explanation/Reference:

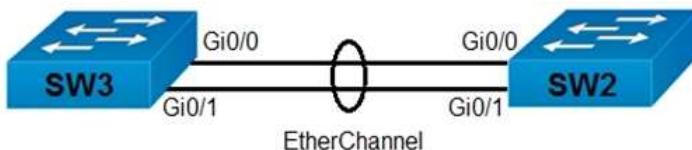
The AP will attempt to resolve the DNS name CISCO-CAPWAP-CONTROLLER.localdomain. When the AP is able to resolve this name to one or more IP addresses, the AP sends a unicast CAPWAP Discovery Message to the resolved IP address(es). Each WLC that receives the CAPWAP Discovery Request Message replies with a unicast CAPWAP Discovery Response to the AP.

After that, LAP will join one of the controllers based on:

- any previous primary, secondary and tertiary settings.
- master controller
- based on the excess capacity in the Discovery Response from each controller.
- the first controller that responded.

#### QUESTION 380

Refer to the exhibit.



```
SW2# show ip interface brief | include Port
Port-channel1 unassigned YES unset down down
```

```

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

Group Port-channel Protocol Ports
-----+-----+-----+
1    Po1(SD)        PAgP     Gi0/0(I) Gi0/1(I)

```

```

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

Group Port-channel Protocol Ports
-----+-----+-----+
1    Po1(SD)        LACP     Gi0/0(I) Gi0/1(I)

```

Which action resolves the EtherChannel issue between SW2 and SW3?

- A. Configure switchport mode trunk on SW2
- B. Configure switchport nonegotiate on SW3
- C. Configure channel-group 5 mode desirable on both interfaces
- D. Configure channel-group 1 mode active on both interfaces

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Although there is one more show output, this question is the same as Q 260.

Unless the ports in both switches are configured to form unconditionally (no such choice in the answer), either LACP or PAgP negotiation is required to form EtherChannel properly.

Both C and D can be correct and form the EtherChannel required but:

- D is better if you want to keep the original Port Channel number "1" can be kept. However, for the switch that involves the change of negotiation protocol (i.e. Sw2 from PAgP to LACP), you need to remove the Port Channel first (i.e. "no int Po1"). Moreover you also need to remove the port from channel group 1 first or the ports will be shutdown and you need to no shut them after the removal of Port Channel 1.

- C is better if you want to use the least commands since there is no change of negotiation protocol required on an existing Port Channel interface.

Remarks: The following shows the fields in the output for "sh int brief" for your reference:

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	NVRAM	administratively down	down

#### QUESTION 381

Which characteristic distinguishes Ansible from Chef?

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

**Correct Answer:** D

**Section:** (none)

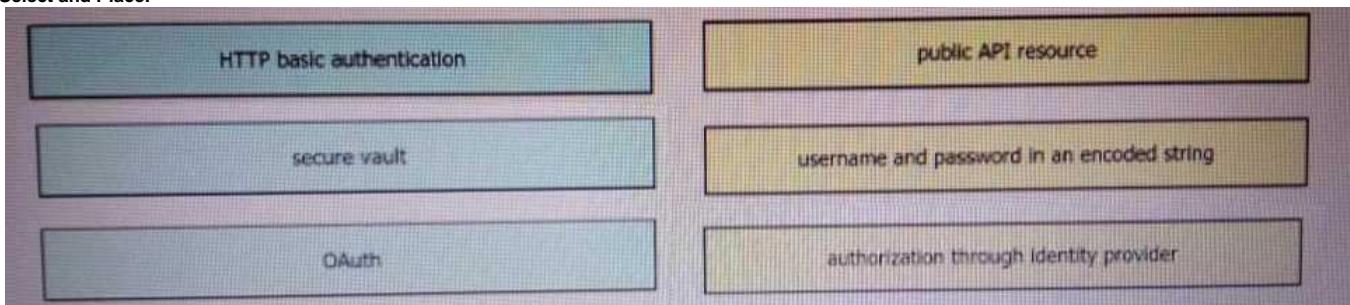
**Explanation**

**Explanation/Reference:**

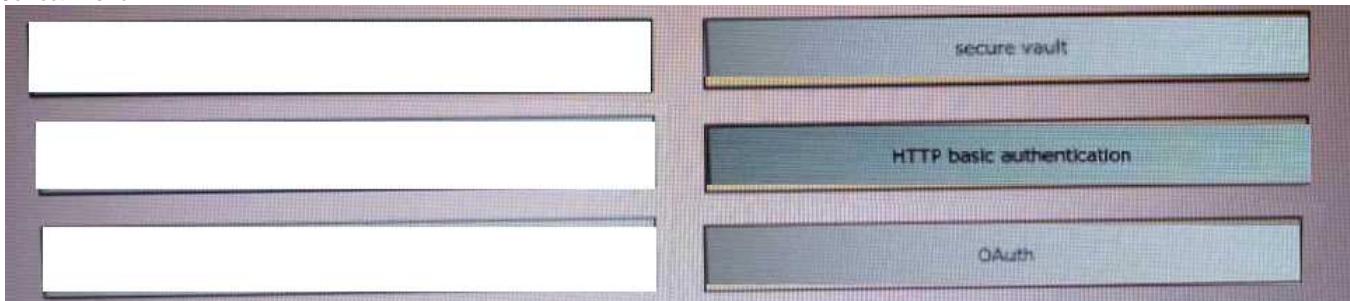
**QUESTION 382**

Drag and drop the REST API authentication method from the left to the description on the right.

**Select and Place:**



**Correct Answer:**



**Section: Selected Explanation**

**Explanation/Reference:**

**QUESTION 383**

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

---

```
SW1# show run interface
gigabitethernet 0/0
Building configuration...
Current configuration : 189 bytes
!
interface GigabitEthernet0/0
switchport trunk encapsulation isl
switchport mode access
switchport nonegotiate
channel-group 1 mode active
end

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

---

```
SW1# show run interface
gigabitethernet 0/1
Building configuration...
Current configuration : 189 bytes
!
interface GigabitEthernet0/1
switchport trunk encapsulation isl
switchport mode trunk
switchport nonegotiate
channel-group 1 mode active
end

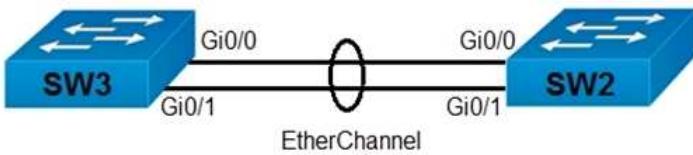
SW2# show run interface
gigabitethernet 0/0
Building configuration...
Current configuration : 189 bytes
!
interface GigabitEthernet0/0
switchport trunk encapsulation isl
switchport mode access
switchport nonegotiate
channel-group 1 mode active
end

SW2# show run interface
gigabitethernet 0/1
Building configuration...
Current configuration : 189 bytes
!
interface GigabitEthernet0/1
switchport trunk encapsulation isl
switchport mode trunk
switchport noneegotiate
channel-group 1 mode active
end

SW3# show run interface
gigabitethernet 0/0
Building configuration...
Current configuration : 151 bytes
!
interface GigabitEthernet0/0
switchport trunk encapsulation isl
switchport mode trunk
switchport noneegotiate
channel-group 1 mode passive
end

SW3# show run interface
gigabitethernet 0/1
Building configuration...
Current configuration : 151 bytes
!
interface GigabitEthernet0/1
switchport trunk encapsulation isl
switchport mode trunk
switchport noneegotiate
channel-group 1 mode passive
end
```

Remarks :missing top part of the above exhibit should be similar as follows:



Refer to the exhibit. The EtherChannel between Sw3 and Sw2 is not operational. Which action resolves the issue?

- Configure the channel-group mode on Sw3 g0/0 and g0/1 to active
- Configure the mode on Sw2 g0/0 to trunk
- Configure the mode on Sw2 g0/1 to access
- Configure the channel-group mode on Sw2 g0/0 and g0/1 to on

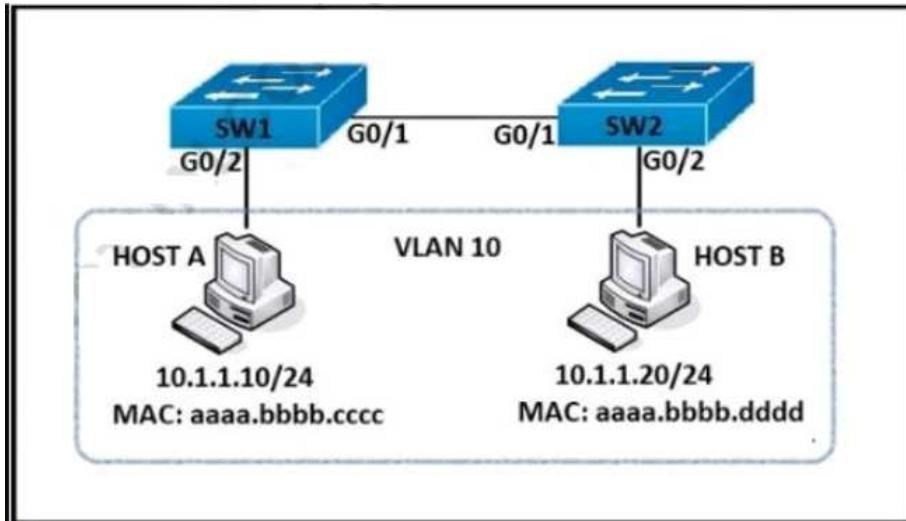
**Correct Answer: B**  
**Section: (none)**

## Explanation

Explanation/Reference:

### QUESTION 384

Refer to the exhibit.



An engineer must deny HTTP traffic from host A to host B while allowing all other communication between the hosts. Drag and drop the commands to achieve this result. (A command can be used more than once and not all commands are used.)

Select and Place:

```
SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)# permit tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# ip access-list extended MATCH_ALL
SW1(config-ext-nacl)# permit ip any any

SW1(config)# vlan access-map HOST-A-B 10
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)#
SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address MATCH_ALL
SW1(config-access-map)#

SW1(config)# vlan filter HOST-A-B vlan 10
```

action drop    action forward    filter    permit    deny    match

Correct Answer:

```
SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)# permit tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# ip access-list extended MATCH_ALL
SW1(config-ext-nacl)# permit ip any any

SW1(config)# vlan access-map HOST-A-B 10
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)#
action drop
SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address MATCH_ALL
SW1(config-access-map)#
action forward

SW1(config)# vlan filter HOST-A-B vlan 10
```

action drop    action forward    filter    permit    deny    match

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 385**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 386**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The Link Management Protocol (LMP) is activated on each link of the StackWise Virtual link as soon as it is brought up online. The LMP is used for exchanging hello for health monitoring and can rejects any unidirectional links.

**QUESTION 387**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 388**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

$\text{SNR} = (-75) - (-90) = 15$ .

**QUESTION 389**

What is the differences between TCAM and the MAC address table? (Choose Four)

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

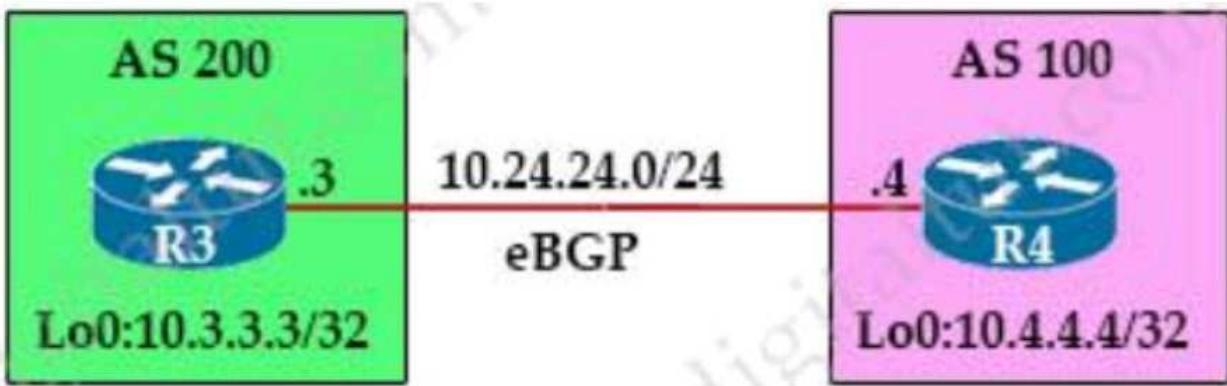
**Correct Answer:** DEGH

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 390**



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

- A. R3(config)#router bgp 200  
R3(config-router)#neighbor 10.24.24.4 remote-as 100  
R3(config-router)#bgp router-id 10.3.3.3  
R4(config)#router bgp 100  
R4(config-router)#neighbor 10.24.24.3 remote-as 200  
R4(config-router)#bgp router-id 10.4.4.4
- B. R3(config)#router bgp 200  
R3(config-router)#neighbor 10.4.4.4 remote-as 100  
R3(config-router)#neighbor 10.4.4.4 update-source loopback0  
R4(config)#router bgp 100  
R4(config-router)#neighbor 10.3.3.3 remote-as 200  
R4(config-router)#neighbor 10.3.3.3 update-source loopback0
- C. R3(config)#router bgp 200  
R3(config-router)#neighbor 10.24.24.4 remote-as 100  
R3(config-router)#neighbor 10.24.24.4 update-source loopback0  
R4(config)#router bgp 100  
R4(config-router)#neighbor 10.24.24.3 remote-as 200  
R4(config-router)#neighbor 10.24.24.3 update-source loopback0
- D. R3(config)#router bgp 200  
R3(config-router)#neighbor 10.4.4.4 remote-as 100  
R3(config-router)#bgp router-id 10.3.3.3  
R4(config)#router bgp 100  
R4(config-router)#neighbor 10.3.3.3 remote-as 200  
R4(config-router)#bgp router-id 10.4.4.4

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Note that the question just asks to use loopback as Router ID. Not forming neighbor with loopback.  
Moreover, the choices with commands for forming neighbor with loopback are wrong since `ebgp-multihop` has not been included.

**QUESTION 391**

How does the EIGRP metric differ from the OSPF metric?

- A. The EIGRP metric is calculated based on bandwidth only. The OSPF metric is calculated on delay only.
- B. The EIGRP metric is calculated based on delay only. The OSPF metric is calculated on bandwidth and delay.
- C. The EIGRP metric is calculated based on bandwidth and delay. The OSPF metric is calculated on bandwidth only.
- D. The EIGRP metric is calculated based on hop count and bandwidth. The OSPF metric is calculated on bandwidth and delay.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 392**

```

Current configuration : 192 bytes
!
interface FastEthernet0/0
 ip address 192.168.3.5 255.255.255.0
 duplex full
 vrrp 1 ip 192.168.3.1
 vrrp 1 priority 110
 vrrp 1 authentication text cisco
 vrrp 1 track 20 decrement 20
end

R1#show running-config | include track 20
track 20 ip route 10.10.1.1 255.255.255.0 reachability

R2#show running-config interface fa0/0
building configuration...
Current configuration : 141 bytes
!
interface FastEthernet0/0
 ip address 192.168.3.2 255.255.255.0
 duplex full
 vrrp 1 ip 192.168.3.1
 vrrp 1 authentication text cisco
end

```

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

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

**Correct Answer:** D

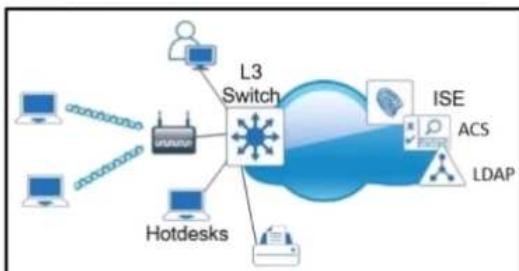
**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since preempt is enabled by default in VRRP, R1 will be master after it recovers.

#### QUESTION 393



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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 394

```

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

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

R1#debug ip icmp
ICMP packet debugging is on

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

```

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

B and D is wrong since the issue should be related to MTU.

C is rational but actually it is NOT the cause of the issue. It is a workaround to solve the issue.

A is therefore the only possible cause although there is no no evident about PMTUD and/or ACL has been implemented.

#### QUESTION 395

```

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

```

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Note that not all IOS versions support "aaa common-criteria policy"

#### QUESTION 396

```

flow record Recorder
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
!
flow exporter Exporter
  destination 192.168.100.22
  transport udp 2055
!
flow monitor Monitor
  exporter Exporter
  record Recorder
!
et-analytics
  ip flow-export destination 192.168.100.22 2055
!
interface g1
  ip flow monitor Monitor input
  ip flow monitor Monitor output
  et-analytics enable
!
```

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

## option (Flexible NetFlow)

To configure options data parameters for a Flexible NetFlow flow exporter, use the **option** command in Flexible NetFlow flow exporter configuration mode. To remove options for a Flexible NetFlow flow exporter, use the **no** form of this command.

**option {application-table | exporter-stats | interface-table | sampler-table | vrf-table} [timeout seconds]**

**no option {application-table | exporter-stats | interface-table | sampler-table | vrf-table}**

**Syntax Description**

<b>application-table</b>	Configures the application table option for flow exporters.
<b>exporter-stats</b>	Configures the exporter statistics option for flow exporters.
<b>interface-table</b>	Configures the interface table option for flow exporters.
<b>sampler-table</b>	Configures the export sampler information option for flow exporters.
<b>vrf-table</b>	Configures the virtual routing and forwarding (VRF) ID-to-name table option for flow exporters.
<b>timeout seconds</b>	(Optional) Configures the option resend time in seconds for flow exporters. Range: 1 to 86400. Default 600.

The following example causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

```

Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# option interface-table
```

### QUESTION 397

Which AP mode detects a malicious AP?

- A. Sniffer
- B. Detect
- C. Local
- D. Autonomous

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:****Local**

This is the normal operation of an AP. This mode allows data clients to be serviced while configured channels are scanned for noise and rogues. In this mode of operation, **the AP goes off-channel for 50 ms and listens for rogues**. It cycles through each channel, one at a time, for the period specified under the Auto RF configuration.

**Monitor**

This is radio receive only mode, and allows the AP to scan all configured channels every 12 seconds. Only de-authentication packets are sent in the air with an AP configured this way. **A monitor mode AP can detect rogues**, but it cannot connect to a suspicious rogue as a client in order to send the RLDP packets.

**QUESTION 398**

Drag and drop the Qos mechanisms from the left to the correct descriptions on the right.

**Select and Place:**

shaping	bandwidth management technique which delays datagrams
policing	tool to enforce rate limiting on ingress/egress
Cos	portion of the 802.1Q header used to classify packets

**Correct Answer:**

	shaping
	policing
	Cos

**Section: (none)****Explanation****Explanation/Reference:****QUESTION 399**

Drag and drop the characteristics from the left to the correct Infrastructure deployment type on the right.

Which of the followings are the characteristics of Cloud (Choose 3)?

- A. significant initial investment but lower recurring costs
- B. pay-as-you-go-model
- C. physical location of data can be defined in contract with provider
- D. very scalable and fast delivery of changes in scale
- E. company has control over the physical security of equipment

**Correct Answer: BCD****Section: (none)****Explanation****Explanation/Reference:**

	<b>On-premises</b>
	significant initial investment but lower reoccurring costs
	company has control over the physical security of equipment
	<b>Cloud</b>
	pay-as-you-go model
	physical location of data can be defined in contract with provider
	very scalable and fast delivery of changes in scale

**QUESTION 400**

```

DSW2#sh spanning-tree vlan 10

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

  Bridge ID Priority  4106  (priority 4096 sys-id-ext 10)
  Address  0018.7363.4300
  Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time 300

Interface      Role Sts Cost      Prio.Nbr Type
-----+-----+-----+-----+-----+
Fa1/0/7        Root FWD 2       128.9    P2p
Fa1/0/10       Desg FWD 4       128.12   P2p
Fa1/0/11       Desg FWD 2       128.13   P2p
Fa1/0/12       Desg FWD 2       128.14   P2p

DSW2#
*Mar 3 07:19:24.654: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa1/0/7
with BPDU Guard enabled. Disabling port.
*Mar 3 07:19:24.654: %PM-4-ERR_DISABLE: bpduguard error detected on Fa1/0/7, putting Fa1/0/7 in err-disable state
*Mar 3 07:19:24.679: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa1/0/7
with BPDU Guard enabled. Disabling port.
*Mar 3 07:19:25.889: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtherne
t1/0/7, changed state to down
*Mar 3 07:19:26.884: %LINE-3-UPDOWN: Interface FastEthernet1/0/7, changed state
to down

```

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

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

**Correct Answer:** A

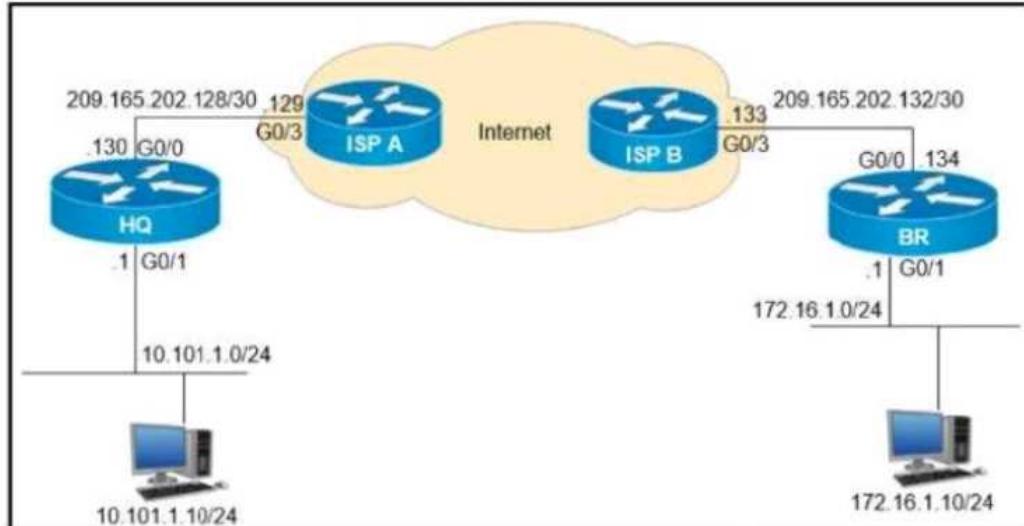
**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 401

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



- > Frame 24: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
- > Ethernet II, Src: 50:00:00:01:00:01 (50:00:00:01:00:01), Dst: 50:00:00:02:00:01 (50:00:00:02:00:01)
- > Internet Protocol Version 4, Src: 209.165.202.130, Dst: 209.165.202.134
- > Generic Routing Encapsulation (IP)
- > Internet Protocol Version 4, Src: 10.101.1.111.1, Dst: 10.101.1.111.2
- > Internet Control Message Protocol

- A. 10.111.111.1
- B. 10.111.111.2
- C. 209.165.202.103
- D. 209.165.202.134

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 402**

```
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#
```

Refer to the exhibit. Which command must be applied to Router1 to bring the GRE tunnel to an up/up state?

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

**Correct Answer: D**

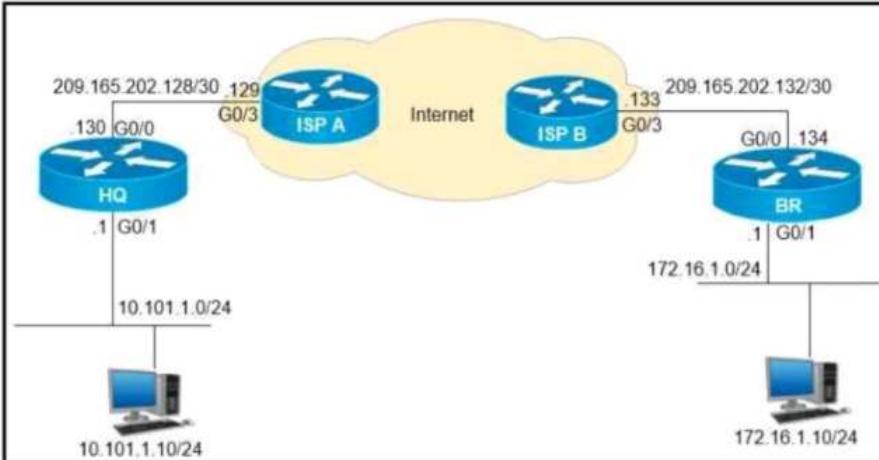
**Section: (none)**

**Explanation**

**Explanation/Reference:**

Tunnel source is missing. Note that g0/1 cannot be used as tunnel source since it is shut down and has no IP address.

**QUESTION 403**



Refer to the exhibit. Which configuration must be applied to the HQ router to set up a GRE tunnel between the HQ and BR routers?

- A. interface Tunnel1  
ip address 209.165.202.130 255.255.255.252  
tunnel source GigabitEthernet0/0  
tunnel destination 209.165.202.129
- B. interface Tunnel1  
ip address 10.111.111.1 255.255.255.0  
tunnel source GigabitEthernet0/0  
tunnel destination 209.165.202.133
- C. interface Tunnel1  
ip address 10.111.111.1 255.255.255.0  
tunnel source GigabitEthernet0/0  
tunnel destination 209.165.202.129
- D. interface Tunnel1  
ip address 10.111.111.1 255.255.255.0  
tunnel source GigabitEthernet0/0  
tunnel destination 209.165.202.134

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 404**

Which outcome is achieved with this Python code?

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 405**

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

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

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 406**

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 407**

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

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

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

- A. configure option 43 Hex F104.AC10.3205
- B. configure option 43 Hex F104.CA10.3205
- C. configure dns-server 172.16.50.5
- D. configure dns-server 172.16.100.1

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Depending on the AP model, one of the following can be configured:

```
option 43 hex f104.ac10.3205
option 43 ascii 172.16.50.5
```

Note that in the incorrect answer B, CA in hexidecimal means 202

**QUESTION 408**

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

Which three commands are required? (Choose three.)

- A. standby 300 timers 1 110
- B. standby 300 priority 90

- C. standby 300 priority 110
- D. standby version 2
- E. standby 300 preempt
- F. standby version 1

**Correct Answer:** CDE

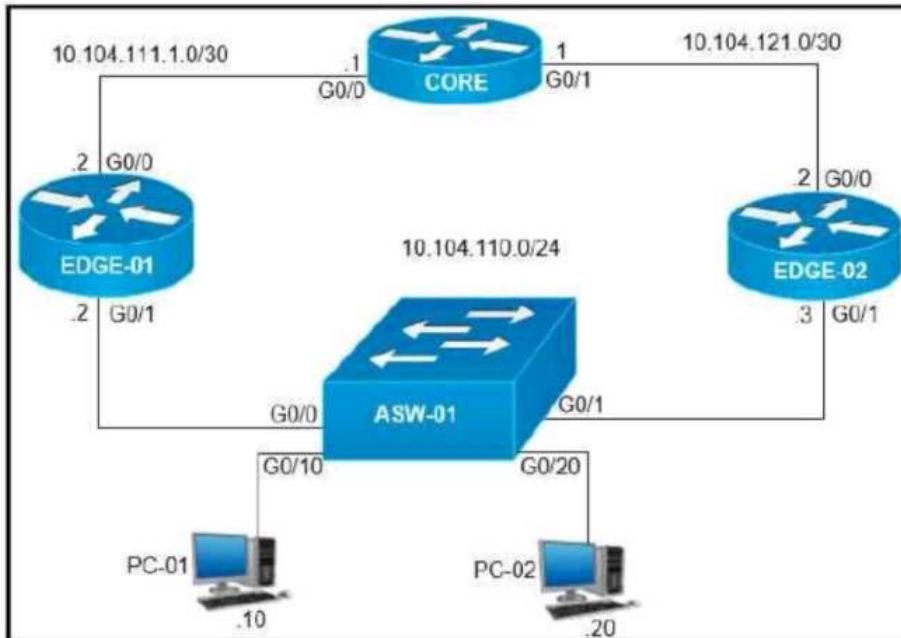
**Section:** (none)

**Explanation**

**Explanation/Reference:**

HSRP version 2 is required since HSRPv1 only supports group number 0 - 255.

#### QUESTION 409



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

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

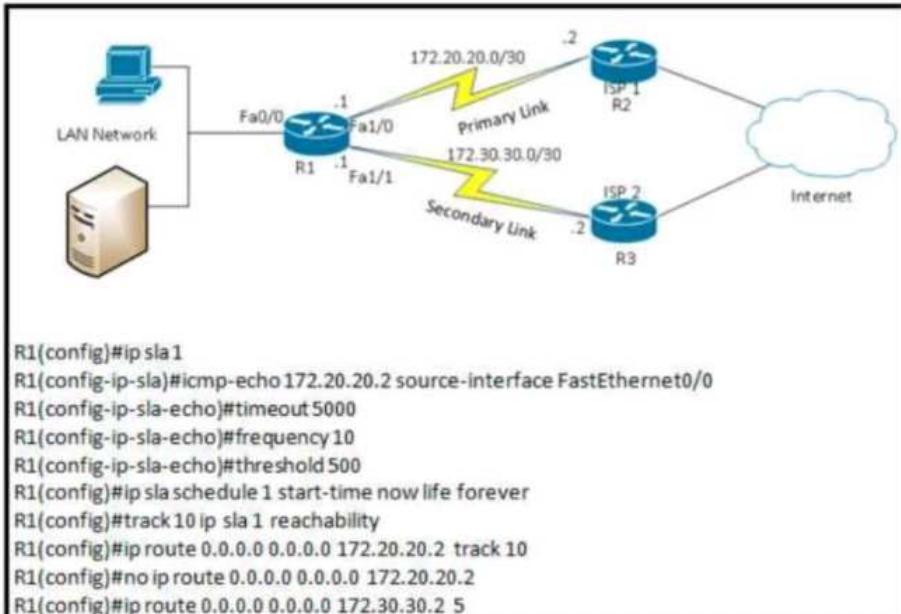
**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 410



Refer to exhibit. What are two reasons for IP SLA tracking failure? (Choose two)

- A. The destination must be 172.30 30 2 for icmp-echo
- B. The threshold value is wrong
- C. A route back to the R1 LAN network is missing in R2
- D. The source-interface is configured incorrectly.
- E. The default route has the wrong next hop IP address

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

D is the answer since the source interface should be f1/0.

Since A, B and E are wrong answers, only answer left is C. However the question shows no information about R2's settings.

Note that in the 2nd last command, it removes a previous default route that do not have track object configured. The command will not remove the default route with track object configured in 3rd last command.

**QUESTION 411**

```
aaa new-model
aaa authentication login local tacacs+
tacacs-server host 10.1.1.1
tacacs-server key CISCO
!
line con 0
login authentication local
line aux 0
line vty 0 4
!
username tommy password 0 Cisco
end
```

### TACACS+ Server Passwords

**username tommy password 0 Tommy**

Refer to the exhibit. Which password allows access to line con 0 for a username of "tommy" under normal operation?

- A. Cisco
- B. local
- C. 0 Cisco
- D. Tommy

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The AAA authentication name is local (you must specify a list name or "default") before specifying the authentication method (which is tacacs+ in the above case). Hence "local" above is actually a list name.

```
Router(config)#aaa authentication login ?
WORD      Named authentication list (max 31 characters, longer will be
           rejected).
default   The default authentication list.

Router(config)#aaa authentication login local ?
cache     Use Cached-group
enable    Use enable password for authentication.
group     Use Server-group
krb5     Use Kerberos 5 authentication.
krb5-telnet  Allow logins only if already authenticated via Kerberos V
              Telnet.
line      Use line password for authentication.
local     Use local username authentication.
local-case Use case-sensitive local username authentication.
none      NO authentication.
passwd-expiry enable the login list to provide password aging support
```

The "0" in the username command means the following is a clear text password. Therefore "0" is optional.

**QUESTION 412**

In a traditional 3 tier topology, an engineer must explicitly configure a switch as the root bridge and exclude it from any further election process for the spanning-tree domain. Which action accomplishes this task?

- A. Configure the spanning-tree priority to 32768
- B. Configure root guard and portfast on all access switch ports.
- C. Configure BPDU guard in all switch-to-switch connections.
- D. Configure the spanning-tree priority equal to 0.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since 0 is the smallest value that can be configured for bridge priority, the switch will be the root bridge without any further election.

**QUESTION 413**

Why would a log file contain a "\*" next to the date?

- A. The network device was receiving NTP time when the log messages were recorded
- B. The network device was unable to reach the NTP server when the log messages were recorded.
- C. The network device is not configured to use NTP
- D. The network device is not configured to use NTP time stamps for logging.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

For B, it can be correct. However it is not chosen since NTP has probably been unreachable before the log messages were recorded. Therefore C seems to be a better answer.

**QUESTION 414**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 415**

```
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?

- A. access-list 23 permit 10.10.10.0 0.0.0.255
 line vty 0 4
 access-class 23 in
 transport input ssh
- B. access-list 23 permit 10.10.10.0 0.0.0.255
 line vty 0 15
 access-class 23 in
 transport input ssh
- C. access-list 23 permit 10.10.10.0 0.0.0.255
 line vty 0 15
 access-class 23 out
 transport input all
- D. access-list 23 permit 10.10.10.0 255.0.0.0
 line vty 0 15
 access-class 23 in
 transport input ssh

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since 16 vty lines are defined, you must apply the settings to all of them.

**QUESTION 416**

Refer to the exhibit.



**Configuration in London router:**

```
London(config)#int range f0/1-2
London(config-if-range)#switchport trunk encapsulation dot1q
London(config-if-range)#switchport mode trunk
London(config-if-range)#channel-group 1 mode active
```

**Output for EtherChannel summary in NewYork router::**

```
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
W - unsuitable for bundling
W - waiting to be aggregated
d - default port
Number of channel-groups in user: 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 = 2
SC = 0x00000000 HotStandBy port = null
Port state = Port-channel |
Protocol = PAgP
Port Security = Disabled
```

Communication between London and New York is down. What commands should be configured in NewYork router to solve the issue?

- A. no int po1
   
 int range g0/0-1
   
 channel-group 1 mode passive
- B. no int po1
   
 int range g0/0-1
   
 channel-group 1 mode on
- C. no int po1
   
 int range g0/0-1
   
 channel-group 1 mode negotiate
- D. no int po1
   
 int range g0/0-1
   
 channel-group 1 mode auto

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Problem occur since London is configured with "mode active" (LCAP) but New York router is showing the use of "PaGP". Hence, you need to configure NewYork router to use "mode active" or "mode passive".

**QUESTION 417**

Which QOS setup has 4 static queues?

- A. LLQ
- B. Custom
- C. Weighted Fair Queue
- D. Priority

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Priorty Queue (PQ) and Custom Queue (CQ) are the old ways of configuring queueing in a Cisco router. For packets meeting a classification, only queueing can be provided.

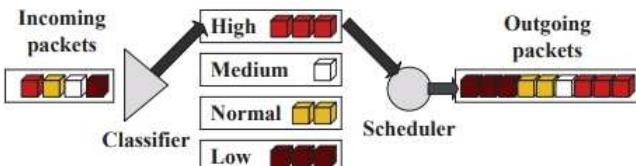


Figure 3. PQ.

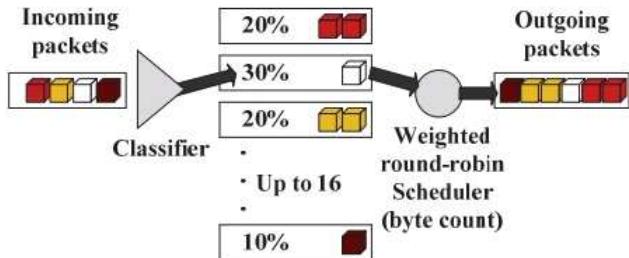


Figure 5. CQ.

CBWFQ and LLQ is the newer way to configure QoS. For packets matching a class, other assigning to different queues just like PQ or CQ, you can also configure shaping, policing, WRED .... etc configured for the traffic of those packets under the corresponding class map.

Feature	FIFO	PQ	CQ	WFQ	CBWFQ	LLQ
Includes a strict-priority queue		Yes				Yes
Polices priority queues to prevent starvation						Yes
Reserves bandwidth per queue			Yes		Yes	Yes
Includes robust set of classification fields					Yes	Yes
Classifies based on flows				Yes	Yes <sup>2</sup>	Yes <sup>2</sup>
Maximum number of queues	1	4	16 <sup>1</sup>	4096	64	64

**QUESTION 418**

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

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

**Correct Answer:** CD

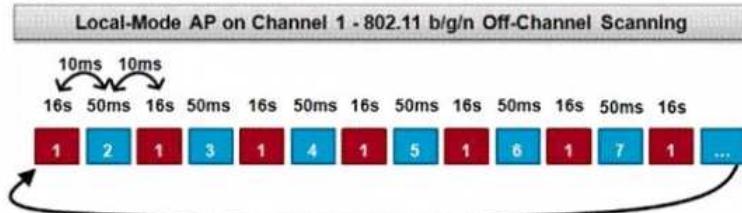
## **Section: Selected**

## Explanation

### **Explanation/Reference:**

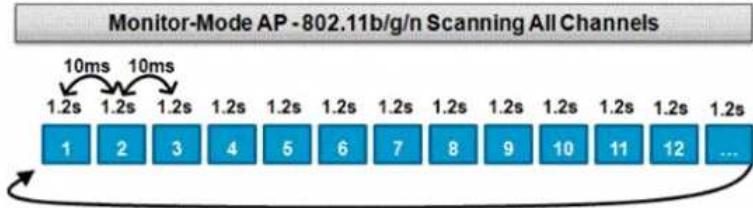
## Off-Channel Scanning

This operation is performed by **Local and Flex-Connect** (in connected mode) mode APs and utilizes a time-slicing technique which allows client service and channel scanning with the usage of the same radio. With the move to off channel for a period of 50ms every 16 seconds, the AP, by default, only spends a small percentage of its time to not serve clients.



## **Monitor Mode Scanning**

This operation is performed by Monitor Mode and Adaptive wIPS monitor mode APs which utilizes 100% of the radio's time for scanning all channels in each respective frequency band. This allows a greater speed of detection and enables more time to be spent on each individual channel. **Although monitor mode also scan for rogue AP, the APs cannot serve normal wireless clients.**



#### QUESTION 419

##### Script

```
import ncclient

with ncclient.manager.connect(host='192.168.1.1', port=830, username='root', password='test123!',
    allow_agent=False) as m:
    print(m.get_config('running').data_xml)
```

##### Output

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

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

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

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Note that using the answer "from ncclient import manager" to replace the first statement in the script, you also need to change the calling of connect function to "manager.connect(...)"

Remarks:

Another alternative way is without changing the calling of the connection function is to change the import statement to "import ncclient.manager"

For reference only:

In Python, both "import ncclient" or "from ncclient import \*" can be a valid way to perform the import of modules of ncclient only if special settings are added to the file "\_\_init\_\_.py" under the folder "ncclient".

However, in a standard "ncclient" package, the "\_\_init\_\_.py" under "ncclient" does NOT have such special settings included. You can either use a modified version of "ncclient" or perform the required modification manually. Then you can use the syntax as shown in this question without this error.

#### QUESTION 420

```
def get_token():
    device_url = "https://192.168.1.1/dna/system/api/v1/auth/token"
    http_result = requests.post(device_url, auth = ("test", "test399079338!"))
    if http_result.status_code != requests.codes.ok:
        print ("Call failed! Review get_token () . ")
        sys.exit ()
    return (http_result.json () ["Token"] )
```

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The script checks the status code. It will exit if the status code is not OK (HTTP code 200). Therefore the script will not exit if HTTP code 200 is received.

#### QUESTION 421

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The underlay network is defined by the physical switches and routers that are used to deploy the SD-Access network. All network elements of the underlay must establish IP connectivity via the use of a routing protocol. Instead of using arbitrary network topologies and protocols, the underlay implementation for SD-Access uses a well-designed Layer 3 foundation inclusive of the campus edge switches which is known as a Layer 3 Routed Access design. This ensures performance, scalability, and resiliency, and deterministic convergence of the network.

**In SD-Access, the underlay switches (edge nodes) support the physical connectivity for users and endpoints. However, end-user subnets and endpoints are not part of the underlay network—they are part of the automated overlay network.**

**QUESTION 422**

An administrator needs to configure a rule that permits packets that have ACK in the TCP header. Which of the following entry should be used?

- A. access-list 1 permit tcp any any established
- B. access-list 1 permit tcp any any tcp-ack
- C. access-list 100 permit tcp any any tcp-ack
- D. access-list 100 permit tcp any any established

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

A and B must be wrong since 1 is a standard access list which can only specify condition for source address.

There is a keyword "ack" for matching packets with ACK flag. However since C is using the wrong keyword "tcp-ack".

Only D is the answer since "established" matches for either ACK or RST.

**QUESTION 423**

```
password = base64.b64decode(pass).decode("UTF-8")
d = datetime.date.today()
date = str(1000*d.year + 100*d.month + d.day)
```

What does the above Python code perform?

- A. The code converts time to the yyymmdd format.
- B. The code converts time to Epoch Unix time
- C. The code converts time to year/month/day format
- D. The code encrypts a base64 decrypted password

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

The first line decodes the base64 bytes stored in "pass" into bytes and then into UTF-8 string. Therefore no encryption is involved.

**QUESTION 424**

What is centralized control policy in SD-WAN?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The default behavior of the controller is to advertise all routes (omp, tloc, and service) which results in a full mesh overlay fabric and any-to-any IP reachability. However, in most cases, this is not the desired network outcome that companies require. Therefore, in most scenarios, the network topology should be customized and the IP reachability must follow the company's policy.

**When we want to control the route information that is stored in the controllers' route tables or the route information that is advertised to vEdges, we provision a Centralized Control Policy.**

When such a policy is applied, the behavior of the controllers change as follows:

- When a Centralized Control Policy is applied in an inbound direction, it filters or modifies the route information that is coming from vEdges before it is placed in the controller's routing table.
- When a Centralized Control Policy is applied in an outbound direction, it filters or modifies the route information that is advertised to vEdges.

**QUESTION 425**

What are two characteristics of VXLAN? (Choose two)

- A. It uses VTEPs to encapsulate and decapsulate frames.
- B. It allows up to 16 million VXLAN segments
- C. It extends Layer 2 and Layer 3 overlay networks over a Layer 2 underlay.

- D. It has a 12-bit network identifier
- E. It lacks support for host mobility

**Correct Answer:** AB

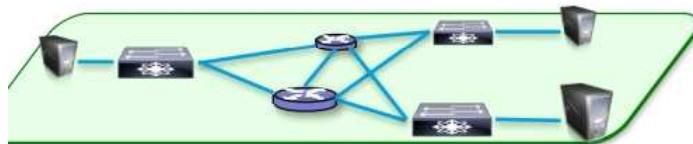
**Section:** (none)

**Explanation**

**Explanation/Reference:**

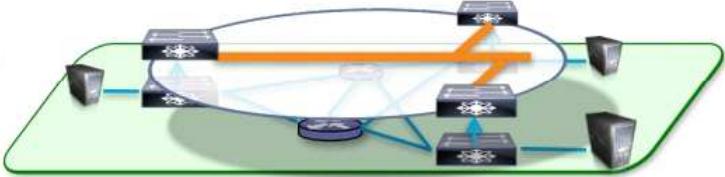
VXLAN is a technology which allows overlaying a **Layer 2 (L2) network over a Layer 3 (L3) underlay** with use of any IP routing protocol. It uses MAC-in-UDP Encapsulation.

VXLAN extends the L2 Segment ID field to 24-bits, which potentially allows up to 16 million unique L2 segments over the same network.



**Robust Underlay/Fabric**

- High Capacity Resilient Fabric
- Intelligent Packet Handling
- Programmable & Manageable



**Flexible Overlay Virtual Network**

- Mobility – Track end-point attach at edges
- Segmentation
- Scale – Reduce core state
  - Distribute and partition state to network edge
- Flexibility/Programmability
  - Reduced number of touch points

#### QUESTION 426

Which of the following can be blocked by AMP4E?

- A. ransomware
- B. SQL injection
- C. email phishing
- D. Microsoft Word macro attack
- E. DDoS

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 427

Which of the following is a reason for using external antenna within a building?

- A. When it can provide the required coverage
- B. When using 5 GHz only
- C. When using 2.4 GHz only
- D. When using Mobility Express

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 428

Which of the following is true for WLC layer 3 roaming?

- A. The original controller pass the client entry to the new controller.
- B. The original controller updates the client entry as Anchor and the new controller updates the client entry as Foreign.
- C. The new controller assigns an IP address from the new subnet to the client
- D. 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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Controllers within a mobility group communicate among themselves over a well-known UDP port and exchange data traffic through an Ethernet-over-IP (EoIP) tunnel. Therefore the tunnel is not created with the wireless client.

#### QUESTION 429

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

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

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 430**

Which of the following components allow the communication between guest VMs?

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

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 431**

Which two statements about AAA authentication are true? (Choose two)

- A. RADIUS authentication queries the router's local username database
- B. TACACS+ authentication uses an RSA server to authenticate users
- C. Local user names are case-insensitive
- D. Local authentication is maintained on the router
- E. KRB5 authentication disables user access when an incorrect password is entered

**Correct Answer:** CD  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

Unless `local-case` is used instead of `local` in the authentication list, username is case-insensitive.

The RSA server can be accessed with RADIUS or the proprietary RSA protocol: SDI. Both the ASA and the ACS can use both protocols (RADIUS, SDI) in order to access the RSA i.e. NOT TACACS+.

Some Cisco IOS versions include Kerberos 5 (KRB5) support, which allows organizations already deploying Kerberos 5 to use the same Kerberos authentication database on their routers that they are already using on their other network hosts (such as UNIX servers and PCs).

Normally, a user will be prompted again for login if an incorrect password is entered for just once or twice. Moreover, a KRB 5 server will not disable a user account if an incorrect password is entered. Disabling will only be implemented if incorrect password are entered for several times.

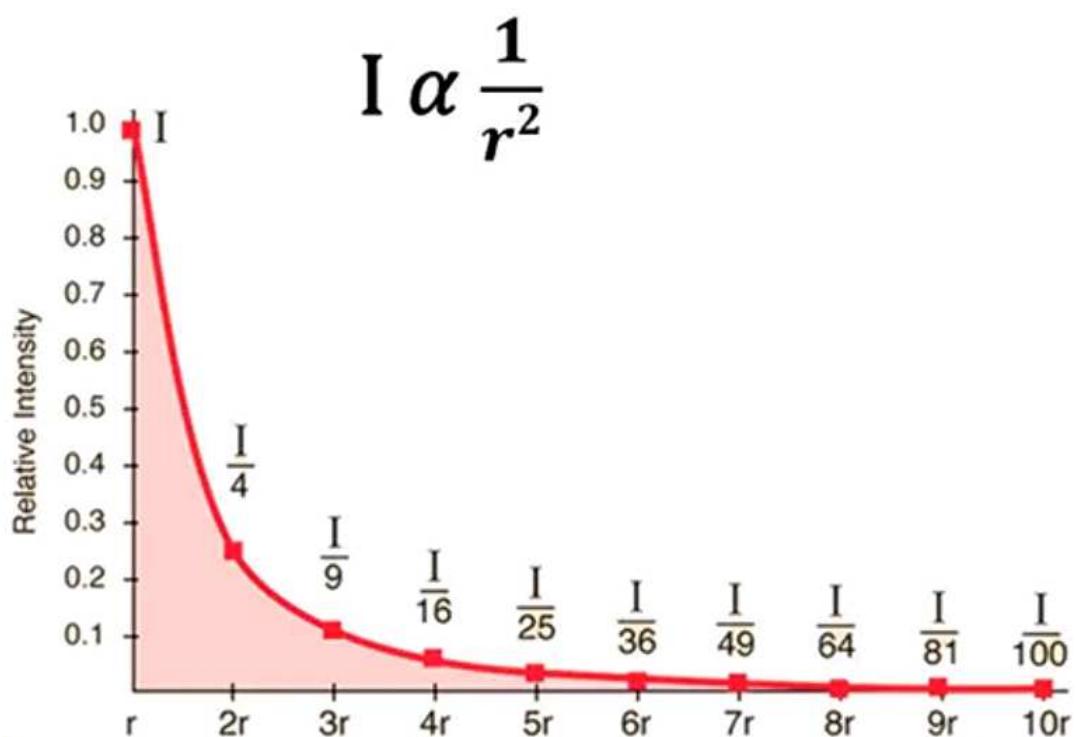
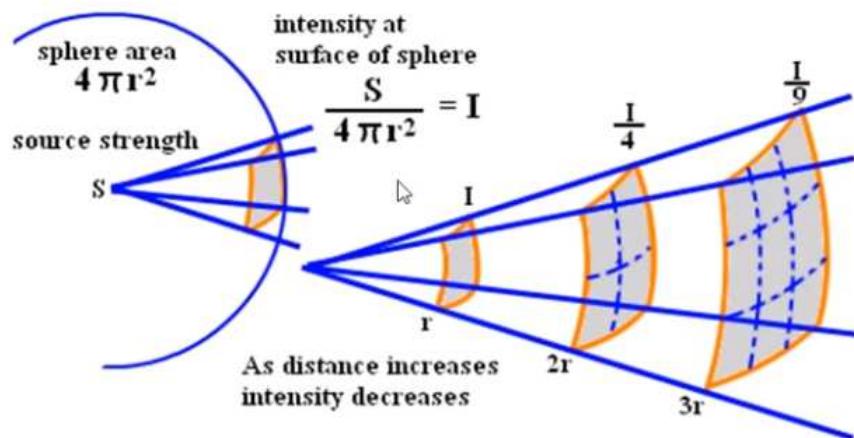
**QUESTION 432**

What happens to the signal strength of an RF signal due to wave spreading?

- A. The signal strength of the RF signal will fall off equally near the transmitter and also farther away.
- B. The signal strength at the RF signal will fall off quickly near the transmitter but more slowly farther away.
- C. The signal strength at the RF signal will fall off slowly near the receiver and more quickly farther away.
- D. The signal strength of the RF signal will fall off slowly near the transmitter but more quickly farther away.

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**



#### QUESTION 433

Drag and drop the snippets onto the blanks within the code to construct a script that advertises the network prefix 192.168.5.0/24. Not all options are used.

Select and Place:

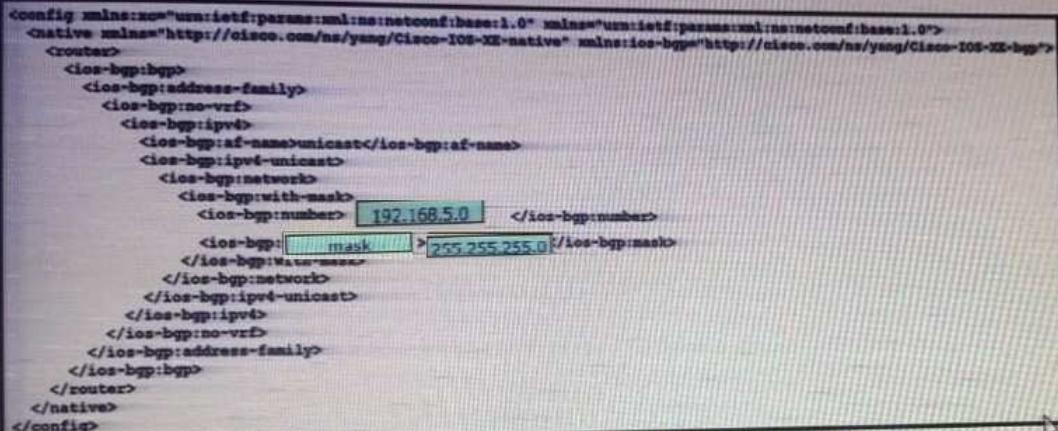
```

<config xmlns:ze="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
<router>
<ios-bgp:bgp>
<ios-bgp:address-family>
<ios-bgp:ipv4>
<ios-bgp:af-name>unicast</ios-bgp:af-name>
<ios-bgp:ip4-unicast>
<ios-bgp:network>
<ios-bgp:with-mask>
<ios-bgp:number>[ ]</ios-bgp:number>
<ios-bgp:[ ]>[ ]</ios-bgp:mask>
</ios-bgp:with-mask>
</ios-bgp:network>
<ios-bgp:ip4-unicast>
</ios-bgp:ipv4>
</ios-bgp:address-family>
</ios-bgp:bgp>
</router>
</native>
</config>

```

192.168.5.0    255.255.255.0    with-mask    mask    subnet-mask

**Correct Answer:**



```
<config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
<router>
<ios-bgp:bgp>
<ios-bgp:address-family>
<ios-bgp:no-vrf>
<ios-bgp:ipv4>
<ios-bgp:af-name>unicast</ios-bgp:af-name>
<ios-bgp:ipv4-unicast>
<ios-bgp:network>
<ios-bgp:with-mask>
<ios-bgp:number>192.168.5.0</ios-bgp:number>
<ios-bgp:>mask</ios-bgp:>255.255.255.0</ios-bgp:mask>
</ios-bgp:with-mask>
</ios-bgp:network>
</ios-bgp:ipv4-unicast>
</ios-bgp:ipv4>
</ios-bgp:no-vrf>
</ios-bgp:address-family>
</ios-bgp:bgp>
</router>
</native>
</config>
```

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The following shows a simple example of configure BGP network command for 10.10.1.0/24 with YANG.

```
<config>
<native xmlns=" http://cisco.com/ns/yang/Cisco-IOS-XE-native"; xmlns:ios-bgp=" http://cisco.com/ns/yang/Cisco-
IOS-XE-bgp">;
<router>
<ios-bgp:bgp>
<ios-bgp:id>2</ios-bgp:id>
<ios-bgp:address-family>
<ios-bgp:no-vrf>
<ios-bgp:ipv4>
<ios-bgp:af-name>unicast</ios-bgp:af-name>
<ios-bgp:network>
<ios-bgp:number>10.10.1.0</ios-bgp:number>
<ios-bgp:mask>255.255.255.0</ios-bgp:mask>
</ios-bgp:network>
</ios-bgp:ipv4>
</ios-bgp:no-vrf>
</ios-bgp:address-family>
</ios-bgp:bgp>
</router>
</native>
</config>
```

**QUESTION 434**

```
def get_credentials():
    creds={'username': 'cisco', 'password': 'c3577dc8ae4e36c0bf86fe5399079338'}
    return (creds.get('username'))

print(get_credentials())
```

What is the output of this code?

- A. cisco
- B. get\_credentials
- C. username
- D. username: cisco

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The above Python function get\_credentials() will return the value of the field 'username' in the object "creds".

**QUESTION 435**

```

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-Fal/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 messages generated on R2. What is the cause of the message?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The VIP may already be used by another HSRP group in the same network segment since ARP message about duplicated IP address is sourced by a MAC address for HSRP 0000.0c07.acXX.

#### QUESTION 436

The screenshot shows a POSTMAN API request. The method is GET, and the URL is <https://sandboxdnac.cisco.com/dna/intent/api/v1/network-devices>. The Headers tab is selected, showing an X-Auth-Token header with a long value and a Key field. The Body tab is selected, showing a JSON payload with a response object containing an errorCode of "Bad request", a message of "Invalid input request", a detail of "s is not a valid UUID of device", and a version of "1.0". The status bar at the bottom indicates a 400 Bad Request status and a time of 19ms.

```

1 - {
2 -   "response": {
3 -     "errorCode": "Bad request",
4 -     "message": "Invalid input request",
5 -     "detail": "s is not a valid UUID of device"
6 -   },
7 -   "version": "1.0"
8 -

```

Refer to the exhibit. POSTMAN is showing an attempt to retrieve network device information from Cisco DNA Center API. What is the issue?

- A. The URI string is incorrect.
- B. The token has expired.
- C. Authentication has failed
- D. The JSON payload contains the incorrect UID.

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

You can use API with the URL "/dna/intent/api/v1/network-device" to get a list of network devices from DNA center.

The error detail "s is not a valid UUID of device" is probably due to the wrong URL e.g. with an extra "s" at the end i.e. "/dna/intent/api/v1/network-devices" being used as shown in the above exhibit.

#### QUESTION 437

Drag and drop the wireless elements on the left to their definitions on the right.

**Select and Place:**

beamwidth	a graph that shows the relative intensity of the signal strength of an antenna within its space
polarization	the relative increase in signal strength of an antenna in a given direction
radiation patterns	measures the angle of an antenna pattern in which the relative signal strength is half-power below the maximum value
gain	radiated electromagnetic waves that influence the orientation of an antenna within its electromagnetic field

**Correct Answer:**

	radiation patterns
	gain
	beamwidth
	polarization

**Section: Selected Explanation**

**Explanation/Reference:**

**QUESTION 438**

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

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

**Correct Answer: B**

**Section: Selected Explanation**

**Explanation/Reference:**

**QUESTION 439**

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

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

**Correct Answer: CD**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 440**

How are the different versions of IGMP compatible?

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Actually:

IGMPv2 is backward compatible with v1.

IGMPv3 is backward compatible with v1 and v2.

B and C seems wrong since there cannot be two correct answers. May be the same version is not considered as compatible.  
D is wrong since v3 can compatible with v1 and v2.

**QUESTION 441**

```
ip vrf BLUE
rd 1:1
!
interface Vlan100
description GLOBAL_INTERFACE
ip address 10.10.1.254 255.255.255.0
!
access-list 101 permit ip 10.10.5.0 0.0.0.255 10.10.1.0
255.255.255.0
!
route-map VRF_TO_GLOBAL permit 10
match ip address 101
set global
!
interface Vlan500
description VRF_BLUE
ip vrf forwarding BLUE
ip address 10.10.5.254 255.255.255.0
ip policy route-map VRF_TO_GLOBAL
```

Refer to the exhibit. An engineer attempts to create a configuration to allow the Blue VRF to leak into the global routing table, but the configuration does not function as expected. Which action resolves this issue?

- A. Change the access-list destination mask to a wildcard.
- B. Change the source network that is specified in access-list 101
- C. Change the route-map configuration to VRF\_BLUE.
- D. Change the access-list number in the route map

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 442**

Which entity is a Type 1 hypervisor?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 443**

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

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

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**Monitor**

This is radio receive only mode, and allows the AP to scan all configured channels every 12 seconds. Only de-authentication packets are sent in the air with an AP configured this way. A monitor mode AP can detect rogues, but it cannot connect to a suspicious rogue as a client in order to send the RLDN packets.

Since the questions said "configured channels", B seems better than D.

**QUESTION 444**

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

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 445**

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

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

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Multigroup HSRP (MHSRP) simply means the configuration of multiple HSRP groups for a network segment.

In this case, one HSRP group uses virtual IP 10.0.0.1 and the other HSRP group uses virtual IP 10.0.0.2. Then some clients use 10.0.0.1 as default gateway and other clients use 10.0.0.2 as default gateway.

**QUESTION 446**

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

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

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

An Endpoint Detection and Response (EDR) solution detects threats across your environment. It investigates the entire lifecycle of the threat, providing insights into what happened, how it got in, where it has been, what it's doing now, and how to stop it. By containing the threat at the endpoint, the EDR solution helps eliminate the threat and prevent it from spreading.

Cisco AMP for Endpoints is an example of EDR solution with the following feature:

**Global Threat Intelligence**

Prevention starts with strengthening your defenses using the **best global threat intelligence** so you can block malware as new threats emerge. Cisco's team of threat researchers continuously feed threat intelligence into AMP for Endpoints so customers are protected 24/7.

**Malware Blocking**

AMP for Endpoints uses a framework of complementary detection engines, including one-to-one signatures, fuzzy fingerprinting, **machine learning**, and an AV detection engine—all working together to catch and block malware before it can execute.

**File Sandboxing**

A built-in sandbox automatically analyzes unknown files against over 700 behavioral indicators to detect malicious files and automatically **block and quarantine them**. (<-- this means containment)

**Proactive Protection**

Closing attack pathways before they can be exploited is a key strategy for preventing compromise. AMP's vulnerable software feature shows you all the software on your endpoints that can be exploited, with the ability to use application control to harden against attacks. AMP's low prevalence capability detects targeted malware and prevents it from slipping under the detection radar.

**QUESTION 447**

In Cisco SD-WAN, which protocol is used to measure link quality?

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

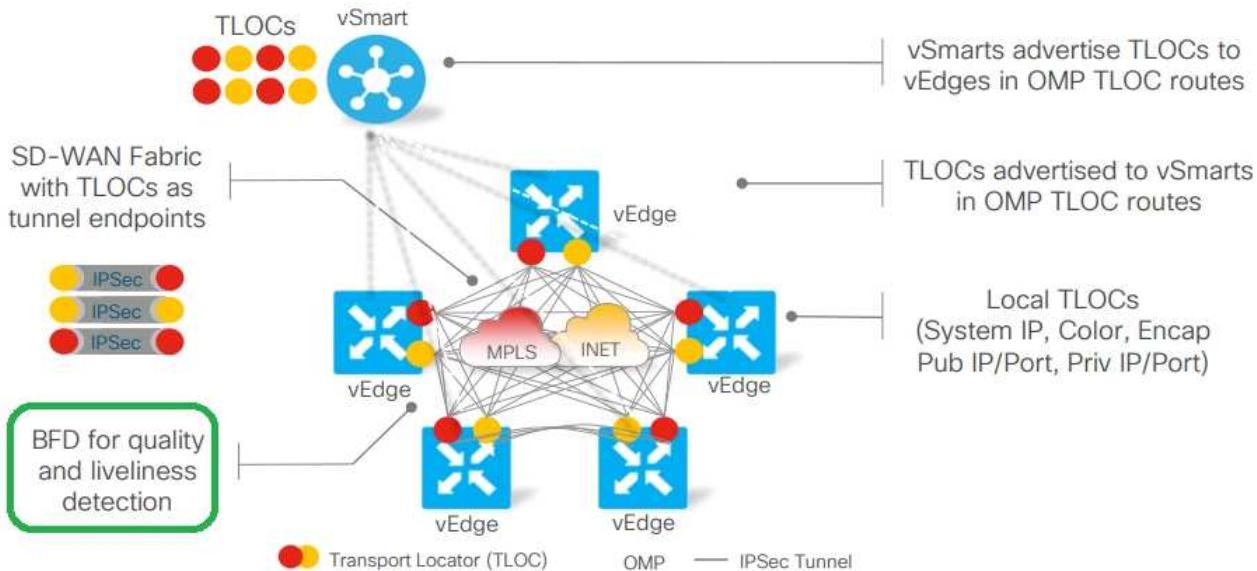
**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

# Data Plane Establishment



## QUESTION 448

Which measurement is used from a post wireless survey to depict the cell edge of the access points?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

### Explanation/Reference:

From Cisco book "Voice Over Wireless LAN (VoWLAN)" about Site Survey and RF Design Validation

### Analyze and define the cell edge:

This requires the use of AirMagnet Survey, although there are simple tools like Omnipcap or Wireshark that can be used to measure wireless traffic as a client roams from one AP to another. According to design best practices that revolve around the Cell Edge Design, a wireless handset should roam before the RSSI reaches -67 dBm. You can analyze signal strength and determine the approximate cell edge by measuring the signal strength in a beacon frame as you move from the center of one cell towards the edge of that cell.

## QUESTION 449

What is a characteristic of a virtual machine?

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

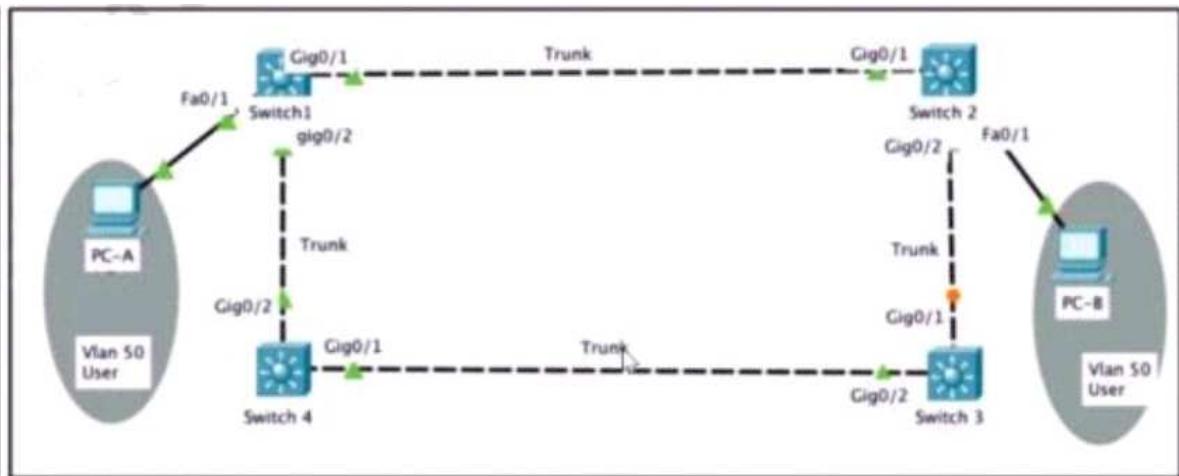
**Correct Answer: D**

**Section: (none)**

**Explanation**

### Explanation/Reference:

## QUESTION 450



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

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Choice A achieves point 1 and point 3 (with portfast disabled). However portfast port will still send BPDU.

Choice C and D configures BPDU guard for all portfast port and specific port respectively. However, the port(s) will be disabled if BPDU is received.

Choice B adds BPDU filter to all portfast ports and can prevent a portfast port from sending BPDU. Moreover if BPDU received, the port can still send / receive frames, only the portfast and BPDU filter features are disabled.

**QUESTION 451**

Refer to the exhibit.

\*\*\*

An exhibit where a router:

- g0/0 having IP 209.165.200.225/27 is connecting to Internet

- g0/1 having IP 10.1.1.1 is connecting to a internal web server

The internal web server has an IP 10.1.1.100 and is listening to 8080 port

\*\*\*

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

- A. **interface G0/0  
ip address 209.165.200.225 255.255.255.224  
ip nat inside**
- interface G0/1  
ip address 10.1.1.1 255.255.255.0  
ip nat outside**
- ip nat inside source static tcp 10.1.1.1 8080 209.165.200.225 80**

- B.
- ```
interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat outside

interface G0/1
ip address 10.1.1.1 255.255.255.0
ip nat inside

ip nat inside source static tcp 10.1.1.100 8080 interface G0/0 80
```
- C.
- ```
interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat inside

interface G0/1
ip address 10.1.1.1 255.255.255.0
ip nat outside

ip nat inside source static tcp 209.165.200.225 80 10.1.1.100 8080
```
- D.
- ```
interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat outside

interface G0/1
ip address 10.1.1.1 255.255.255.0
ip nat inside

ip nat inside source static tcp 209.165.200.225 8080 10.1.1.100 8080
```

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Only B and D is configured correctly for NAT insdie and outside interface.

But for D, the static mapping is incorrectly configured since the internal host IP / port should be configured first in the command.

For B, although it uses "interface g0/0 80" for the public IP / port for translation. It is a valid configuration since the question does not require you to configure a specific public IP address and there is no requirement for the external port number being used for translatiion.

**QUESTION 452**

A network engineer configures BGP between R1 and R2. Both routers use BGP peer group CORP and are set up to use MD5 authentication. This message is logged to the console of router R1:

"May 5 39:85:86.070: %TCP-6-BADAUTH" Invalid MD5 digest from 10.10.10.1 (29832) to 10.120.10.1 (179) tebleid -0

Which two configurations allow a peering session to form between R1 and R2? (Choose two.)

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

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since the message is shown in R1 which detects authentication problem in the BGP messages, this means that:

- the neighbor i.e. R2 has an IP 10.10.10.1
- R1 itself has an IP 10.120.10.1

Hence R1 should configure a password for neighbor R2 of 10.10.10.1

Hence R2 should configure the same password for neighbor R1 of 10.120.10.1

**QUESTION 453**

What is used to perform QoS 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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 454**

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

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

**Correct Answer:** BCD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Four things determine Air Time Efficiency:

- Data rate (Modulation density) or QAM
- Number of spatial streams and spatial reuse
- Channel bandwidth
- Protocol overhead e.g. Preamble/Ack/BA, Guard Interval "GI" etc.

**QUESTION 455**

While configuring an IOS router for HSRP with a virtual IP of 10.1.1.1, an engineer sees this log message.

Jan 1 12:12:12.111 : %HSRP-4-DIFFVIP1: GigabitEthernet0/0 Grp 1 active routers virtual IP address 10.1.1.1 is different to the locally configured address 10.1.1.25

Which configuration change must the engineer make?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 456**

An engineer runs the code against an API of Cisco DNA 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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The HyperText Transfer Protocol (HTTP) 405 Method Not Allowed response status code indicates that the request method is known by the server but is not supported by the target resource.

For obtaining a token, you need to supply credential to "Create" a new token. Therefore, you should use "POST".

The Python code above uses `requests.get(...)` which send request using "GET" method.

**QUESTION 457**

Which step reduces the amount of data that NETCONF server returns to the NETCONF client, to only the interface's configuration?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 458**

Which line must be added in the Python function to return the JSON object {"cat\_9k": "FXS193202SE")?

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 459**

What is a characteristic of YANG?

- A. It is a Cisco proprietary language that models NETCONF data

- B. It allows model developers to create custom data types
- C. It structures data in an object-oriented fashion to promote model reuse
- D. It provides loops and conditionals to control now within models

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 460**

What is one difference between saltstack and ansible?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The SaltStack framework consists of a server that is called the Salt primary, and Salt nodes that run client programs, called minions. The Cisco device e.g. Nexus switch (switch) is a Salt node.

SaltStack minions can run either on-box or off-box, respective to the switch, to execute the configuration or management operations:

- On-box, the minions run in the switch's Bash shell. These native minions receive and execute remote commands from the primary, and relay the command's results to the primary. In an on-box deployment, the minions are enabled in the switch's Guest shell.
- Off-box, a different type of minion, a proxy minion, runs over anSSH connection to the switch or through the NX-API. The proxy minion, either theSSH proxy minion or the NX-API proxy minion, receives and executes the commands. The proxy then relays the command's results to the primary.

The choice A is running the SaltStack minions as off-box.

**QUESTION 461**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 462**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 463**

What does the Cisco DMA REST response Indicate?

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

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

**Correct Answer:** C

**Section:** (none)

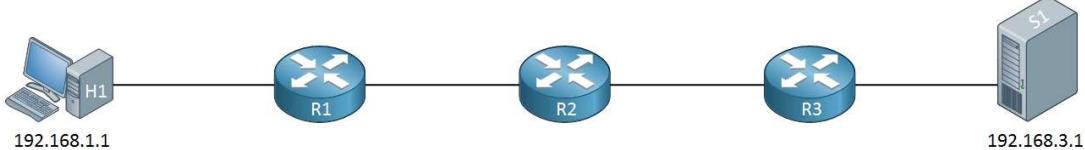
**Explanation**

**Explanation/Reference:**

Remarks :

Cisco DNA Center Is unable to communicate with cat3850-1

#### QUESTION 464



\*\*\* A protocol analyzer showing the ping packet sent by H1 has a TTL value of 2 in the IP header \*\*\*

Refer to the exhibit. When troubleshooting a routing issue, an engineer issues a ping from H1 to S1. Which two actions can be found due to the initial value of the TTL? (Choose two.)

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

**Correct Answer:** BD

**Section:** (none)

**Explanation**

Explanation/Reference:



**QUESTION 465**

What is the responsibility of a secondary WLC?

- A. It shares the traffic load of the LAPs with the primary controller.
- B. It avoids congestion on the primary controller by sharing the registration load on the LAPs.
- C. It registers the LAPs if the primary controller fails.
- D. It enables Layer 2 and Layer 3 roaming between itself and the primary controller.

Correct Answer: C

Section: Selected

Explanation

Explanation/Reference:

**QUESTION 466**

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

WLANS > Edit 'office\_hq'

The screenshot shows the 'Policy-Mapping' tab of the 'office\_hq' WLAN configuration. The 'Allow AAA Override' checkbox is checked and highlighted with a red box. Other settings include Coverage Hole Detection (Enabled), Session Timeout (1800 seconds), and various interface and client-related parameters. The right side of the screen shows sections for DHCP, Management Frame Protection (MFP), DTIM Period, NAC, Load Balancing, and Passive Client settings.

**QUESTION 467**

Vlan	Role	Sts	Cost	Prio.	Nbr	Type
VLAN0001	Desg	FWD	4	128.4	P2p	Edge
VLAN0010	Desg	FWD	4	128.4	P2p	Edge
VLAN0020	Desg	FWD	4	128.4	P2p	Edge
VLAN0030	Desg	FWD	4	128.4	P2p	Edge
VLAN0040	Desg	FWD	4	128.4	P2p	Edge

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

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The interface is a trunk port. Since each of the 5 VLANs is shown with the port role, MST is not configured. Since the wordings "Edge" are shown, the port is configured with portfast feature. However since the interface is a trunk port, portfast feature can only be enabled by "**spanning-tree portfast trunk**".

#### QUESTION 468



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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 469

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

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 470

```
R1
int tu 100
ip addr 192.168.100.1 255.255.255.0
keepalive 5 3
tunnel source g0/0
tunnel dest 200.0.0.2

int g0/0
ip addr 100.0.0.1

router ospf 100
network 0.0.0.0 255.255.255.255 area 0

ip route 0.0.0.0 0.0.0.0 100.0.0.254

R2
int tu 100
ip addr 192.168.100.2 255.255.255.0
keepalive 6 4
tunnel source g0/0
tunnel dest 100.0.0.1
```

```
int g0/0
ip addr 100.0.0.1

router ospf 100
network 0.0.0.0 255.255.255.255 area 0

ip route 0.0.0.0 0.0.0.0 200.0.0.254
```

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The tunnel will first be formed through the static default route.

However once the tunnel is formed, OSPF will exchange routing information and the remote tunnel destination will be learnt through the tunnel. This will cause the tunnel to become down.

Keepalives do NOT need to be matched in both ends of the tunnel.

**QUESTION 471**

\*\*\*\*\* show outputs with Sw1's interface configured with dynamic auto and Sw2's interface configured with dynamic auto \*\*\*\*\*

Refer to the exhibit. An engineer attempts to configure a trunk between switch SW1 and switch SW2 using DTP, but the trunk does not form. Which command should the engineer apply to switch SW2 to resolve this issue?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 472**

What does a router do when configured with the default DNS lookup settings, and a URL is entered on the CLI?

- A. initiates a ping request to the URL
- B. prompts the user to specify the desired IP address
- C. continuously attempts to resolve the URL until the command is cancelled
- D. attempts to query a DNS server on the network

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

This occurs when DNS server's IP address is obtained from DHCP or manually configured.

**QUESTION 473**

What does a router do when configured with the default DNS lookup settings, and a URL is entered on the CLI?

- A. initiates a ping request to the URL
- B. prompts the user to specify the desired IP address
- C. continuously attempts to resolve the URL until the command is cancelled
- D. sends a broadcast message in an attempt to resolve the URL

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

This occurs when DNS server's IP address is NOT obtained from DHCP or NOT manually configured.

**QUESTION 474**

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

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

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 475**

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.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 476**

Refer to the exhibit.

\*\*\*

An exhibit in which a router f0/0 is connecting to LAN and f0/1 is connecting to Internet

It also has the following NAT mapping

10.10.10.101 155.1.1.101  
10.10.10.102 155.1.1.102  
10.10.10.103 155.1.1.103

\*\*\*

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

A.

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

B.

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

C.

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

D.

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

deterministic translation means a fixed NAT mapping. This requires the configuration of static NAT mapping entries.  
D is wrong since the NAT inside / outside interface is wrongly configured.

#### QUESTION 477

What is the function of a VTEP in VXLAN?

- A. provide the routing underlay and overlay for VXLAN headers
- B. dynamically discover the location of end hosts in a VXLAN fabric
- C. encapsulate and de-encapsulate traffic into and out of the VXLAN fabric
- D. statically point to end host locations of the VXLAN fabric

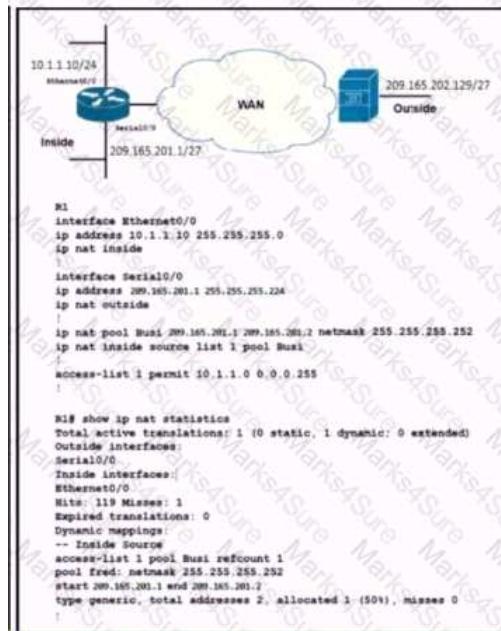
**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 478



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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

There is no static mapping configured and therefore the public IP address is allocated when the first packet is received.  
No "overload" keyword is configured in the "ip nat inside source list ..." command, therefore there is no "overload" i.e. no PAT.

#### QUESTION 479

Drag and drop the snippets onto the blanks within the code construct a script that configure a loopback interface with an IP address (not all options are used)?

Select and Place:

The XML code in the left pane is:

```
{
  "@message-id": "101",
  "edit-config": {
    "running": null
  },
  "config": {
    "native": {
      "interface": {
        "Loopback": {
          "ip": {
            "address": [
              {
                "address": "10.10.10.10",
                "mask": "255.255.255.255"
              }
            ]
          }
        }
      }
    }
  }
}
```

The right pane contains the following colored boxes:

- "fixed": (light blue)
- "config": (dark blue)
- "mask": (light green)
- "primary": (light green)
- "name": "100" (light green)
- "target": (light blue)

Correct Answer:

The XML code in the left pane is now correctly configured:

```
{
  "@message-id": "101",
  "edit-config": {
    "target": "running",
    "running": null
  },
  "config": {
    "native": {
      "interface": {
        "Loopback": {
          "name": "100"
        }
      }
    }
  }
}
```

Section: (none)

Explanation

Explanation/Reference:

#### QUESTION 480

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

Which are the characteristics of OSPF (Choose Two)?

- A. Supports virtual links
- B. can automatically summarize networks at the boundary
- C. requires manual configuration of network summarization

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 481

\*\*\* Missing exhibit. Several lines of logging messages including...

- a line about changed from area 0 to 1.

- a line similar to the following:

%OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from x.x.x.x vlan xx

Refer to me exhibit. What is the cause of the log messages?

- A. hello packet mismatch
- B. OSPF area change
- C. MTU mismatch
- D. IP address mismatch

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 482

A network engineer is configuring Flexible NetFlow and enters these commands:

```
Sampler Netflow1
mode random one-out-of 100
interface fastethernet 1/0
flow-sampler netflow1
```

Which are two results of implementing this feature instead of traditional NetFlow? (Choose two)

- A. Only the flows of top 100 talkers are exported
- B. CPU and memory utilization are reduced
- C. The data export flow is more secure
- D. The accuracy of the data to be analyzed is improved
- E. The number of packets to be analyzed are reduced

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 483

<u>Script</u> <pre>import ncclient  with ncclient.manager.connect(host='192.168.1.1', port=830, username='root', password='test123!',     allow_agent=False) as m:     print(m.get_config('running').data_xml)</pre>	<u>Output</u> <pre>\$ python get_config.py Traceback (most recent call last):   File "get_config.py", line 3, in &lt;module&gt;     with ncclient.manager.connect(host='192.168.1.1', port=830, username='root', AttributeError: 'module' object has no attribute 'manager'</pre>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

- A. ncclient import manager

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Similar to 419 but the best choice "from ncclient import manager" is not available.  
Therefore the only valid answer is to import all classes from ncclient.

However, for this change to work, you need a "ncclient" package that includes special settings in the "\_\_init\_\_.py" file. Moreover, you also need to change the calling of the connect function to "manager.connect(...)"

#### QUESTION 484

Refer to the exhibit. What is the effect of the configuration?

```
aaa new-model
aaa authentication login authorizationlist tacacs+
tacacs-server host 192.168.0.202
tacacs-server key ciscotestkey
line vty 0 4
login authentication authorizationlist
```

- A. The device will allow users at 192.168.0.202 to connect to vty lines 0 through 4 using the password ciscotestkey
- B. The device will allow only users at 192.168.0.202 to connect to vty lines 0 through 4
- C. When users attempt to connect to vty lines 0 through 4, the device will authenticate them against TACACS+ if local authentication fails
- D. The device will authenticate all users connecting to vty lines 0 through 4 against TACACS+

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 485

\*\*\* missing exhibit. A show output similar to the following:

```
Router# show crypto isakmp sa
dst          src          state      conn-id slot status
10.0.0.1    10.0.0.2    QM_IDLE      1      0 ACTIVE
***
```

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

"QM\_IDLE" state means that the ISAKMP SA is authenticated and can be used for subsequent Quick Mode (Phase 2) exchanges.  
QM\_IDLE state + ACTIVE status usually means a healthy IPsec tunnel has been formed.

#### QUESTION 486

Refer to the exhibit.

```
ip sla 10
icmp-echo 192.168.10.20
timeout 500
frequency 3
ip sla schedule 10 life forever start-time now
track 10 ip sla 10 reachability
```

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

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

**Correct Answer:** A

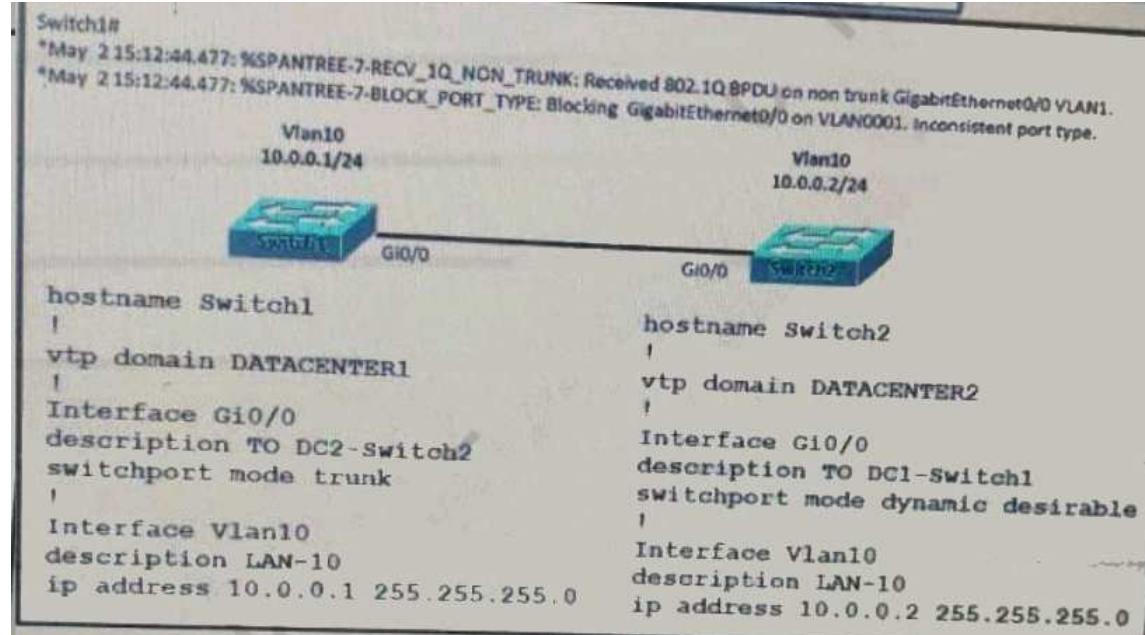
**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 487**

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



- A. Change the VTP domain to match on both switches
- B. Change Switch2 to switch port mode dynamic auto
- C. Change Switch1 to switch port mode dynamic auto
- D. Change Switch1 to switch port mode dynamic desirable

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The logging message is shown since Switch2's g0/0 remains as Access Port.

Normally without disabling negotiation, "trunk" and "dynamic desirable" can form trunk. However, since DTP will also check the VTP domain name configured, trunk cannot be formed in the above case.

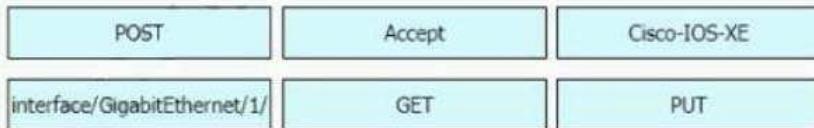
**QUESTION 488**

Refer to the exhibit Drag and drop the snippets into the RESTCONF request to form the request that returns this response. Not all options are used.

```
{
  "Cisco-IOS-XE-native:GigabitEthernet": {
    "name": "1",
    "vrf": {
      "forwarding": "MANAGEMENT"
    },
    "ip": {
      "address": {
        "primary": {
          "address": "10.0.0.151",
          "mask": "255.255.255.0"
        }
      }
    },
    "mop": {
      "enabled": false
    },
    "Cisco-IOS-XE-ethernet:negotiation": {
      "auto": true
    }
  }
}
```

**Select and Place:**

URL - http://10.10.10.10/restconf/api/running/native/  
HTTP Verb-    
Body- N/A  
Headers-  -application/vnd.yang.data+json  
Authentication-privileged level 15 credentials



Correct Answer:

URL - http://10.10.10.10/restconf/api/running/native/  
HTTP Verb- GET  
Body- N/A  
Headers- Accept-application/vnd.yang.data+json  
Authentication-privileged level 15 credentials



Section: Selected  
Explanation

Explanation/Reference:

**QUESTION 489**

Which WLAN Layer 3 setting must be configured to provide users with a splash page for authentication?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 490**

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 491**

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

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

D. Mozilla

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Many other questions about REST API in this exam are using Postman as example.

#### QUESTION 492

What does the Cisco DNA Center use to enable the delivery of applications through a network and to yield analytics for innovation?

- A. process adapters
- B. Command Runner
- C. intent-based APIs
- D. domain adapters

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Intent-based APIs leverage the controller to enable business and IT applications to deliver intent to the network and to reap network analytics and insights for IT and business innovation. These enable APIs that allow Cisco DNA Center to receive input from a variety of sources, both internal to IT and from line-of-business applications, related to application policy, provisioning, software image management, and assurance.

#### QUESTION 493

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

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

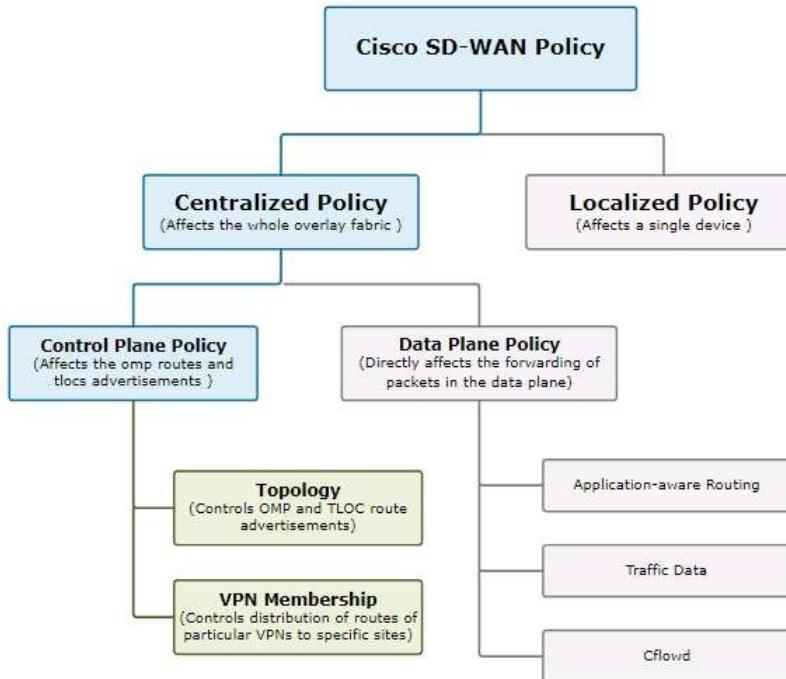
**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

A centralized control policy is a policy that manipulates the route and tloc information that is exchanged between the vSmart controllers and the vEdge devices in the Cisco SD-WAN overlay fabric. It can influence the overlay topology of IPsec tunnels and the routing paths through the fabric.



**Topology** - Topology policies control the route information such as omp, tloc, and service routes that are being redistributed to a list of sites. As the name implies, they are typically used for limiting the number of overlay tunnels between sites and controlling the overlay topology.

**VPN Membership** - VPN Membership policies are used to control the distribution of routing information for specific VPNs to a list of sites. A typical use-case is for creating guest networks that have Internet access but site-to-site communication is restricted.

#### QUESTION 494

Which DHCP option provides CAPWAP APs with the address of a wireless LAN controller(s)?

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

**Correct Answer:** A

**Section: (none)****Explanation****Explanation/Reference:**

Similar to Q122

**QUESTION 495**

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

- A. to perform initial authentication of devices
- B. to provide secure data plane connectivity over WAN links
- C. to monitor, configure, and maintain SD-WAN devices
- D. to establish secure control plane connections

**Correct Answer: D****Section: (none)****Explanation****Explanation/Reference:**

vSmart controller - This software-based component is responsible for the centralized control plane of the SD-WAN network. It maintains a secure connection to each WAN Edge router and distributes routes and policy information via the Overlay Management Protocol (OMP), acting as a route reflector. It also orchestrates the secure data plane connectivity between the WAN Edge routers by reflecting crypto key information originating from WAN Edge routers, allowing for a very scalable, IKE-less architecture.

**QUESTION 496**

Which are the characteristics of EIGRP?

- A. uses Dijkstra's Shortest Path First algorithm
- B. uses Diffused Update Algorithm
- C. uses bandwidth, delay, reliability, and load for routing metric
- D. uses an election process

**Correct Answer: BC****Section: (none)****Explanation****Explanation/Reference:****QUESTION 497**

Which are the characteristics of OSPF?

- A. uses Dijkstra's Shortest Path First algorithm
- B. uses Diffused Update Algorithm
- C. uses bandwidth, delay, reliability, and load for routing metric
- D. uses an election process

**Correct Answer: AD****Section: (none)****Explanation****Explanation/Reference:****QUESTION 498**

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

- A. username netadmin secret 9 \$9\$vFpMfBelbRVV8SseX/bDAxtuV
- B. line Console 0  
password \$15b1Ju\$
- C. username netadmin secret 5 \$1\$b1JUSkZbBS1Pyh4OzwXyZ1kSZ2
- D. username netadmin secret \$15b1JuSk404850110QzwXyZ1k SZ2

**Correct Answer: A****Section: (none)****Explanation****Explanation/Reference:****QUESTION 499**

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

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

- A. show netconf | section rpc-reply
- B. show netconf rpc-reply

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The output of the show netconf schema command displays the element structure for a NETCONF request and the resulting reply. This schema can be used to construct proper NETCONF requests and parse the resulting replies.

#### QUESTION 500

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

- uses syslog IP address: 10.10.10.1
- uses a reliable protocol
- must not use any well-known TCP/UDP ports

- A. logging host 10.10.10.1 transport tcp port 1024
- B. logging origin-id 10.10.10.1
- C. logging host 10.10.10.1 transport udp port 1023
- D. logging host 10.10.10.1 transport udp port 1024

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 501

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

(The above question do not mentioned about the router being configured, the following assume the Client router is being configured).

**Select and Place:**

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



192.168.1.1

192.168.1.2

65000

65001

Client

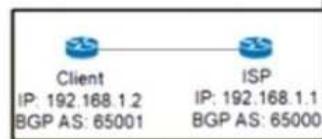
ISP

**Correct Answer:**

```

<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
<router>
<ios-bgp:bgp>
<ios-bgp:id> 65001 </ios-bgp:id>
<ios-bgp:neighbor>
<ios-bgp:id> 192.168.1.1 </ios-bgp:id>
<ios-bgp:remote-as> 65000 </ios-bgp:remote-as>
</ios-bgp:neighbor>
<ios-bgp:address-family>
<ios-bgp:ipv4>
<ios-bgp:af-name>unicast</ios-bgp:af-name>
<ios-bgp:ipv4-unicast>
<ios-bgp:neighbor>
<ios-bgp:id> 192.168.1.1 </ios-bgp:id>
<ios-bgp:soft-reconfiguration>inbound</ios-bgp:soft-reconfiguration>
</ios-bgp:neighbor>
</ios-bgp:ipv4-unicast>
</ios-bgp:ipv4>
</ios-bgp:no-vrf>
</ios-bgp:address-family>
</ios-bgp:bgp>
</router>
</native>
</config>

```



192.168.1.1

192.168.1.2

65000

65001

Client

ISP

**Section: (none)**  
**Explanation**

**Explanation/Reference:**

The "id" under bgp is the router's own AS number since CLI also uses AS number in the start of the BGP configuration section e.g. "router bgp 65000. (Note that for BGP router-id, the tag should include the wording "router-id".)

Under "neighbor" sections, the "id" there means the neighbor router's IP address.

**QUESTION 502**

What are the characteristics of EIGRP?

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

**Correct Answer: BDE**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

The question may be in the form of Drag and Drop as follows:

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.	
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.	

OSPF	

**QUESTION 503**

What are the characteristics of OSPF?

- A. The default Administrative Distance is equal to 110.
- B. It requires an Autonomous System number to create a routing instance for exchanging routing information

- C. It uses virtual links to connect two paths of a partitioned backbone through a non-backbone area.
- D. It is an Advanced Distance Vector routing protocol.
- E. It relies on the Diffused Update Algorithm to calculate the shortest path to a destination.
- F. It requires a process ID that is local to the router.

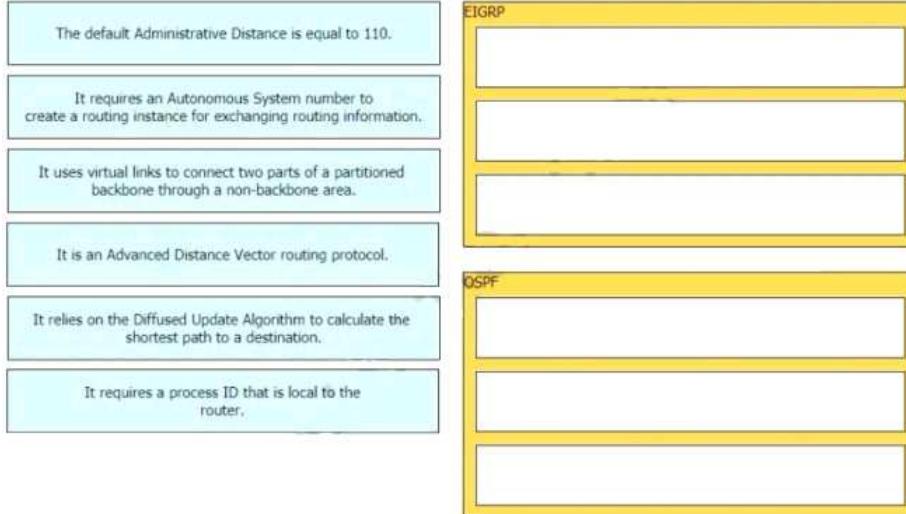
**Correct Answer:** ACF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The question may be in the form of Drag and Drop as follows:



#### QUESTION 504

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

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

- A. Device(config)# netconf lock-time 500
- B. Device(config)# netconf max-message 1000
- C. Device(config)# no netconf ssh acl 1
- D. Device(config)# netconf max-sessions 100

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The most probable reason is that the output of show run is too large to be shown properly.

netconf ssh [acl access-list-number]

Optionally, you can configure an access control list for this NETCONF session

netconf lock-time seconds

(Optional) Specifies the maximum time, in seconds, a NETCONF configuration lock is in place without an intermediate operation.

netconf max-sessions session

(Optional) Specifies the maximum number of concurrent NETCONF sessions allowed.

netconf max-message size

(Optional) Specifies the maximum size, in kilobytes (KB), for the messages received in a NETCONF session.

#### QUESTION 505

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

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

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

The splash page for authentication is probably web authentication.

**QUESTION 506**

Refer to the exhibit. \*\*\* missing \*\*\*

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

- A. 

```
router ospf 1
default-information originate always
end
```
- B. 

```
router ospf 1
redistribute bgp 65001 metric 100 route-policy BGP-TO-OSPF
end
```
- C. 

```
router ospf 1
default-metric 100
end
```
- D. 

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since the default route is sourced from BGP, it should be better if OSPF advertises the default route only if a default route is found in the routing table (i.e. learnt from BGP).

**QUESTION 507**

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

- A. 

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

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

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Only C and D monitor the syslog message for OSPF neighbor down.

Since debug command can only be issued in privileged mode, enable is required and it is only included in choice C.

**QUESTION 508**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

When you create an MPLS traffic engineering tunnel interface, you need to establish a label distribution session between the tunnel headend and the tailend routers. You establish these non-directly connected MPLS LDP sessions by enabling the transmission of targeted Hello messages.

You can use the `mpls ldp neighbor targeted` command to set up a targeted session.

**QUESTION 509**

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

- Include a permit statement as the first entry
- Include at least one explicit deny statement
- Remove the implicit deny entry
- Include a permit statement as the last entry

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 510**

Refer to the exhibit. (\*\* missing \*\*\* Assume R2 is shown as Level 2.)

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

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

**Correct Answer:** A

**Section:** (none)

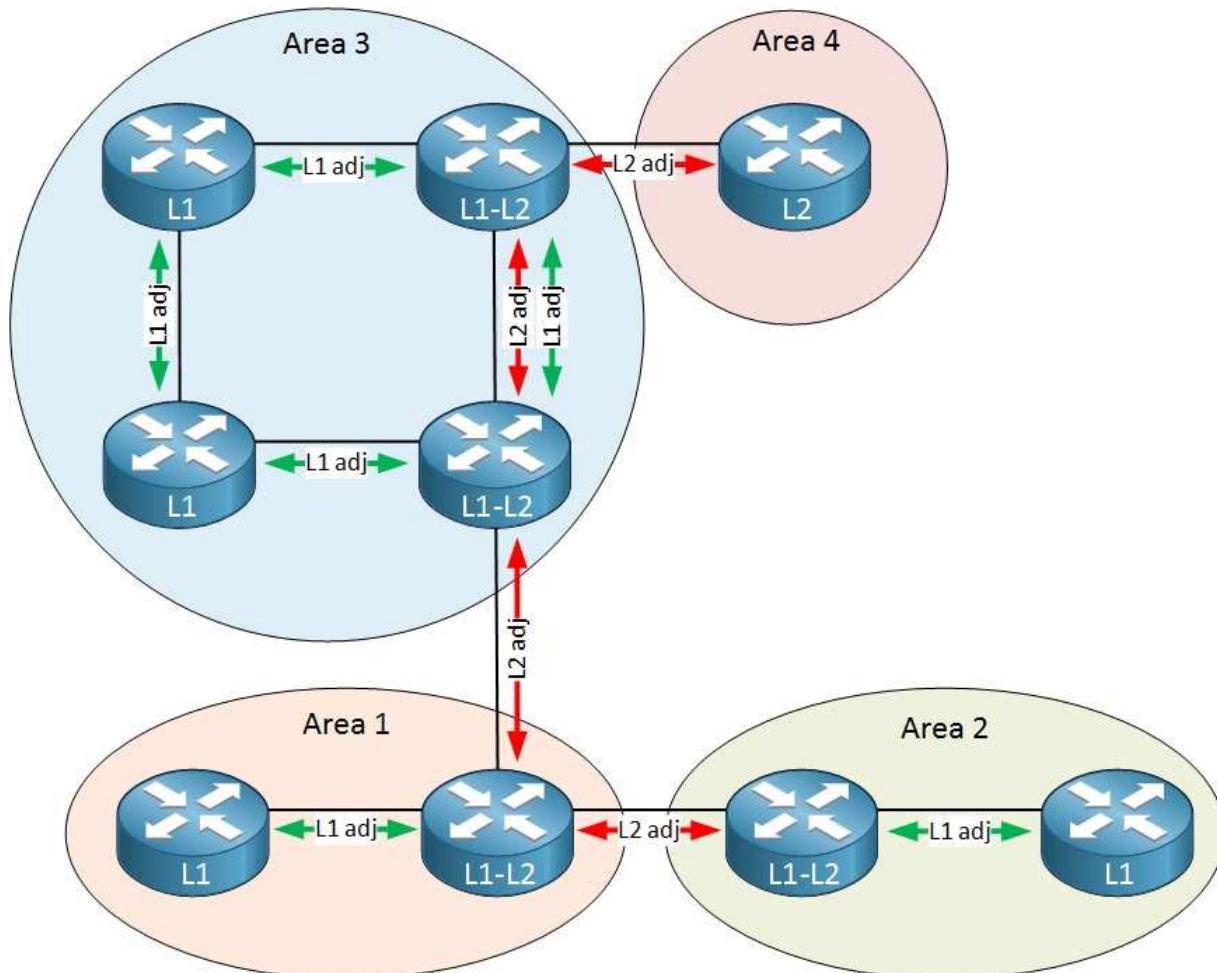
**Explanation**

**Explanation/Reference:**

**Important :** The answer should be B if R2 is shown as level 1 !!!

**Remarks :**

IS-IS has two levels or hierarchy, Level 1 and Level 2. All interconnected Level 1 routers work like areas. Level 2 routers are used to provide inter-area topology of different areas of level 1.



A IS-IS router can be level 1 only, level 2 only or level 1 & 2. There is no adjacency between L1 only and L2 only router.

There are only two network types in IS-IS. Broadcast and Point-to-Point.

**QUESTION 511**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

MVPN IP allows a service provider to configure and support multicast traffic in an MPLS VPN environment. This feature supports routing and forwarding of multicast packets for each individual VRF instance, and it also provides a mechanism to transport VPN multicast packets across the service provider backbone.

When the multicast transmission exceeds the defined threshold, the sending PE router creates the data MDT and sends a UDP message, which contains information about the data MDT, to all routers on the default MDT.

MVPN also supports the dynamic creation of MDTs for high-bandwidth transmission. Data MDTs are a feature unique to Cisco IOS software. Data MDTs are intended for high-bandwidth sources such as full-motion video inside the VPN to ensure optimal traffic forwarding in the MPLS VPN core.

Data MDTs are created only for (S, G) multicast route entries within the VRF multicast routing table. They are not created for (\*, G) entries regardless of the value of the individual source data rate.

**QUESTION 512**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

MPLS Operations, Administration, and Maintenance (OAM) helps service providers to monitor label-switched paths (LSPs) and quickly isolate MPLS forwarding problems to assist with fault detection and troubleshooting in an MPLS network.

The MPLS LSP Ping feature is used to check the connectivity between Ingress LSR and egress LSRs along an LSP. MPLS LSP ping uses MPLS echo request and reply messages, similar to Internet Control Message Protocol (ICMP) echo request and reply messages, to validate an LSP.

The destination IP address of the MPLS echo request packet is different from the address used to select the label stack. The destination IP address is defined as a 127.x.y.z/8 address and it prevents the IP packet from being IP switched to its destination, if the LSP is broken.

**QUESTION 513**

An engineer is working with the Cisco DNA Center API Drag and drop the methods from the left onto the actions that they are used for on the right.

**Select and Place:**



**Correct Answer:**



**Section:** (none)

**Explanation**

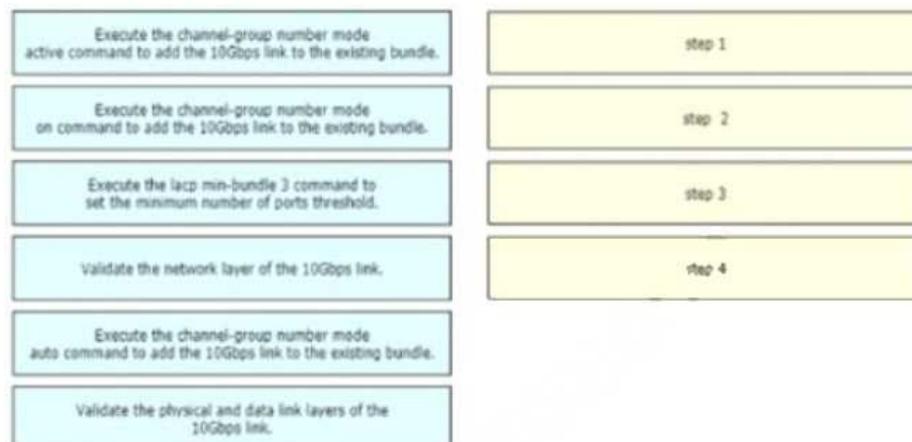
**Explanation/Reference:**

**QUESTION 514**

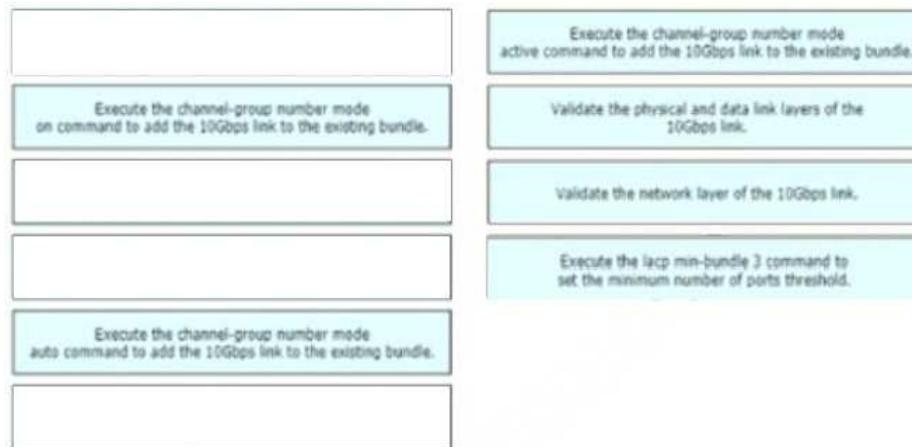
A network engineer is adding an additional 10Gbps link to an existing 2x10Gbps LACP-based LAG to augment its capacity. Network standards require a bundle interface to be taken out of service if one of its member links goes down, and the new link must be added with minimal impact to the production network. Drag and drop the

tasks that the engineer must perform from the left into the sequence on the right. Not all options are used.

**Select and Place:**



**Correct Answer:**



**Section: (none)**

**Explanation**

**Explanation/Reference:**

Active is for LACP

Since bundle should be down if any one port fails, minimum bundle is 3 (2 existing + 1 new). However you must verify that all 3 links are working properly before you configure this. Otherwise the bundle will be down after configuration.

**QUESTION 515**

Which network devices secure API platform?

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Since most API uses HTTP, you can use firewall for web application to protect it. Cisco has a product for providing this features.

**Cisco® Advanced WAF and Bot Protection** defends your online presence and ensures that website, mobile applications, and APIs are secure, protected, and “always on.”



WAF is the short form of Web Application Firewall.

**QUESTION 516**

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

- A. DTLS
- B. IPsec
- C. PGP
- D. HTTPS

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Each Cisco vSmart Controller establishes and maintains a control plane connection with each edge router in the overlay network. Each connection, which runs as a DTLS tunnel, is established after device authentication succeeds, and it carries the encrypted payload between the Cisco vSmart Controller and the edge router.

**QUESTION 517**

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

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

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 518**

Which threat defence mechanism, when deployed at the network perimeter, protects against zero-day attacks?

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

**Correct Answer:** A

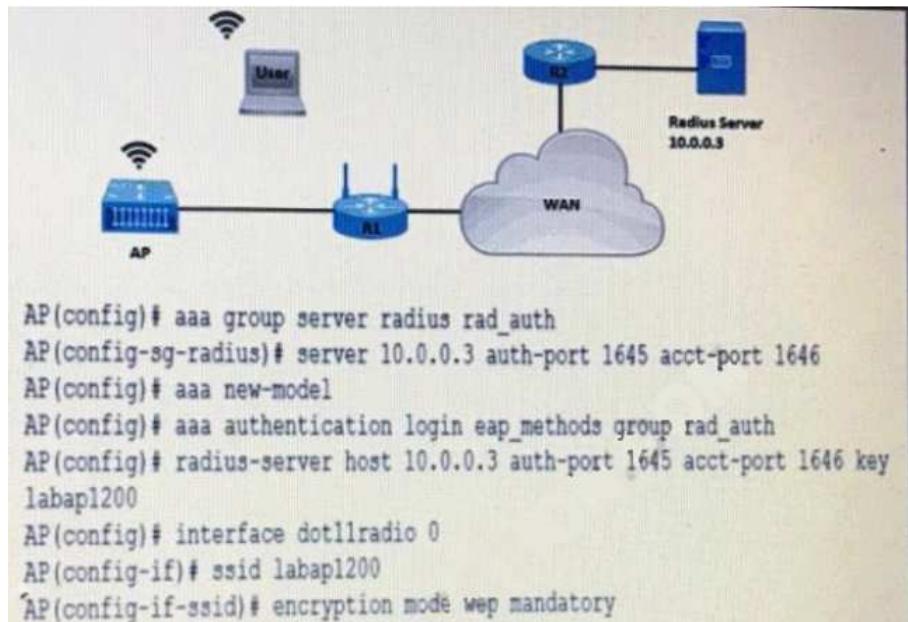
**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 519**

Refer to the exhibit.



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

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

**Correct Answer:** D

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 520**

What is required for a virtual machine to run?

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

**Correct Answer:** B**Section:** (none)**Explanation****Explanation/Reference:****QUESTION 521**

An engineer must configure AAA on a Cisco 9800 WLC for central web authentication. Which two commands are needed to accomplish this task? (Choose two.)

- A. (Cisco Controller) > config wlan aaa-override disable <wlan-id>
- B. (Cisco Controller) > config radius acct add 10.10.10.12 1812 SECRET
- C. (Cisco Controller) > config wlan aaa-override enable <wlan-id>
- D. Device(config-locsvr-da-radius)# client 10.10.10.12 server-key 0 SECRET
- E. Device(config)# aaa server radius dynamic-author

**Correct Answer:** DE**Section:** (none)**Explanation****Explanation/Reference:**

Central web authentication offers the possibility to have a central device that acts as a web portal (in this example, the ISE). The major difference compared to the usual local web authentication is that it is shifted to Layer 2 along with MAC filtering or dot1x authentication.

D and E is part of the steps. They configure AAA for Central Web Authentication in Cisco 9800 WLC.

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide runs Cisco IOS XE image.

A, B and C are commands for previous WLC series. Their configuration commands starts with the keyword "config".

**QUESTION 522**

What is required for intercontroller Layer 3 roaming?

- A. Mobility groups are established between wireless controllers.
- B. The management VLAN is present as a dynamic VLAN on the second WLC.
- C. WLCs use separate DHCP servers.
- D. WLCs have the same IP addresses configured on their interfaces.

**Correct Answer:** A**Section:** (none)**Explanation****Explanation/Reference:**

A mobility group is a set of controllers, identified by the same mobility group name, that defines the realm of seamless roaming for wireless clients. By creating a mobility group, you can enable multiple controllers in a network to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs.

**QUESTION 523**

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

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

**Correct Answer:** A**Section:** (none)**Explanation****Explanation/Reference:****QUESTION 524**

What is a benefit of Type 1 hypervisors?

- A. Administrators are able to load portable virtual machine packages in OVA or QCOW2 formats.
- B. Network engineers are able to create virtual networks or interconnect virtual machines in Layer 2 topologies
- C. Operators are able to leverage orchestrators to manage workloads that run on multiple Type 1 hypervisors
- D. Storage engineers are able to leverage VMDK files to provide storage to virtual machine.

**Correct Answer:** B**Section:** (none)**Explanation**

**Explanation/Reference:**

**QUESTION 525**

What is a characteristic of Cisco DNA Northbound APIs?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 526**

Refer to the exhibit. Which result does the python code achieve?

```
psswd = (base64.b64decode('SzFwM001RzchCg==')).decode('utf-8')).strip('\n')
d = datetime.date.today()
date = str(10000*d.year + 100*d.month + d.day)
```

- A. The code encrypts a base64 decrypted password.
- B. The code converts time to the "year/month/day" time format.
- C. The code converts time to the yyymmdd representation.
- D. The code converts time to the Epoch LINUX time format.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 527**

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 all 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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

This configuration is only applicable to Cisco controllers running AireOS 8.3 or later, devices running iOS 10 or later and MacBook computers running macOS High Sierra 10.13 or later.

The **Cisco Fast lane** configuration is an easy way to ensure that QoS is optimally configured in your WLAN controller, especially if iOS or Mac clients are expected to be a sizeable portion of the wireless clients since iOS devices mark QoS as per IETF recommendations.

**General Security QoS Policy-Mapping Advanced**

Quality of Service (QoS)	Silver (best effort) ▾
Application Visibility	<input type="checkbox"/> Enabled
AVC Profile	none ▾
Netflow Monitor	none ▾
Fastlane	Disable ▾
<b>WMM</b>	
WMM Policy	Allowed ▾
7920 AP CAC	<input type="checkbox"/> Enabled
7920 Client CAC	<input type="checkbox"/> Enabled

This can be changed using the GUI or the CLI command:

- config qos Fastlane enable/disable wlan <wlan id>

#### QUESTION 528

Which of the followings are true for On-Premises Deploymnnet model?

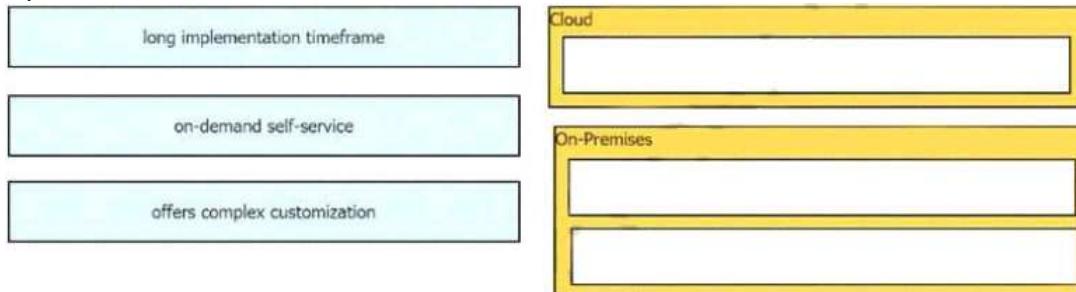
- long implementation timeframe
- on-demand self-service
- offers complex customization

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 529

Which component does Cisco Cyber Threat Defense use to measure bandwidth, application performance, and utilization?

- NetFlow
- Cisco Umbrella
- TrustSec
- Advanced Malware Protection for Endpoints

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

NetFlow was initially created to measure network traffic characteristics such as bandwidth, application performance, and utilization; and has historically been used for billing and accounting, network capacity planning, and availability monitoring.

#### QUESTION 530

A customer has two Cisco WLCs that manage separate APs throughout a building. Each WLC advertises the same SSID but terminates on different interfaces. Users report that they drop their connections and change IP addresses when roaming. Which action resolves this issue?

- Configure high availability.
- Enable test roaming.
- Enable client load balancing.
- Configure mobility groups.

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

#### QUESTION 531

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

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

**Correct Answer:** A  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

To prevent basic replay, a completely random session key can be used for each transaction and can't be used again. Another preventative measure for this type of attack is using timestamps on all messages.

**QUESTION 532**

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

- A. DTLS
- B. IPsec
- C. PGP
- D. HTTPS

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 533**

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

- A. VXLAN
- B. IS-IS
- C. 802.1Q
- D. CTS

**Correct Answer:** C  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

Extended Nodes – An Edge access device that connects Wired IoT Endpoints to the SDA Fabric via a Fabric Edge Node. Extended node connects to a fabric Edge node using an 802.1Q Trunk port.

**QUESTION 534**

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

```
measures = [
    {
        'Accept': 'application/yang-data+json',
        'Content-Type': 'application/yang-data+json'
    },
    data = json.dumps({
        'Cisco-IOS-XE-native:GigabitEthernet': [
            {
                'ip': {
                    'address': [
                        {
                            'primary': {
                                'address': '10.10.10.1',
                                'mask': '255.255.255.0'
                            }
                        }
                    ]
                }
            }
        ],
        verify = False
    })
    # Print the HTTP response code
    print('Response Code: ' + str(response.status_code))
}
```

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

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

Something missing in the top of the diagram. Probably there is an indication that the interface concerned is g2.

The HTTP 204 No Content success status response code indicates that a request has succeeded

**QUESTION 535**

A network engineer is enabling HTTPS access to the core switch, which requires a certificate to be installed on the switch signed by the corporate certificate authority. Which configuration commands are required to issue a certificate signing request from the core switch?

- A. Core-Switch(config)#crypto pki enroll Core-Switch  
Core-Switch(config)#ip http secure-trustpoint Core-Switch
- B. Core-Switch(config)#crypto pki trustpoint Core-Switch  
Core-Switch(ca-trustpoint)#enrollment terminal  
Core-Switch(config)#crypto pki enroll Core-Switch
- C. Core-Switch(config)#crypto pki trustpoint Core-Switch  
Core-Switch(ca-trustpoint)#enrollment terminal  
Core-Switch(config)#ip http secure-trustpoint Core-Switch
- D. Core-Switch(config)#ip http secure-trustpoint Core-Switch  
Core-Switch(config)#crypto pki enroll Core-Switch

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

An example

```
Router(config)#
crypto pki trustpoint TP
Router(ca-trustpoint)#
enrollment terminal
Router(ca-trustpoint)#
crypto pki authenticate TP
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIICNDCCAd6gAwIBAgIQOsCmXpVHwodKryRoqULV7jANBgkqhkiG9w0BAQUFADAS
MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31zdGVtczESMBAGA1UEAxMj
bXNjYS1yb290MB4XDThyMDIxNDAwNDYwMv0XDTA3MDIxNDAwNTQ0OFwOTELMAkG
A1UEBhMCVVMxFjAUBgNVBAoTDUNpc2NvIFN5c3RlbXMxEjAQBgNVBAMTCWlzy2Et
cm9vdDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQOCix8nIGFg+wvy3BjPbVi25wYoG
K2NOHWWHpqxFuFhqvBnIC0OshIn9CtdN3JvUNHr0NIKocEwNKUGYmPwWGTfAgMB
AAGjgcEwgb4wCwYDVROPBQDAGHGMa8GAIUdEWEB/wQFMAMBaf8wHQYDVR0OBByE
FKIacs16dKAfuNDVQymSp7esf8jMG0GA1UdHwRwMGQwL6AtocUgKWh0dHA6Ly9t
c2NhlXJvb3QvQ2VydEVucm9sbFxtdc2NhlXJvb3QuY3JsMDGgL6AthitmaWx1oi8v
XFxtc2NhlXJvb3RcQ2VydEVucm9sbFxtdc2NhlXJvb3QuY3JsMEAGCSeGAQQBgjcV
AQDAGEAMA0GCSqGSIb3DQEBAUAA0EAeuZkZMX9qkoLHFETTYTpVWjZPQbBmwNRA
oJD5dydtL3BcI/ULL57EmOdYGFlyMGxuhQYx5r/o40aSqgLcBq+yg==
-----END CERTIFICATE-----
Certificate has the following attributes:
Fingerprint: D6C12961 CD78808A 4E02193C 0790082A
% Do you accept this certificate? [yes/no]:
y
Trustpoint CA certificate accepted.
% Certificate successfully imported
Router(config)#
crypto pki enroll TP
% Start certificate enrollment..
% The subject name in the certificate will be:
Router.example.com
% Include the router serial number in the subject name? [yes/no]:
n
% Include an IP address in the subject name? [no]:
n
Display Certificate Request to terminal? [yes/no]:
y
Signature key certificate request -
Certificate Request follows:
MIIBhTCB7wIBADALMSwIQUYJKoZIhvcNAQkCFhRTYW5kQmFnZ2VyLmNpc2NvLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxhdXFDFiWAn/hIZs9zfOtssKA
da0Wu0ms9Fe/Pew0ldh14vXdxgacstOs2Pr5wkjLOPxpxvx0JFwYQM6ipLmYVxv
ojhyLTrVohrh6Dnqcvk+G/5ohss9oRxvONwx042pQchFrnx9EkMuZC7evwRxjEqR
mBHBZ8GmP3jYQsjs8MCAwEEAAahMB8GCSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/
BAQDAgeAMA0GCSqGSIb3DQEBAUAA4GBAMT6WtyFw95POY7UfP+YIYhiVRUf4SCq
hRIAGrljUePLo9iTqyPU1Pnt8JnIZ5P5BHU3MfgP8sqodaWub6mubkzaohJ1qD06
O87fnLCNid5Tov5jKogFHlki2EGGZxBosUw9lJlenQdNdDPbJc5LIWdfDvcia6jo
N18rOtKnt8+
!
!
!
Redisplay enrollment request? [yes/no]:
Encryption key certificate request -
Certificate Request follows:
MIIBhTCB7wIBADALMSwIQUYJKoZIhvcNAQkCFhRTYW5kQmFnZ2VyLmNpc2NvLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAWG60QojpDbzbKnyj8FyTiOcv
THkDP7XD4vLT1XaJ409z0gSICnIcdFtXhVLBWrpg3/09zYFXrltH+BMCRQ13Lts
0IpxyA3D9iFPqev7SPXpsAlIsY8a6FMq7TiwlObqijQjLKL4cbuV0Frjl0Yuv5A/z+
kqM0m7c+pWNWFde9lsCAwEEAAahMB8GCSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/
BAQDAgUgMA0GCSqGSIb3DQEBAUAA4GBACF7feURj/fJMojpBLR6fa9Br1MJx+2F
H91YM/Cli2n4mHTeWTWKhLoT8wUfa9NGOk7yi+nF/F7035twlfq6n2bSCTW4aem
8jLMmaefFkwkrV/ceQKrcumNC1uVx+fBy9rhnx8j60XE25tnp1U08r6om/pBQABU
eNPPhozcaQ/2
!
!
!
Redisplay enrollment request? [yes/no]:
```

```
n  
Router(config)#
```

**QUESTION 536**

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

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

**Correct Answer:** CD

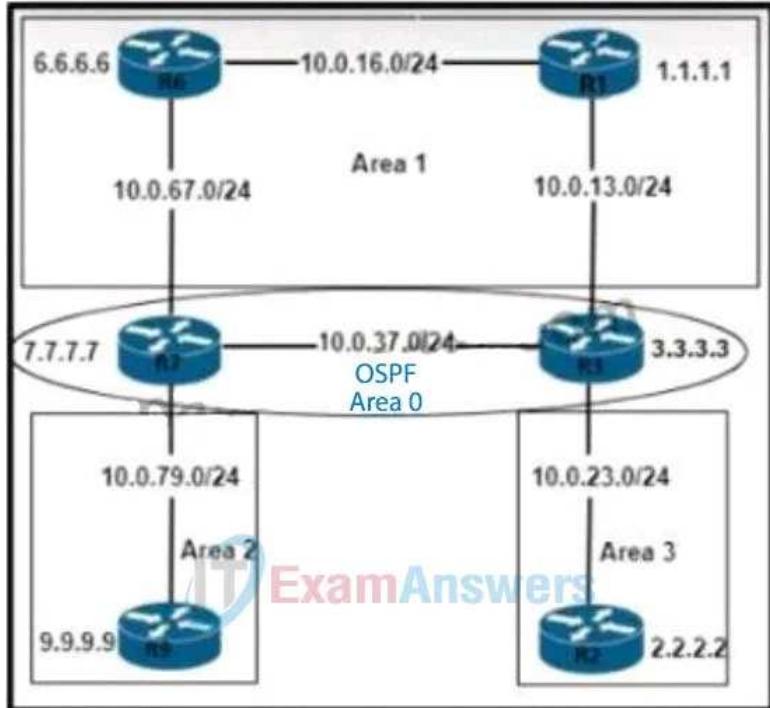
**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 537**

Refer to the exhibit. An engineer must prevent the R6 loopback from getting into Area 2 and Area 3 from Area 0. Which action must the engineer take?



- A. Apply a filter list inbound on R2 and R9
- B. Apply a filter list outbound on R3 and R7
- C. Apply a filter list outbound on R7 only.
- D. Apply a filter list inbound on R3 and R7

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

These two routers R7 (having 7.7.7.7) and R3 (having 3.3.3.3) are the ABRs which you can configure filtering.

**QUESTION 538**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 539**

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

```

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

```

#### Channel group 1

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

- 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-channel

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Gi0/0 is in hot-standby. Probably the max-bundle is set to 1 only.

#### QUESTION 540

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 541

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

```

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

```

- A. access-list acl\_subnets permit ip 10.0.32.0 0 0.0.255 log
- B. access-list acl\_subn\*ls permit ip 10.0.32.0 0.0.7.255 log
- C. access-list acl\_subnets permit ip 10.0.32.0 0.0.7.255
 access-list acl\_subnets deny ip any log
- D. access-list acl\_subnets permit ip 10.0.32.0 255.255.248.0 log

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

keyword "log" is required for generating informational log message

**QUESTION 542**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 543**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The first 24 bits will be default CISCO address i.e. 0000.0c

The next 16 bits are HSRP ID i.e. 07.ac

The next 8 bits will be the group number in hexadecimal. Decimal 16 means 10 in hexadecimal.

**QUESTION 544**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

An ETR (egress tunnel router) sends periodic Map-Register messages to all its configured map servers. The Map-Register messages contain all the EID-to-RLOC entries for the EID-numbered networks that are connected to the ETR's site.

**QUESTION 545**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Cisco StackWise Virtual provides you with the unified control and management plane architecture, so that you can manage, configure and troubleshoot two redundant Catalysts 9500 switches to function as a single logical entity in your topology.

**QUESTION 546**

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?

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

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

- A. R1(config)# router ospf 1  
R1(config-router)# network 192.168.10.0 255.255.255.0 area 0
- B. R1(config)#interface loopback0  
R1(config-if)# ip ospf 1 area 0
- C. R1(config)# interface loopback0  
R1(config-if)# ip ospf network point-to-point
- D. R1(config)# interface loopback0  
R1(config-if)# ip ospf network non-broadcast

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 547**

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

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Identity PSKs are unique pre-shared keys created for individuals or groups of users on the same SSID.

**QUESTION 548**

What does a northbound API accomplish?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 549**

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.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 550**

```
enable secret cisco
username cisco privilege 15 secret cisco
aaa new-model
aaa authentication login default group radius local
aaa authorization network default group radius
```

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 551**

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

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

- A. The router with IP 10.10.1.3 is active because it has a higher IP address
- B. If Fa0/0 is shut down, the HSRP priority on R2 becomes 80
- C. R2 Fa1/0 regains the primary role when the link comes back up
- D. R2 becomes the active router after the hold time expires.
- E. R2 is using the default HSRP hello and hold timers.

**Correct Answer:** BE

**Section:** (none)

**Explanation**

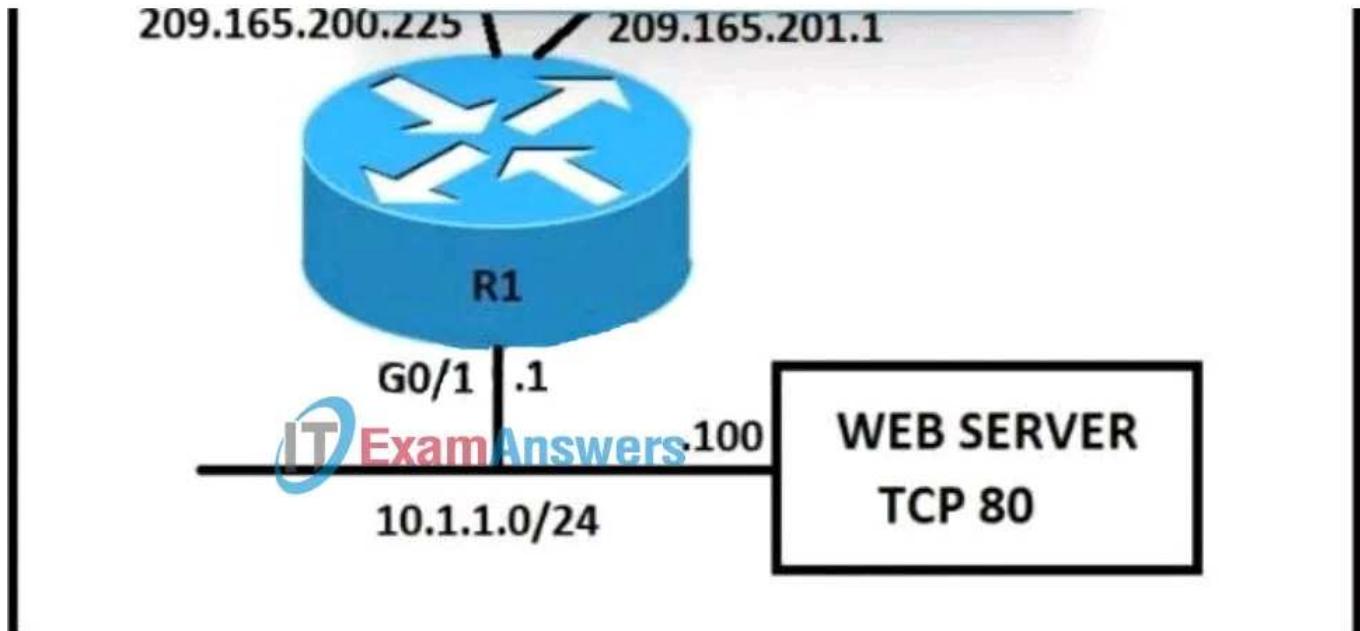
**Explanation/Reference:**

R2 is the standby router since "Standby router is local"

R2 will not become Active automatically even it has a higher priority since "Preemption disabled".  
R2 will only become Active if R1 is dead.

**QUESTION 552**

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



- A. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 extendable  
ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80 extendable
- B. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80  
ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80
- C. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80  
ip nat inside source static tcp 10.1.1.100 8080 209.165.201.1 8080
- D. p nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 no-alias  
ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80 no-alias

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The NAT extendable parameter can be used if you want to translate a private IP address to more than one public IP address.

#### QUESTION 553

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

- A. 15 dB
- B. 16 dB
- C. 18 dB
- D. 20 dB

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 554

Why would an engineer use YANG?

- A. to transport data between a controller and a network device
- B. to access data using SNMP
- C. to model data for NETCONF
- D. to translate JSON into an equivalent XML syntax

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 555

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

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

**Correct Answer:** A

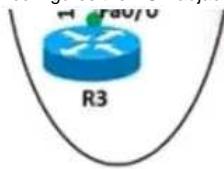
**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 556**

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



**Router R1**

```
router bgp 5500
no synchronization
bgp router-id 10.10.10.10
bgp log-neighbor-changes
network 192.168.100.0
redistribute connected
neighbor 172.16.10.2 remote-as 5500
neighbor 172.16.10.2 soft-reconfiguration inbound
neighbor 192.168.100.11 remote-as 5500
no auto-summary
!
address-family vpnv4
  neighbor 172.16.10.2 activate
  neighbor 172.16.10.2 send-community both
exit-address-family
```

```
router bgp 6500
no synchronization
bgp router-id 20.20.20.20
bgp log-neighbor-changes
neighbor 172.16.10.1 remote-as 5500
no auto-summary
!
!
address-family vpnv4
  neighbor 172.16.10.1 activate
  neighbor 172.16.10.1 send-community both
exit-address-family
address-family ipv4 vrf WAN
  redistribute connected
  redistribute static
  neighbor 172.16.10.1 remote-as 5500
  neighbor 172.16.10.1 activate
  no synchronization
exit-address-family
```

- A. Change the network statement on R1 to 172.16.10.0
- B. Change the remote-as number for 192.168.100.11.
- C. Enable synchronization on R1 and R2
- D. Change the remote-as number on R1 to 6500.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In R1:

neighbor 172.16.10.2 remote-as 5500 --> neighbor 172.16.10.2 remote-as 6500

**QUESTION 557**

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

- A. line vty 0 15
 

```
login local
    transport input none
```
- B. line vty 0 15
 

```
login local
    transport input telnet ssh
```
- C. line vty 0 15
 

```
login local
    transport input ssh
```
- D. line vty 0 15
 

```
login local
    transport input all
```

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 558**

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

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

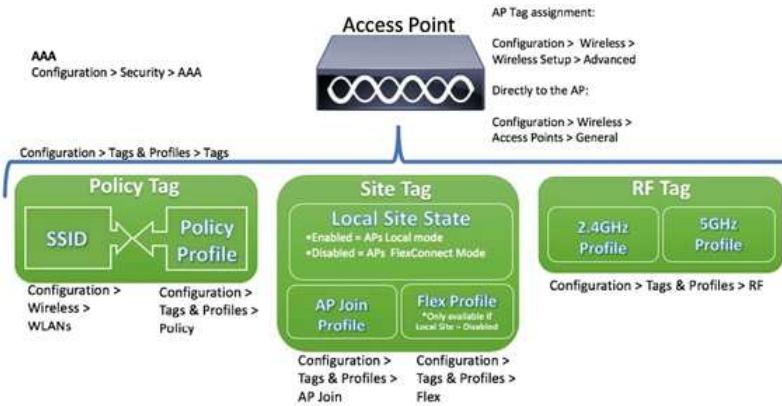
**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

On 9800 WLCs, tags are used to control the features that are available for each AP. There are three tags and various profiles can be configured under these tags.



For example:

**WLAN Profile** configures settings such as Security Settings (**PSK**, 802.1x, WebAuth), Client Association Limit ... etc.  
**Policy Profile** configures settings such as AAA, QoS ...etc.

#### QUESTION 559

What is one primary REST security design principle?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 560

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

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

**Correct Answer:** AD

**Section:** Selected

**Explanation**

**Explanation/Reference:**

OMP (Overlay Management Protocol):

The OMP protocol is a routing protocol similar to BGP that manages the Cisco SD-WAN overlay network. OMP runs inside DTLS control plane connections and carries the routes, next hops, keys, and policy information needed to establish and maintain the overlay network.

OMP runs between the Cisco vSmart Controller and the edge routers and carries only control plane information. The Cisco vSmart Controller processes the routes and advertises reachability information learned from these routes to other edge routers in the overlay network.

#### QUESTION 561

Refer to the exhibit. A network engineer is enabling logging to a local buffer, to the terminal and to a syslog server for all debugging level logs filtered by facility code 7. Which command is needed to complete this configuration snippet?

```
logging buffered discriminator Disc1
logging monitor discriminator Disc1
logging host 10.1.55.237 discriminator Disc1
```

- A. logging buffered debugging
- B. logging discriminator Disc1 severity includes 7
- C. logging buffered discriminator Disc1 debugging
- D. logging discriminator Disc1 severity includes 7 facility includes fac7

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 562

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

```

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)

```

- A. R1(config)#router bgp 65002  
R1(config-router)#neighbor 192.168.50.2 activate
- B. R1(config)#router bgp 65001  
R1(config-router)#neighbor 192.168.50.2 activate
- C. R1(config)#router bgp 65001  
R1(config-router)#no neighbor 192.168.50.2 shutdown
- D. R1(config)#router bgp 65001  
R1(config-router)#neighbor 192.168.50.2 remote-as 65001

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 563

When is the Design workflow used in Cisco DNA Center?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In networking, a greenfield deployment is the installation and configuration of a network where none existed before, for example in a new office. A brownfield deployment, in contrast, is an upgrade or addition to an existing network and uses some legacy components.

For Cisco DNA, 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.

#### QUESTION 564

A customer transitions a wired environment to a Cisco SD-Access solution. The customer does not want to integrate the wireless network with the fabric. Which wireless deployment approach enables the two systems to coexist and meets the customer requirement?

- A. Deploy the APs in autonomous mode.
- B. Deploy the wireless network over the top of the fabric.
- C. Deploy a separate network for the wireless environment.
- D. Implement a Cisco DNA Center to manage the two networks.

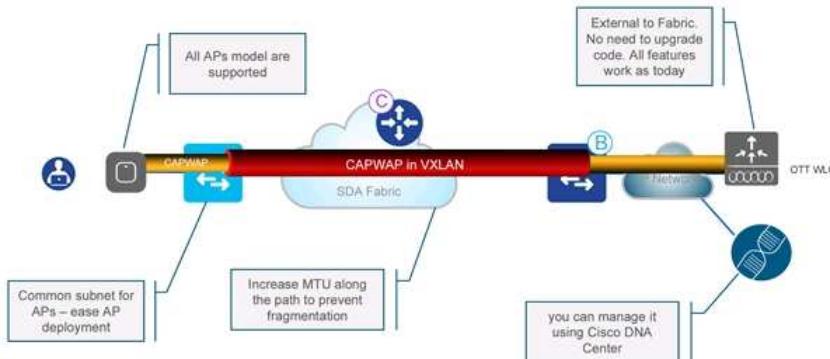
**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Wireless Over the Top (OTT) is the traditional CAPWAP deployment connected on top of a Fabric wired network. SD-Access Fabric is the transport for CAPWAP traffic. It is usually used as a migration step when a company wants to first migrate wired before wireless or a company cannot migrate wireless to Fabric immediately (e.g. needs to upgrade hardware / software).



#### QUESTION 565

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

- A. value that identifies a specific tunnel within the Cisco SD-WAN overlay

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Transport locations (TLOCs)—Identifiers that tie an OMP route to a physical location. The TLOC is the only entity of the OMP routing domain that is visible to the underlying network, and it must be reachable via routing in the underlying network. A TLOC can be directly reachable via an entry in the routing table of the physical network, or it can be represented by a prefix residing on the outside of a NAT device and must be included in the routing table. In comparison with BGP, the TLOC acts as the next hop for OMP routes.

**QUESTION 566**

Which two solutions are used for backing up a Cisco DNA Center Assurance database? (Choose two.)

- A. NFS share
- B. non-linux server
- C. local server
- D. remote server
- E. bare metal server

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 567**

What are the main components of Cisco TrustSec?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 568**

Which three resources must the hypervisor make available to the virtual machines? (Choose three.)

- A. memory
- B. bandwidth
- C. IP address
- D. processor
- E. storage
- F. secure access

**Correct Answer:** ADE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 569**

Which protocol is implemented to establish secure control plane adjacencies between Cisco SD-WAN nodes?

- A. IKF
- B. DTLS
- C. IPsec
- D. ESP

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 570**

Which benefit is realized by implementing SSO

- A. IP first-hop redundancy
- B. communication between different nodes for cluster setup
- C. physical link redundancy
- D. minimal network downtime following an RP switchover

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 571**

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

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

**Correct Answer:** AE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 572**

How do EIGRP metrics compare to OSPF metrics?

- A. EIGRP metrics are based on a combination of bandwidth and packet loss, and OSPF metrics are based on interface bandwidth.
- B. EIGRP uses the Dijkstra algorithm, and OSPF uses The DUAL algorithm.
- C. The EIGRP administrative distance for external routes is 170. and the OSPF administrative distance for external routes is undefined.
- D. The EIGRP administrative distance for external routes is 170. and the OSPF administrative distance for external routes is 110.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 573**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 574**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 575**

What is one characteristic of the Cisco SD-Access control plane?

- A. It is based on VXLAN technology.
- B. Each router processes every possible destination and route.
- C. It allows host mobility only in the wireless network.
- D. It stores remote routes in a centralized database server.

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 576**

What is the API keys option for REST API authentication?

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

- D. a credential that is transmitted unencrypted

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 577**

What is an OVF?

- A. a package that is similar to an IMG and that contains an OVA file used to build a virtual machine
- B. an alternative form of an ISO that is used to install the base operating system of a virtual machine
- C. the third step in a P2V migration
- D. a package of files that is used to describe a virtual machine or virtual appliance

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 578**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 579**

What is a characteristic of traffic policing?

- A. lacks support for marking or remarking
- B. must be applied only to outgoing traffic
- C. can be applied in both traffic directions
- D. queues out-of-profile packets until the buffer is full

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 580**

Which two Cisco SD-WAN components exchange OMP information? (Choose two.)

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

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 581**

Which type of tunnel is required between two WLCs to enable intercontroller roaming?

- A. mobility
- B. LWAPP
- C. CAPWAP
- D. iPsec

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 582**

Which protocol is responsible for data plane forwarding in a Cisco SD-Access deployment?

- A. VXLAN
- B. IS-IS
- C. OSPF
- D. LISP

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 583**

What is one main REST security design principle?

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

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

REST Security Design Principles:

- Least Privilege
- Fail-Safe Defaults
- The economy of Mechanism
- Complete Mediation
- Open Design
- Least Common Mechanism
- Psychological Acceptability

Least Privilege: An entity should only have the required set of permissions to perform the actions for which they are authorized, and no more. Permissions can be added as needed and should be revoked when no longer in use.

**QUESTION 584**

What is the recommended minimum SNR for data applications on wireless networks?

- A. 15
- B. 20
- C. 25
- D. 10

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Generally, a signal with an SNR value of 20 dB or more is recommended for data networks where as an SNR value of 25 dB or more is recommended for networks that use voice applications.

**QUESTION 585**

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

- A. economy of mechanism
- B. complete mediation
- C. separation of privilege
- D. least common mechanism

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Complete Mediation: A system should validate access rights to all its resources to ensure that they're allowed and should not rely on the cached permission matrix. If the access level to a given resource is being revoked, but that isn't reflected in the permission matrix, it would violate the security.

**QUESTION 586**

What is a characteristic of the overlay network in the Cisco SD-Access architecture?

- A. It uses a traditional routed access design to provide performance and high availability to the network.
- B. It consists of a group of physical routers and switches that are used to maintain the network.
- C. It provides isolation among the virtual networks and independence from the physical network.
- D. It provides multicast support to enable Layer 2 Hooding capability in the underlay network.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 587**

Which VXLAN component is used to encapsulate and decapsulate Ethernet frames?

- A. VNI
- B. GRE
- C. VTEP
- D. EVPN

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 588**

An engineer must configure an EXEC authorization list that first checks a AAA server then a local username. If both methods fail, the user is denied. Which configuration should be applied?

- A. aaa authorization exec default local group tacacs+
- B. aaa authorization exec default local group radius none
- C. aaa authorization exec default group radius local none
- D. aaa authorization exec default group radius local

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 589**

What is a characteristic of a vSwitch?

- A. supports advanced Layer 3 routing protocols that are not offered by a hardware switch
- B. enables VMs to communicate with each other within a virtualized server
- C. has higher performance than a hardware switch
- D. operates as a hub and broadcasts the traffic toward all the vPorts

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 590**

What is a characteristic of a Type I hypervisor?

- A. It is installed on an operating system and supports other operating systems above it.
- B. It is referred to as a hosted hypervisor.
- C. Problems in the base operating system can affect the entire system.
- D. It is completely independent of the operating system.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 591**

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

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

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Cisco® Secure Endpoint integrates prevention, detection, threat hunting, and response capabilities in a unified solution leveraging the power of cloud-based analytics.

Secure Endpoint employs a robust set of preventative technologies to stop malware, in real-time, protecting endpoints against today's most common attacks as well as emerging cyberthreats.

**QUESTION 592**

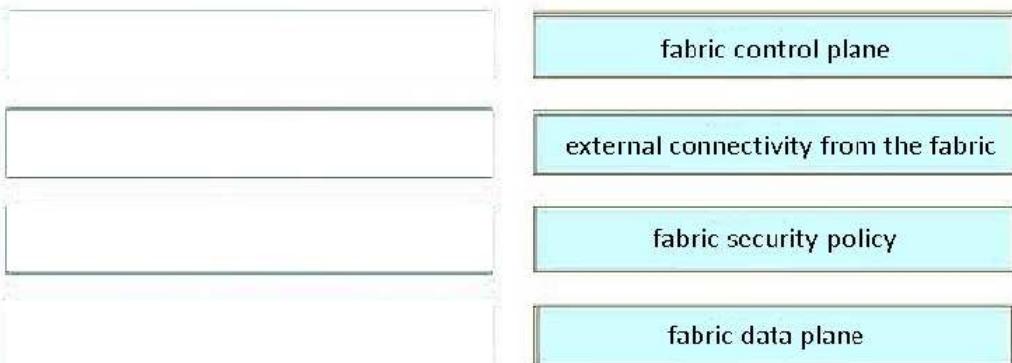
Drag and drop the Cisco SD-Access solution areas from the left onto the protocols they use on the right.

**Select and Place:**



[www.passleader.com](http://www.passleader.com)

**Correct Answer:**



[www.passleader.com](http://www.passleader.com)

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 593**

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

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

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 594**

Drag and drop the snippets onto the blanks within the code to construct a script that adds a prefix list to a route map and sets the local preference. Not all options are used.

**Select and Place:**

```
{
  "@message-id": "101",
  "edit-config": {
    "target": [
      "running"
    ],
    "config": {
      "native": {
        "ip": {
          "prefix-list": {
            "prefixes": [
              "running"
            ],
            "permit": [
              "prefix-only-list": {
                "prefix": "192.168.1.0/24"
              }
            ]
          }
        }
      }
    }
  }
}

{
  "name": "Routes",
  "route-map-without-order-seq": [
    {
      "seq_no": "10",
      "set": {
        "local-preference": "200"
      },
      "match": [
        {
          "ip": {
            "address": {
              "prefix-list": "100"
            }
          }
        }
      ]
    }
  ]
}
```

Correct Answer:

```
{
  "@message-id": "101",
  "edit-config": {
    "target": [
      "running"
    ],
    "config": {
      "native": {
        "ip": {
          "prefix-list": {
            "prefixes": [
              {
                "name": "100",
                "permit": [
                  "prefix-only-list": {
                    "prefix": "192.168.1.0/24"
                  }
                ]
              }
            ]
          }
        }
      }
    }
  }
}

{
  "name": "Routes",
  "route-map-without-order-seq": [
    {
      "seq_no": "10",
      "set": {
        "local-preference": "200"
      },
      "match": [
        {
          "ip": {
            "address": {
              "prefix-list": "100"
            }
          }
        }
      ]
    }
  ]
}
```

Section: (none)  
Explanation

**Explanation/Reference:**

**QUESTION 595**

What is one benefit of adopting a data modeling language?

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

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 596**

Which option must be used to support a WLC with an IPv6 management address and 100 Cisco Aironet 2800 Series access points that will use DHCP to register?

- A. 43
- B. 52
- C. 60
- D. 82

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

■IPv4—Cisco lightweight APs implement DHCP option 43 to supply the IPv4 management interface addresses of the primary, secondary, and tertiary wireless controllers (see the guide).

■IPv6—Cisco lightweight APs implement DHCPv6 option 52 (RFC 5417) to supply the IPv6 management interface addresses of the primary, secondary, and tertiary wireless controllers.

**QUESTION 597**

An engineer is configuring Local WebAuth on a Cisco Wireless LAN Controller. According to RFC 5737, which virtual IP address must be used in this configuration?

- A. 192.0.2.1
- B. 172.20.10.1
- C. 1.1.1.1
- D. 192.168.0.1

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

RFC 5737 : IPv4 Address Blocks Reserved for Documentation

The blocks **192.0.2.0/24** (TEST-NET-1), **198.51.100.0/24** (TEST-NET-2), and **203.0.113.0/24** (TEST-NET-3) are provided for use in documentation.

**QUESTION 598**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

HSRPv1 : 0000.0C07.AC\*\*

HSRPv2 : 0000.0C9F.F\*\*\*

Hexidecimal 20 is :  $16 \times 2 + 0 = 32$ .

**QUESTION 599**

What is one characteristic of VXLAN?

- A. It supports a maximum of 4096 VLANs.
- B. It supports multitenant segments.
- C. It uses STP to prevent loops in the underlay network.
- D. It uses the Layer 2 header to transfer packets through the network underlay.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Traditional VLAN has 4096 VLANs but VXLAN can support 16M VNIs.

VXLAN provides L2 connectivity by using L3 for transport through the underlay.

Multi-tenancy is supported by using e.g. VXLAN BGP EVPN fabric

#### QUESTION 600

In which two ways does the routing protocol OSPF differ from EIGRP? (Choose two.)

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

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

```
Router(config)#router eigrp 1
Router(config-router)#metric maximum-hops ?
<1-255> Hop count
```

#### QUESTION 601

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In IGMPv1, there is no election of an IGMP querier. If more than one device on the segment exists, all the devices send periodic IGMP queries.

On the other hand for IGMPv2, The device with the lowest IP address on the subnet is elected the IGMP querier.

#### QUESTION 602

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### WPA3-Personal: Robust, password-based authentication

- Resistant to offline dictionary attacks; stronger protections for users against password guessing attempts by third parties
- Protection even when users choose passwords that fall short of complexity recommendations
- No change to the way users connect to a network
- Provides forward secrecy; protects data traffic even if a password is later compromised

#### WPA3-Enterprise: Enterprise-grade security for sensitive data networks

- Available 192-bit cryptographic strength for networks transmitting sensitive data
- 192-bit Security suite provides additional security for networks like government and finance
- Greater consistency in application of security protocols
- Better network resiliency

#### QUESTION 603

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.

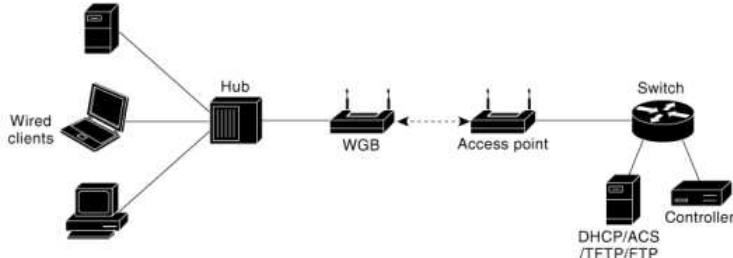
**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

A workgroup bridge (WGB) is a Cisco access point that can be configured in a mode that permits it to associate with a wireless infrastructure, providing network access on behalf of wired clients. The WGB mode is supported on autonomous IOS (Wave 1) APs and on some Wave 2 APs.



To enable the WGB to communicate with the lightweight access point, create a WLAN and make sure that Aironet IE is enabled.

**QUESTION 604**

Which function does a Cisco SD-Access extended node perform?

- A. provides fabric extension to nonfabric devices through remote registration and configuration
- B. performs tunneling between fabric and nonfabric devices to route traffic over unknown networks
- C. used to extend the fabric connecting to downstream nonfabric enabled Layer 2 switches
- D. in charge of establishing Layer 3 adjacencies with nonfabric unmanaged node

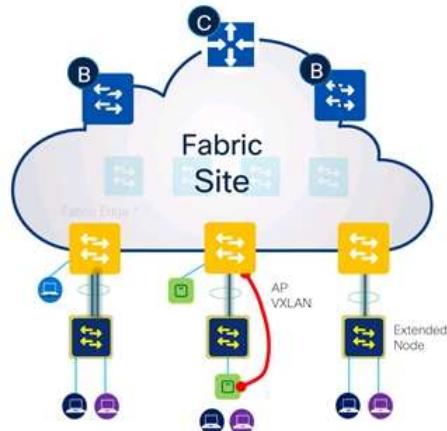
**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The Extended Enterprise network is an extension from the carpeted enterprise fabric network to its non-carpeted outdoor corridors which usually use ruggedized IE access switches / outdoor AP / other devices which can withstand the outdoor environment. Extended Nodes/Policy Extended Nodes are used for providing such extension.



**QUESTION 605**

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.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 606**

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

- Until interrupted from the keyboard, the script reads in the hostname of a device, its management IP address, operating system type, and CLI remote access protocol.
- After being interrupted, the script displays the entered entries and adds them to the JSON-formatted file, replacing existing entries whose hostname matches.

The contents of the JSON-formatted file are as follows:

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

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

Select and Place:

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

Correct Answer:

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

**Section: Selected Explanation**

**Explanation/Reference:**

**QUESTION 607**

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

Which are the characteristics of Cisco Express Forwarding (Choose two)?

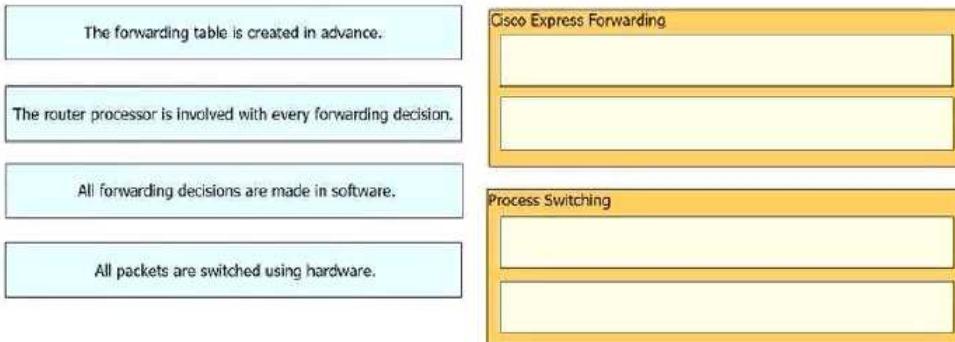
- A. The forwarding table is created in advance.
- B. The router processor is involved with every forwarding decision.
- C. All forwarding decisions are made in software.
- D. All packets are switched using hardware.

**Correct Answer: AD**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 608**

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

are the characteristics of Process Switching (Choose two)?

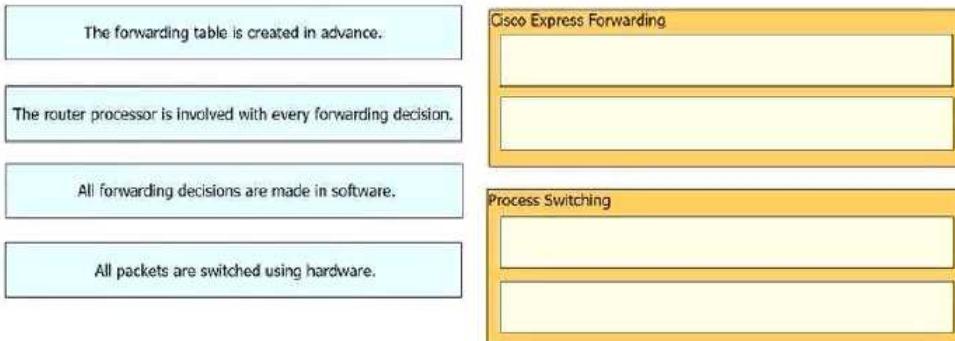
- A. The forwarding table is created in advance.
- B. The router processor is involved with every forwarding decision.
- C. All forwarding decisions are made in software.
- D. All packets are switched using hardware.

**Correct Answer: BC**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 609**

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

Characteristics for **Ansible**:

- A. provides intent-based networking feedback loop
- B. agent or agentless automation platform
- C. agentless automation platform
- D. assesses the impact of changes before applied

**Correct Answer: AC**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 610**

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

Characteristics for **Puppet**:

- A. provides intent-based networking feedback loop
- B. agent or agentless automation platform
- C. agentless automation platform
- D. assesses the impact of changes before applied

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 611**

```
SW1#show cdp neighbors | include Local|0/1
Device ID      Local Infrfce   Holdtime     Capability Platform Port ID
SW2            Fa0 0/1        131          R S WS-C3750- Fa0 0/1

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

SW2#show cdp neighbors | include Local|0/1
Device ID      Local Infrfce   Holdtime     Capability Platform Port ID
SW1            Fa0 0/1        142          R S WS-C3750- Fa0 0/1

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

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 612**

How does Protocol Independent Multicast function?

- A. In sparse mode, it establishes neighbor adjacencies and sends hello messages at 5-second intervals.
- B. It uses the multicast routing table to perform the multicast forwarding function
- C. It uses unicast routing information to perform the multicast forwarding function.
- D. It uses broadcast routing information to perform the multicast forwarding function.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 613**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The Developer Toolkit provides documentation about each API call, organized according to functional areas of the Intent API.

# Platform

Version 1.0.0 - Released 9/17/2018

[Overview](#) [Manage](#) [Developer Toolkit](#) [Runtime Dashboard](#)

## APIs

Know Your Network

### Sites

Sites

Method ▾

Name

Description

Networks

[GET](#) Get Site Health Intent

Returns Overall Health information for a site.

Devices

Clients

Site Management

### Networks

Operational Tools

Method ▾

Name

Description

Authentication

[GET](#)

Get VLAN details

Returns the list of VLAN names.

[GET](#)

Get L3 Topology Details

Returns the Layer 3 network topology details.

Returns Overall Network Health information.

**QUESTION 614**

When does a Cisco StackWise primary switch lose its role?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 615**

How do the RIB and the FIB differ?

- A. FIB contains routes learned through a dynamic routing protocol, and the RIB contains routes that are static or directly connected.
- B. RIB contains the interface for a destination, and the FIB contains the next hop information.
- C. FIB is derived from the control plane, and the RIB is derived from the data plane.
- D. RIB is derived from the control plane, and the FIB is derived from the RIB.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

RIB can also contain next hop information e.g. the IP address of the next hop router.

**QUESTION 616**

How do stratum levels relate to the distance from a time source?

- A. Stratum 1 devices are connected directly to an authoritative time source
- B. Stratum 15 devices are connected directly to an authoritative time source.
- C. Stratum 0 devices are connected directly to an authoritative time source.

D. Stratum 15 devices are an authoritative time source.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 617**

A customer deploys a new wireless network to perform location-based services using Cisco DNA Spaces. The customer has a single WLC located on-premises in a secure data center. The security team does not want to expose the WLC to the public Internet. Which solution allows the customer to securely send RSSI updates to Cisco DNA Spaces?

- A. Implement Cisco Mobility Services Engine.
- B. Replace the WLC with a cloud-based controller.
- C. Perform tethering with Cisco DNA Center.
- D. Deploy a Cisco DNA Spaces connector as a VM.

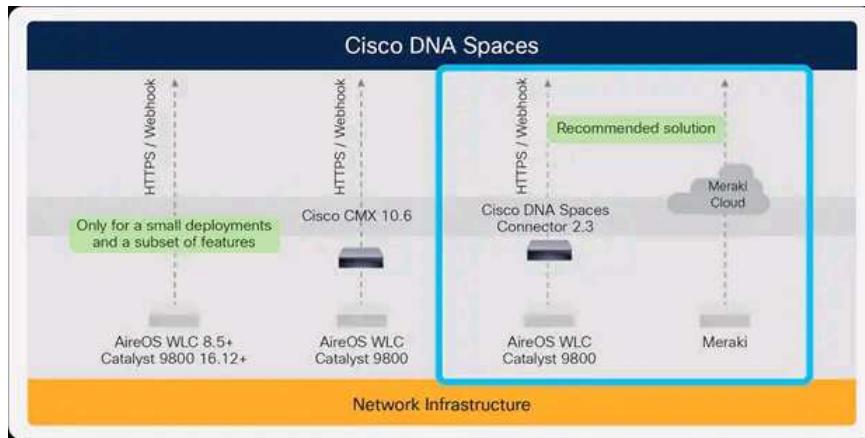
**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Cisco DNA Spaces: Detect and Locate maintains a device eviction time of 10 minutes. As long as you receive updates (RSSI, AOA, Info, Stats) from the controller, the device is kept active and is displayed on the dashboard.



**QUESTION 618**

What does a YANG model provide?

- A. standardized data structure independent of the transport protocols
- B. creation of transport protocols and their interaction with the OS
- C. user access to interact directly with the CLI of the device to receive or modify network configurations
- D. standardized data structure that can be used only with NETCONF or RESTCONF transport protocols

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

YANG can also be used by other protocols e.g.:

gNMI is gRPC Network Management Interface developed by Google. gNMI provides the mechanism to install, manipulate, and delete the configuration of network devices, and also to view operational data. The content provided through gNMI can be modeled using YANG.

gNMI is supported in e.g. Cisco IOS XE Gibraltar 16.10.x.

**QUESTION 619**

By default, which virtual MAC address does HSRP group 22 use?

- A. c0:42:01:67:05:16
- B. c0:07:0c:ac:00:22
- C. 00:00:0c:07:ac:16
- D. 00:00:0c:07:ac:22

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The last two hexadecimal digits "16" has a decimal value 22.

**QUESTION 620**

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

- A. Cisco aWIPS policies on the WLC
- B. Cisco aWIPS policies on Cisco DNA Center.

- C. Malicious rogue rules on the WLC.
- D. Malicious rogue rules on Cisco DNA Center.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The Rogue Management application in Cisco DNA Center detects and classifies threats and enables network administrators, network operators, and security operators to monitor network threats. Cisco DNA Center helps in quickly identifying the highest-priority threats and allows you to monitor these threats in the Rogue and aWIPS dashboard within Cisco DNA Assurance.

As the aWIPS functionality is integrated into Cisco DNA Center, the aWIPS can configure and monitor WIPS policies and alarms and report threats.

#### QUESTION 621

In a Cisco SD-Access wireless environment, which device is responsible for hosting the anycast gateway?

- A. fusion router
- B. control plane node
- C. fabric border node
- D. fabric edge node

**Correct Answer:** D

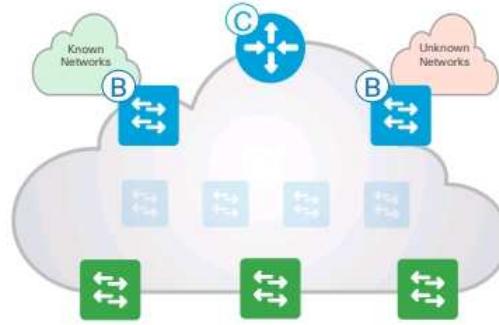
**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Edge Node** provides first-hop services for Users / Devices connected to a Fabric

- Responsible for Identifying and Authenticating Endpoints (e.g. Static, 802.1X, Active Directory)
- Register specific Endpoint ID info (e.g. /32 or /128) with the Control-Plane Node(s)
- Provide an Anycast L3 Gateway for the connected Endpoints (same IP address on all Edge nodes)
- Performs encapsulation / de-encapsulation of data traffic to and from all connected Endpoints



#### QUESTION 622

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

Which of the followings are agentless (Choose Two):

- A. Ansible
- B. Terraform
- C. Chef

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 623

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

Which of the following is Agent-based::

- A. Ansible
- B. Terraform
- C. Chef

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 624

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

Which of the following are characteristics of Cisco Express Forwarding (Choose Two):

- A. proprietary switching mechanism
- B. supports the centralized and distributed modes of operation

C. low switching performance

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 625**

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

Which of the following is the characteristic of Process Switching:

- A. proprietary switching mechanism
- B. supports the centralized and distributed modes of operation
- C. low switching performance

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 626**

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

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

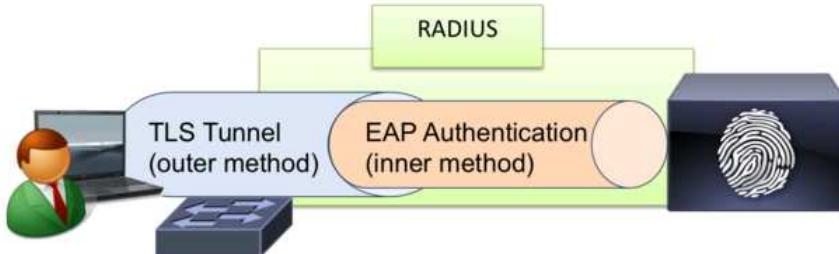
**Correct Answer:** B

**Section:** Selected

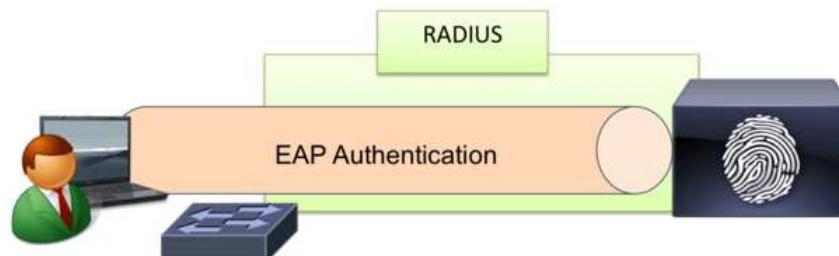
**Explanation**

**Explanation/Reference:**

Both EAP-FAST and PEAP are tunneled EAP types and can be used as the outer methods for tunneling EAP-MSCHAPv2



EAP-TLS, on the other hand, is a native EAP type that does not use tunnel:



Since there is no mentioning about the installation of certificate required by PEAP in the client, EAP-FAST is chosen as suggested answer. However, some old clients may not support EAP-FAST.

**QUESTION 627**

What are two characteristics of Cisco SD-Access elements? (Choose two.)

- A. The border node is required for communication between fabric and nonfabric devices.
- B. Traffic within the fabric always goes through the control plane node.
- C. Fabric endpoints are connected directly to the border node.
- D. The control plane node has the full RLOC-to-EID mapping database.
- E. The border node has the full RLOC-to-EID mapping database.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 628**

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

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 629**

What is the recommended minimum SNR for Voice applications for networks?

- A. 15
- B. 20
- C. 25
- D. 10

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

Achieving a packet error of one percent requires an SNR value of 25 dB or more.

**QUESTION 630**

Which two results occur if Cisco DNA center loses connectivity to devices in the SD-ACCESS fabric? (Choose two.)

- A. All devices reload after detecting loss of connection to Cisco DNA Center.
- B. Already connected users are unaffected, but new users cannot connect.
- C. User connectivity is unaffected.
- D. Cisco DNA Center is unable to collect monitoring data in Assurance.
- E. Users lose connectivity.

**Correct Answer:** CD  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 631**

Which two actions provide controlled Layer 2 network connectivity between virtual machines running on the same hypervisor? (Choose two.)

- A. Use a single trunk link to an external Layer2 switch.
- B. Use a virtual switch provided by the hypervisor.
- C. Use a virtual switch running as a separate virtual machine.
- D. Use a single routed link to an external router on stick.
- E. Use VXLAN fabric after installing VXLAN tunneling drivers on the virtual machines.

**Correct Answer:** BC  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 632**

If AP power level is increased from 25 mW to 100 mW, what is the power difference in dBm?

- A. 6 dBm
- B. 14 dBm
- C. 17 dBm
- D. 20 dBm

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**  
 $1 \text{ dBm} = 10^{\log(P/1\text{mW})}$

25mW is therefore around 14 dBm  
100mW is therefore around 20 dBm

The difference is 6 dBm.

**QUESTION 633**

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

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

D. signal strength -66 dBm, noise -90 dBm

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Only one of the following can achieve the SNR value of 25 dB or more.

- 67 - -91 = 24
- 69 - -94 = 25
- 68 - -89 = 21
- 66 - -90 = 24

**QUESTION 634**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 635**

Which activity requires access to Cisco DNA Center CLI?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 636**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

NTP is a server-client mechanism.

A node can be:

- in Server mode
- in Client mode
- in Server / Client mode.

For server mode, you can use "ntp master" or "ntp broadcast" commands in a Cisco router.

**QUESTION 637**

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

Which of the following characteristics are for Configuration Management tool:

- A. mutable infrastructure
- B. immutable infrastructure
- C. designed to provision servers
- D. designed to install and manage software on existing servers.

**Correct Answer:** AD

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Traditional server environments are mutable, in that they are changed after they are installed. Administrators are always making tweaks or adding code. CM tools evolved to manage this complexity and bring order to the configuration and updating of tens to thousands of servers. An immutable infrastructure is one in which servers are never modified after they're deployed. If something needs to be updated or changed, new servers are built afresh from a common template with the desired changes. This is the world of Terraform, where new servers replace the existing servers. This is also the philosophy of containers.

Generally, Ansible, Puppet, SaltStack, and Chef are considered to be configuration management (CM) tools and were created to install and manage software on existing server instances

Tools like Terraform are considered to be orchestrators. They are designed to provision the server instances themselves, leaving the job of configuring those servers to other tools.

	Chef	Puppet	Ansible	SaltStack	Terraform
Cloud	All	All	All	All	All
Type	Config Mgmt	Config Mgmt	Config Mgmt	Config Mgmt	Orchestration
Infrastructure	Mutable	Mutable	Mutable	Mutable	Immutable
Language	Procedural	Declarative	Procedural	Declarative	Declarative
Architecture	Client/Server	Client/Server	Client only	Client only	Client only
Orchestration					
Lifecycle (state) management	No	No	No	No	Yes
VM provisioning	Partial	Partial	Partial	Partial	Yes
Networking	Partial	Partial	Partial	Partial	Yes
Storage Management	Partial	Partial	Partial	Partial	Yes
Configuration					
Packaging	Yes	Yes	Yes	Yes	Partial <sup>1</sup>
Templating	Yes	Yes	Yes	Yes	Partial <sup>1</sup>
Service provisioning	Yes	Yes	Yes	Yes	Yes
Using CloudInit					

#### QUESTION 638

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

Which of the following characteristics are for **Orchestration** tool:

- A. mutable infrastructure
- B. immutable infrastructure
- C. designed to provision servers
- D. designed to install and manage software on existing servers.

**Correct Answer:** BC

**Section:** Selected

**Explanation**

#### Explanation/Reference:

Traditional server environments are mutable, in that they are changed after they are installed. Administrators are always making tweaks or adding code. CM tools evolved to manage this complexity and bring order to the configuration and updating of tens to thousands of servers. An immutable infrastructure is one in which servers are never modified after they're deployed. If something needs to be updated or changed, new servers are built afresh from a common template with the desired changes. This is the world of Terraform, where new servers replace the existing servers. This is also the philosophy of containers.

Generally, Ansible, Puppet, SaltStack, and Chef are considered to be configuration management (CM) tools and were created to install and manage software on existing server instances

Tools like Terraform are considered to be orchestrators. They are designed to provision the server instances themselves, leaving the job of configuring those servers to other tools.

	Chef	Puppet	Ansible	SaltStack	Terraform
Cloud	All	All	All	All	All
Type	Config Mgmt	Config Mgmt	Config Mgmt	Config Mgmt	Orchestration
Infrastructure	Mutable	Mutable	Mutable	Mutable	Immutable
Language	Procedural	Declarative	Procedural	Declarative	Declarative
Architecture	Client/Server	Client/Server	Client only	Client only	Client only
Orchestration					
Lifecycle (state) management	No	No	No	No	Yes
VM provisioning	Partial	Partial	Partial	Partial	Yes
Networking	Partial	Partial	Partial	Partial	Yes
Storage Management	Partial	Partial	Partial	Partial	Yes
Configuration					
Packaging	Yes	Yes	Yes	Yes	Partial <sup>1</sup>
Templating	Yes	Yes	Yes	Yes	Partial <sup>1</sup>
Service provisioning	Yes	Yes	Yes	Yes	Yes
Using CloudInit					

#### QUESTION 639

```

Switch1#show run interface Gi0/0      Switch2#show run interface Gi0/0
!
interface GigabitEthernet0/0          interface GigabitEthernet0/0
  switchport trunk encapsulation dot1q   negotiation auto
  switchport mode trunk                channel-group 1 mode active
  negotiation auto                   end
  channel-group 1 mode active
end

switch1#show run interface Gi0/1      switch2#show run interface Gi0/1
!
interface GigabitEthernet0/1          interface GigabitEthernet0/1
  switchport trunk encapsulation dot1q   negotiation auto
  switchport mode trunk                channel-group 1 mode passive
  negotiation auto                   end
  channel-group 1 mode passive
end

```

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since g0/1 on both switches are passive, you need to configure either one (or both) to be active.

#### QUESTION 640

```

Router#show policy-map control-plane
Control Plane

Service-policy input: CoPP

Class-map: class-telnet (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: access-group 100
  police:
    cir 1000000 bps, bc 3125 bytes
    conformed 0 packets, 0 bytes; actions:
      transmit
    exceeded 0 packets, 0 bytes; actions:
      drop
    conformed 0 bps, exceed 0 bps

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

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

```

Refer to the exhibit. Which commands are required to allow SSH connections to the router?

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

**Correct Answer:** A

**Section: (none)****Explanation****Explanation/Reference:**

Only A is a correct configuration.

For others, one of the following errors / unreasonable setting can be found:

- In the Policy map, action is specified without specifying a class.
- ACL no 10 is a standard ACL and cannot specify "tcp". Port 22 should be set as destination port instead of source port.
- ACL being configured is 100 but the class-map uses the access list number 10.

Remarks :

There are many strange things in this question.

- No sure why there are obvious errors of having ACL number 10 in the choices.
- Even without any additional configuration, SSH traffic is allowed through the class "class-default". The only existing problem that may exist is that SSH traffic is not rate limited.
- In the only correct configuration i.e. the suggested answer, there is no need to add SSH traffic to both ACL 100 and 101. Since class "class-telnet" is configured first and ACL 100 can also match SSH traffic after adding new configuration. Both telnet and SSH traffic will share the bandwidth 100000 configured for this class. The new class "class-ssh" will never be matched.

**QUESTION 641**

With the maximum power level assignment for global TPC 802.11a/n/ac is configured to 10 dBm. which power level effectively doubles the transmit power?

- A. 13 dBm
- B. 14 dBm
- C. 17 dBm
- D. 20 dBm

**Correct Answer: A**

**Section: (none)****Explanation****Explanation/Reference:**

Since  $1 \text{ dBm} = 10^{\log(P/1\text{mW})}$ :

$$10 \text{ dBm} = 10^{\log(P/1\text{mW})}$$

$$P = 10 * 1\text{mW} = 10\text{mW}$$

Doubling power means 20mW which is the same as 13dBm.

OR

Since  $10^{\log(P/1\text{mW})} = 10\text{dBm}$ :

$$10^{\log(2P/1\text{mW})} = 10^{\log(P/1\text{mW})} + 10^{\log(2/1\text{mW})} = 10^{\log(P/1\text{mW})} + 10^{\log 2} = 10^{\log(P/1\text{mW})} + 0.3 = 10 + 0.3 \text{ dBm.}$$

**QUESTION 642**

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

The characteristics for EIGRP (choose two):

- A. maintains alternative loop-free backup path if available.
- B. quickly computes new path upon link failure
- C. selects routes using the DUAL algorithm

**Correct Answer: AC**

**Section: (none)****Explanation****Explanation/Reference:****QUESTION 643**

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

The characteristics for OSPF:

- A. maintains alternative loop-free backup path if available.
- B. quickly computes new path upon link failure
- C. selects routes using the DUAL algorithm

**Correct Answer: B**

**Section: (none)****Explanation****Explanation/Reference:****QUESTION 644**

Line protocol on Interface Port-channel10, changed state to doxvn  
 Gi0/1 suspended: LACP currently not enabled on the remote port.  
 Gi0/0 suspended: LACP currently not enabled on the remote port.

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

- A. SW2(config-if)#channel-group 10 mode on
- B. SW1(config-if)#channel-group 10 mode active
- C. SW1(config-if)#channel-group 10 mode desirable
- D. SW2(config-if)#switchport mode trunk

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

For using LACP to negotiate Ethernet Channel, you need to configure Active or Passive mode.

**QUESTION 645**

**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

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since it is a hidden SSID Wireless Network (i.e. SSID is not being broadcast), you need to check the box "Connect even if this network is not broadcasting".

**QUESTION 646**

General		Security	QoS	Policy Mapping	Advanced
Profile Name:	Cisco				
Type:	WLAN				
SSID:	Cisco				
Status:	<input checked="" type="checkbox"/> Enabled				
Security Policies:	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)				
Radio Policy:	All				
Interface/Interface Group(G):	management				
Multicast Vlan Feature:	<input type="checkbox"/> Enabled				
Broadcast SSID:	<input checked="" type="checkbox"/> Enabled				
NAS-ID:	none				

Refer to the exhibit Clients report that they cannot connect to this SSID using the provided PSK. Which action will resolve this issue?

- A. Apply the correct interface to this WLAN
- B. Define the correct Radio Policy.
- C. Apply the changes to this SSID.
- D. Select the PSK under authentication key management

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since Security Policies shows "[WPA2][Auth(802.1X)]", it requires user name and password authentication. You need to enable PSK in order to use PSK password for authentication.

**Remarks:**

The following diagram is an example of the required setting:

**General Security QoS Policy-Mapping Advanced**

**Layer 2 Layer 3 AAA Servers**

**Layer 2 Security**: WPA+WPA2   
 MAC Filtering

**Fast Transition**  
 Fast Transition  
 Over the DS  
 Reassociation Timeout: 20 Seconds

**Protected Management Frame**  
 PMF: Disabled

**WPA+WPA2 Parameters**  
 WPA Policy  
 WPA2 Policy-AES

**Authentication Key Management**  
 802.1X:  Enable  
 CCKM:  Enable  
 PSK:  Enable ←

**QUESTION 647**

```
enable secret cisco
aaa new-model
```

```
tacacs server ise-1
address 10.1.1.1
key cisco123!
```

```
tacacs server ise-2
address 10.2.2.1
key cisco123!
```

```
aaa group server tacacs+ ISE-Servers
server name ise-1
server name ise-2
```

Refer to the exhibits A network engineer must configure the router to use the ISE.Servers group for authentication. If both ISE servers are unavailable, the local usermame database must be used. If no usernames are defined in the configuration, then the enable password must be the last resort to log in. Which configuration must be applied to achieve this result?

- A. aaa authentication login default group enable local ISE-Servers
- B. aaa authorization exec default group ISE-Servers local enable
- C. aaa authentication logon default group ISE-Servers local enable
- D. aaa authentication login error-enable
 

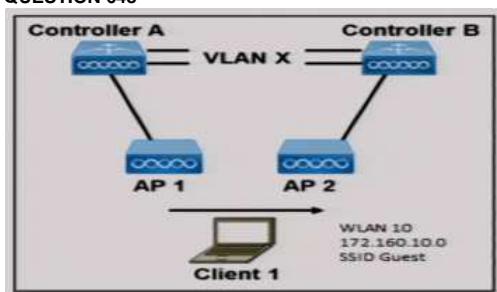
```
aaa authentication login default group enable local ISE-Servers
```

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 648**


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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 649**

The following system log message is presented after a network administrator configures a GRE tunnel:

```
Interface Tunnel 0 temporarily disabled due to recursive routing
```

Why is Tunnel 0 disabled?

- A. Because dynamic routing is not enabled.
- B. Because the tunnel cannot reach its tunnel destination.
- C. Because the best path to the tunnel destination is through the tunnel itself.
- D. Because the router cannot recursively identify its egress forwarding Interface.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 650**

Which outcome is achieved with this Python code?

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

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

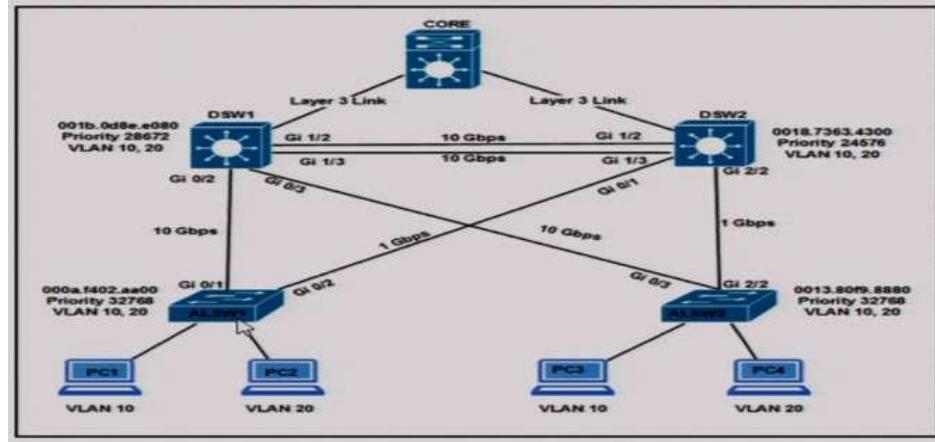
**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 651**



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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since DSW2 has the lowest priority, it is elected as root bridge.

For ALSW1, it has two path to the root bridge DSW2:

- from its g0/1 through DSW1 using two 10Gbps links. This has a cost path of 2 + 2.
- from its g0/2 directly using one 1Gbps links. This has a cost path of 4.

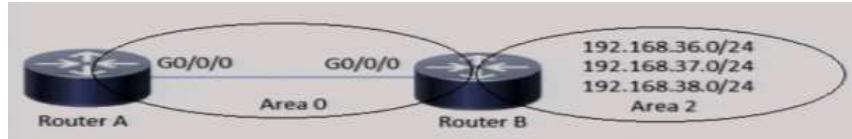
Since both have a path cost of 4, the path connecting to the lowest Bridge ID (bridge priority + MAC) will be used for root port. Since DSW2 is the root bridge which is the one having the lowest bridge priority, ALSW1's g0/2 will be the root port and its g0/1 will be blocked.

Therefore traffic from PC1 will go through ALSW1 and then DSW2 in order to reach DSW1.

### Remarks:

CORE is connecting to others with layer 3 links and therefore does not participate in spanning tree.

## QUESTION 652



Refer to the exhibit. Which configuration is required to summarize the Area 2 networks that are advertised to Area 0?

- A. RouterB(config)# router ospf 1  
RouterB(config-router)# area 2 range 192.168.36.0 255.255.252.0
  - B. RouterB(config)# router ospf 1  
RouterB(config-router)# network 192.168.36.0 255.255.252.0
  - C. RouterB(config)# router ospf 1  
RouterB(config-router)# network 192.168.36.0 255.255.255.0
  - D. RouterB(config)# router ospf 1  
RouterB(config-router)# area 2 range 192.168.36.0 255.255.255.0

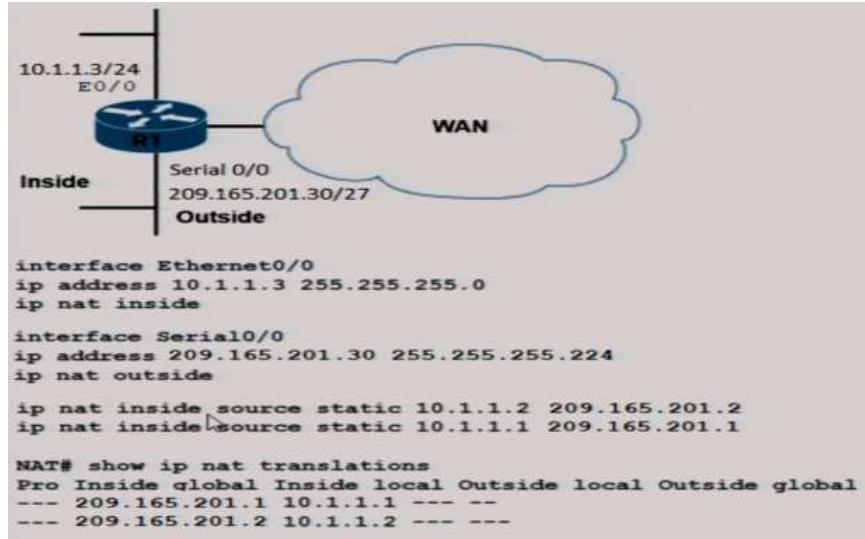
**Correct Answer:** A

**Section: (none)**

## Explanation

### **Explanation/Reference:**

## QUESTION 653



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

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

**Correct Answer:** AD

**Section: (none)**

## Explanation

### **Explanation/Reference:**

**QUESTION 654**

A network engineer is configuring OSPF on a router. The engineer wants to prevent having a route to 172.16.0.0/16 learned via OSPF in the routing table and configures a prefix list using the command `ip prefix-list OFFICE seq 6 deny 172.16.0./16`. Which two additional configuration commands must be applied to accomplish the goal? (Choose two.)

- A. ip prefix-list OFFICE seq 10 permit 0.0.0.0/0 le 32
  - B. distribute-list OFFICE out under the OSPF process
  - C. distribute-list OFFICE in under the OSPF process
  - D. distribute-list prefix OFFICE in under the OSPF process
  - E. ip prefix-list OFFICE seq 10 permit 0.0.0.0/0 ge 32

**Correct Answer:** AD

**Section: (none)**

## Explanation

### Explanation/Reference:

By default "distribute-list" accepts an ACL. You need to include the keyword "prefix" in order to specify a prefix-list.

## QUESTION 655

Based on the routers API output in JSON format below, which Python code will display the value of the "role" key?

```
"response": [{}  
"family": "Routers",  
"macAddress": "00:c8:8b:80:bb:00",  
"hostname": "BorderA",  
"role": "BORDER ROUTER",  
"lastUpdateTime": "111111111111",  
"serialNumber": "XXXXXXXX",  
"softwareVersion": "16-3.2",  
"uptime": "5 days, 1:22:33:44",  
"lastUpdated": "2000-01-01 11:22:33"  
}]
```

- A. `json_data = json.loads(response.text)  
print(json_data[response][0][role])`
- B. `json_data = json.loads(response.text)  
print(json_data["response"]["family"]["role"])`
- C. `json_data = response.json()  
print(json_data["response"]["family"]["role"])`
- D. `json_data = response.json()  
print(json_data["response"][0]["role"])`

**Correct Answer: D**

**Section: (none)**

**Explanation**

### Explanation/Reference:

The data in "response" is enclosed by "[]" which is a List in Python. Therefore, you need to specify a "0" to get the first element before you can access the "role" in this element. Moreover, the field name has to be enclosed by "".

## QUESTION 656

A network engineer must configure a switch to allow remote access for all feasible protocols. Only a password must be requested for device authentication and all idle sessions must be terminated in 30 minutes. Which configuration must be applied?

- A. `username cisco privilege 15 cisco  
line vty 0 15  
transport input telnet ssh  
login local  
exec-timeout 0 30`
- B. `line console 0  
password cisco  
exec-timeout 30 0`
- C. `line vty 0 15  
password cisco  
transport input all  
exec-timeout 0 30`
- D. `line vty 0 15  
password cisco  
transport input telnet ssh  
exec-timeout 30 0`

**Correct Answer: D**

**Section: (none)**

**Explanation**

### Explanation/Reference:

Since only password must be requested, you cannot use username/password for authentication.

```
R1(config-line)#exec-timeout ?  
<0-35791> Timeout in minutes  
  
R1(config-line)#exec-timeout 30 ?  
<0-2147483> Timeout in seconds  
<cr>  
  
R1(config-line)#+
```

## QUESTION 657

R1	R2
<pre>key chain ciscol23 Key 1 key-string Cisco123:  Ethernet0/0 - Group 10 State is Active 9 state changes, last state change 00:02:49 Virtual IP address is 192.168.0.1 Active virtual MAC address is 0000.0c07.ac0a Local virtual MAC address is 0000.0c07.ac0a (vl default) Hello time 5 sec, hold time 15 sec Next hello sent in 2.880 secs Authentication MD5, key-chain "ciscol23" Preemption enabled Active router is local Standby router is unknown Priority 255 (configured 255) Group name is "workstation-group" (cfgd)</pre>	<pre>key chain ciscol23 Key 1 key-string Cisco123:  Ethernet0/0 - Group 10 State is Active 17 state changes, last state change 00:02:17 Virtual IP address is 192.168.0.1 Active virtual MAC address is 0000.0c07.ac0a Local virtual MAC address is 0000.0c07.ac0a (vl default) Hello time 10 sec, hold time 30 sec Next hello sent in 6.720 secs Authentication MD5, Key-chain "ciscol23" Preemption disabled Active router is local Standby router is unknown Priority 200 (configured 200) Group name is "workstation-group" (cfgd)</pre>

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Similar to Q365, the string in one router has an uppercase "C" while the string in the other router has a lowercase "c".

#### QUESTION 658

An engineer must configure a router to leak routes between two VRFs. Which configuration must the engineer apply?

- A. ip access-list extended acl-to-red  
    permit ip any 10.1.1.0 0.0.0.255  
    route-map rm-to-red permit 10  
        match ip address 50  
    ip vrf RED  
        rd 1:1  
        import ipv4 unicast map rm-to-red
- B. ip access-list extended acl-to-red  
    permit ip 10.1.1.0 0.0.0.255 any  
    route-map rm-to-red permit 10  
        match ip address acl-to-red  
    ip vrf RED  
        rd 1:1  
        import ipv4 unicast route-map rm-to-red
- C. ip access-list extended acl-to-red  
    permit ip 10.1.1.0 0.0.0.255 any  
    route-map rm-to-red permit 10  
        match ip address acl-to-red  
    ip vrf RED  
        rd 1:1  
        import ipv4 unicast map rm-to-red
- D. ip access-list extended acl-to-red  
    permit ip 10.1.1.0 0.0.0.255 any  
    route-map rm-to-red permit 10  
        match ip address acl-to-red  
    ip vrf RED  
        rd 1:1  
        import ipv4 unicast acl-to-red

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

There is a way to import / leak a route by using the "import" command under a VRF configuration through the use of a Route Map. The basic syntax is:

```
R1(config)#ip vrf RED
R1(config-vrf)#rd 1:1
R1(config-vrf)#import ipv4 unicast map ?
WORD    VRF import route-map name
```

The other answer having the correct syntax in the "import" command is actually a wrong answer since it is using the access number "50" but the configured ACL is actually a named ACL.

#### QUESTION 659

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Fabric Wireless LAN Controller – The Wireless LAN Controller (WLC) provides centralized access point (AP) image and configuration management and client session management. The WLC integrates and communicates with the fabric Control Plane Node to provide mobility services for endpoints attached to fabric Access Points.

#### QUESTION 660

```
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.)

- A. R1(config)\$control-plane
 R1(config-cp)#service-policy output POLICY-CoPP

B. 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

C. R1(config-pmap)#class CLASS-COPP-Management  
R1(config-pmap-c)#police 32 conform-action transmit exceed-action drop violate-action transmit

D. 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

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

**Correct Answer:** BE

**Section:** (none)

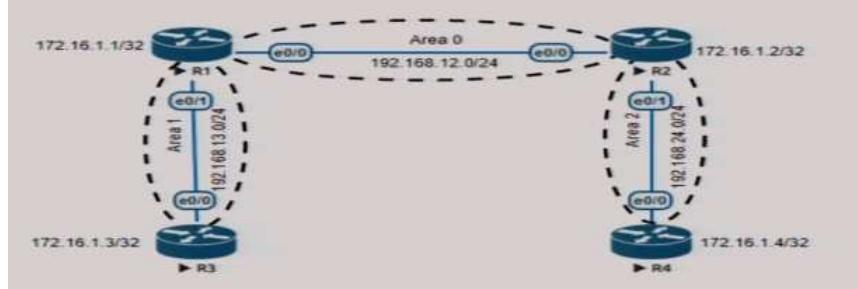
**Explanation**

**Explanation/Reference:**

For limiting CPU usage, you need to configure input CoPP.

For the two choices with the correct "police 320000 ..." commands, their differences is in "exceed-action". For "transmit" in "exceed-action", occassionally burst traffic over 320 kbps is allowed but continuous exceeded will be blocked by "violate-action drop".

**QUESTION 661**



Refer to the exhibit. An engineer must create a configuration that prevents R3 from receiving the LSA about 172.16.1.4/32. Which configuration achieves this goal?

- A. On R3  
`ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32  
ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32`
- `router ospf 200  
area 1 filter-list prefix INTO-AREA1 in`
- B. on R1  
`ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32  
ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32`
- `router ospf 200  
area 1 filter-list prefix INTO-AREA1 out`
- C. On R3  
`ip access-list standard R4_L0  
deny host 172.16.1.4  
permit any`
- `router ospf 200  
distribute-list R4_L0 in`
- D. on R1  
`ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32  
ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32`
- `router ospf 200  
area 1 filter-list prefix INTO-AREA1 in`

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Interarea OSPF routes can only be filtered in an ABR. Therefore you cannot configure it in R3.

Moreover, you can only filter interarea routes when it is leaving or entering a different area. Since R1 and R3 are in the same area 1, you cannot filter an interarea route when R1 is sending routes to R3. Therefore you can only filter the route " 172.16.1.4/3" when it enters Area 1 at R1 i.e. performing filtering for inbound direction.

**QUESTION 662**

Which definition describes JWT in regard to REST API security?

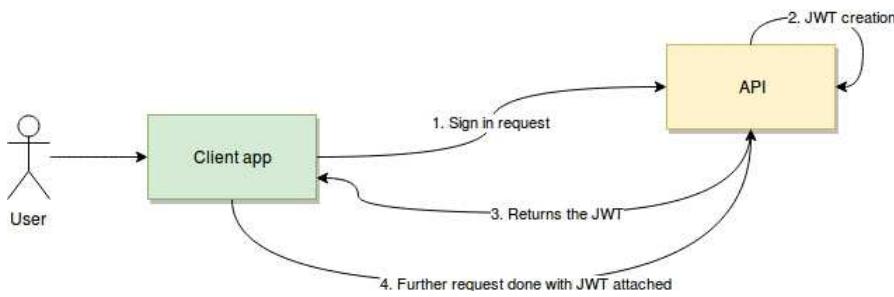
- A. an encrypted JSON token that is used for authentication
- B. an encrypted JSON token that is used for authorization
- C. an encoded JSON token that is used to securely exchange information
- D. an encoded JSON token that is used for authentication

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**



The JSON Web Token returned by the API to the client app is signed using a secret key. Encryption is optional.

#### QUESTION 663

```

Router# show running-config
.....
username cisco password 0 cisco
aaa authentication login group1 group radius line
aaa authentication login group2 group radius local
aaa authentication login group3 group radius none

line con 0
password 0 cisco123
login authentication group1

line aux 0
login authentication group3

line vty 0 4
password 0 test123
login authentication group3

```

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

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

**Correct Answer:** A

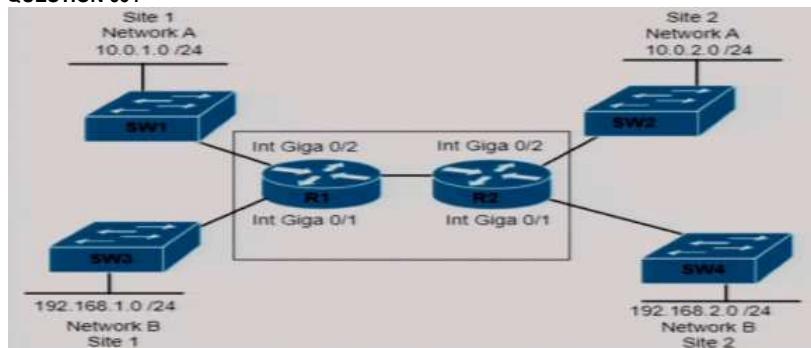
**Section:** (none)

**Explanation:**

#### Explanation/Reference:

"line con 0" is configured with authentication-list "group1" which uses RADIUS and then line password.  
Hence the line password configured in "line con 0" can be used if RADIUS is not available.

#### QUESTION 664



Refer to the exhibit, which set of commands is required to configure and verify the VRF for Site 1 Network A on router R1?

- A. R1#(config)#ip vrf 100
 

```
R1#(config-vrf)#rd 100:1
R1#(config-vrf)#address family ipv4
!
R1(config)#interface Gi0/2
R1(config-if)#ip address 10.0.1.1 255.255.255.0
```
- B. R1#(config)#ip vrf 100
 

```
!
R1(config)#interface Gi0/2
R1(config-if)#ip address 10.0.1.1 255.255.255.0
```
- C. R1#(config)#ip vrf 100
 

```
!
R1(config)#interface Gi0/2
R1(config-if)#ip vrf forwarding 100
R1(config-if)#ip address 10.0.1.1 255.255.255.0
```

R1#show ip vrf

```

D. R1#(config)#ip vrf 100
!
R1(config)#interface Gi0/2
R1(config-if)#ip address 10.0.1.1 255.255.255.0
R1#show ip vrf

```

**Correct Answer: C**  
**Section: (none)**  
**Explanation**

**Explanation/Reference:**

#### QUESTION 665

```

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

```

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

- A. monitor session 12 type erspan-destination
 

```

      destination interface GigabitEthernet4
      source
        erspan-id 11
        ip address 10.10.10.10
      
```
- B. monitor session 11 type erspan-destination
 

```

      destination interface GigabitEthernet4
      source
        erspan-id 12
        ip address 10.100.10.10
      
```
- C. monitor session 12 type erspan-destination
 

```

      destination interface GigabitEthernet4
      source
        erspan-id 12
        ip address 10.10.10.10
      
```
- D. monitor session 11 type erspan-destination
 

```

      destination interface GigabitEthernet4
      source
        erspan-id 11
        ip address 10.10.10.10
      
```

**Correct Answer: C**  
**Section: (none)**  
**Explanation**

**Explanation/Reference:**

For the other side receiving the monitoring traffic, the source should be:

- using the same IP address as that configured as the destination i.e. "10.10.10.10" configured in the traffic source. This is the IP address of the device getting the monitoring traffic (e.g. a PC running wireshark).
- using the same ERSPAN ID as that configured as destination i.e. "12" configured in the traffic source.

The session number does not need to match with the ERSPAN ID.

#### QUESTION 666

```

Router#sh access-list
Extended IP access list 100
  10 permit tcp any any eq telnet
Extended IP access list 101
  10 permit tcp any any eq 22

```

Refer to the exhibit. Which configuration set implements Control Plane Policing for SSH and Telnet?

- A. Router(config)#class-map match-any class-control
 

```

      Router(config-cmap)#match access-group 100
      Router(config-cmap)#match access-group 101
      Router(config)#policy-map CoPP
      Router(config-pmap)#class class-control
      Router(config-pmap-c)#police 1000000 conform-action transmit
      Router(config)#control-plane
      Router(config-cp)#service-policy input CoPP
      
```
- B. Router(config)#class-map match-all class-control
 

```

      Router(config-cmap)#match access-group 100
      Router(config-cmap)#match access-group 101
      Router(config)#policy-map CoPP
      Router(config-pmap)#class class-control
      Router(config-pmap-c)#police 1000000 conform-action transmit
      Router(config)#control-plane
      Router(config-cp)#service-policy output CoPP
      
```
- C. Router(config)#class-map type inspect match-all
 

```

      Router(config-cmap)#match access-group 100
      Router(config-cmap)#match access-group 101
      Router(config)#policy-map CoPP
      Router(config-pmap)#class class-control
      Router(config-pmap-c)#police 1000000 conform-action transmit
      Router(config)#control-plane
      Router(config-cp)#service-policy output CoPP
      
```
- D. Router(config)#class-map class-telnet
 

```

      Router(config-cmap)#match access-group 100
      Router(config)#class-map class-ssh
      Router(config-cmap)#match access-group 101
      Router(config)#policy-map CoPP
      Router(config-pmap)#class class-telnet-ssh
      
```

```
Router(config-pmap-c)#police 1000000 conform-action transmit
Router(config)#control-plane
Router(config-cp)#service-policy input CoPP
```

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

For controlling SSH and Telnet to the router, the policy map has to be applied as input. Moreover, since a packet cannot be of both telnet and SSH types at the same time, the class map will the two ACL must be configured as "match-any".

Note that the choice using the class "class-telnet-ssh" is wrong since this class map name has not be defined.

**QUESTION 667**

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

- A. class-map match-all CoPP\_SSH  
match access-group name CoPP\_SSH

```
!
policy-map CoPP_SSH
class CoPP_SSH
police cir 100000
exceed-action drop
!
!
!
interface GigabitEthernet0/1
ip address 209.165.200.225 255.255.255.0
ip access-group EGRESS out
duplex auto
speed auto
media-type rj45
service-policy input CoPP_SSH
!
ip access-list extended CoPP_SSH
permit tcp any any eq 22
!
```

- B. class-map match-all CoPP\_SSH  
match access-group name CoPP\_SSH

```
!
policy-map CoPP_SSH
class CoPP_SSH
police cir CoPP_SSH
exceed-action drop
!
!
!
interface GigabitEthernet0/1
ip address 209.165.200.225 255.255.255.0
ip access-group EGRESS out
duplex auto
speed auto
media-type rj45
service-policy input CoPP_SSH
!
ip access-list extended CoPP_SSH
deny tcp any any eq 22
!
```

- C. class-map match-all CoPP\_SSH  
match access-group name CoPP\_SSH

```
!
policy-map CoPP_SSH
class CoPP_SSH
police cir 100000
exceed-action drop
!
!
!
control-plane
service-policy input CoPP_SSH
!
ip access-list extended CoPP_SSH
permit tcp any any eq 22
!
```

- D. class-map match-all CoPP\_SSH  
match access-group name CoPP\_SSH

```
!
policy-map CoPP_SSH
class CoPP_SSH
police cir 100000
exceed-action drop
!
!
!
control-plane transit
service-policy input CoPP_SSH
!
ip access-list extended CoPP_SSH
permit tcp any any eq 22
!
```

**Correct Answer:** C

**Section:** (none)

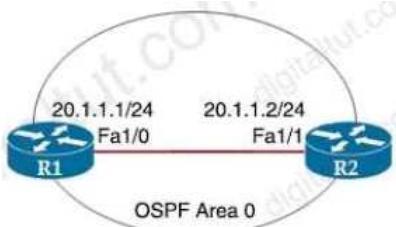
**Explanation**

**Explanation/Reference:**

Similar to Q204. However, since the access list for using for control plane policy can match SSH traffic (permit instead of deny in Q204), Control Plane policy is preferred than policy applied in the interface.

**QUESTION 668**

Refer to the exhibit



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

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

- A. network 20.0.0.2 0.0.0.0 area 0
- B. network 20.0.0.2 0.0.0.3 area 0
- C. network 20.1.1.2 0.0.0.0 area 0
- D. network 20.1.1.0 0.0.0.0 area 0

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Same it is the amended question for Q184. In this question, only C is the correct answer.

**QUESTION 669**

An engineer must configure an ACL that permits packets which include an ACK in the TCP header. Which entry must be included in the ACL?

- A. access-list 110 permit tcp any any eq 21 tcp-ack
- B. access-list 10 permit tcp any any eq 21 established
- C. access-list 110 permit tcp any any eq 21 established
- D. access-list 10 permit tcpp any any eq 21 tcp-ack

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Others are not correct since:

- "tcp-ack" does not exist (only "ack" is available)
- ACL number 10 is a standard ACL which does not support specifying of protocol "tcp".

**QUESTION 670**

```

R1#show policy-map control-plane
Control Plane

Service-policy output: CoPP

Class-map: SNMP-Out (match-all)
  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

```

Refer to the exhibit. 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 generated by R1 that matches access list SNMP is policed.
- D. Traffic passing through R1 that matches access list SNMP is policed.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since the policy is applied as "output", it controls the traffic generated by the router itself.

#### QUESTION 671

What is one difference between EIGRP and OSPF?

- A. EIGRP uses the variance command for unequal cost load balancing, and OSPF supports unequal cost balancing by default.
- B. OSPF is a Cisco proprietary protocol, and EIGRP is an IETF open standard protocol.
- C. OSPF uses the DUAL distance vector algorithm, and EIGRP uses the Dijkstra link-state algorithm.
- D. EIGRP uses the DUAL distance vector algorithm, and OSPF uses the Dijkstra link-state algorithm.

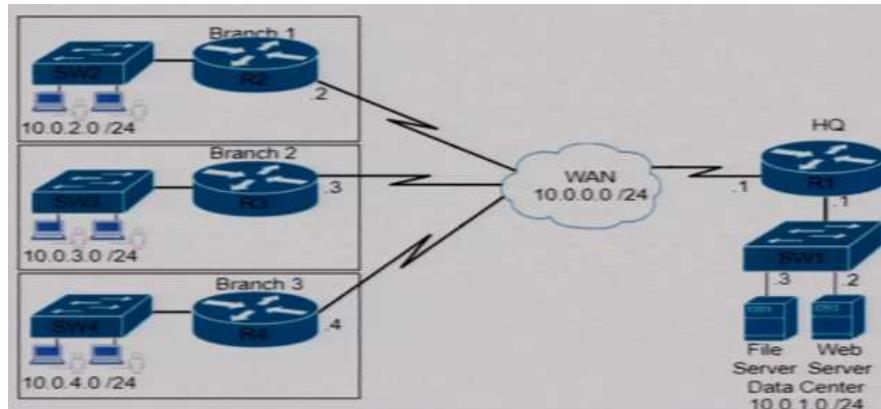
**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 672



Refer to the exhibit. Which command set is needed to configure and verify router R3 to measure the response time from router R3 to the file server located in the data center?

- A. ip sla 6
 

```

        icmp-echo 172.29.139.134 source-ip 172.29.139.132
        frequency 300
        ip sla schedule 6 start-time now
        show ip sla statistics 6
      
```
- B. ip sla 6
 

```

        icmp-echo 172.29.139.134 source-ip 172.29.139.132
        frequency 300
      
```

```

ip sla schedule 6 start-time now
show ip protocol
C. ip sla 6
  icmp-echo 10.0.1.3 source-ip 10.0.0.3
  frequency 300
  ip sla schedule 6 life forever start-time now
  show ip sla statistics 6
D. ip sla 6
  icmp-echo 10.0.1.3 source-ip 10.0.0.3
  frequency 300
  ip sla schedule 6 life forever start-time now
  show ip protocol

```

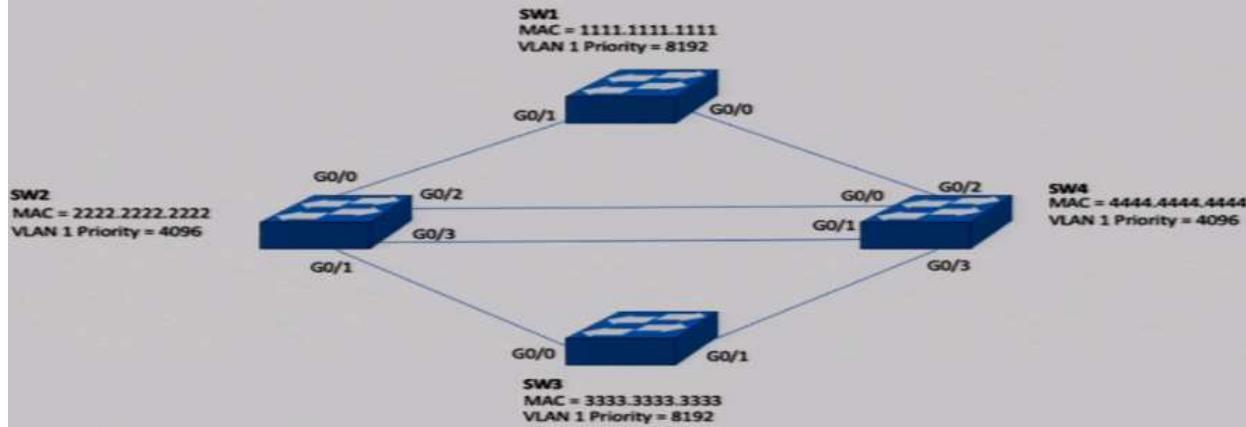
**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 673



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

- A. SW4(config)#spanning-tree vian 1 priority 0
 !  
 Sw2(oonfig)#int G0/2  
 Sw2(config-if)#spanning-tree cost 128
- B. SW4(config)#spanning-tree vian 1 priority 0
 !  
 Sw2(oonfig)#int G0/2  
 Sw2(config-if)#spanning-tree vlan 1 cost 64
- C. SW4(config)#spanning-tree vian 1 priority 32768
 !  
 Sw2(oonfig)#int G0/2  
 Sw2(config-if)#spanning-tree vlan 1 priority 0
- D. SW4(config)#spanning-tree vian 1 priority 32768
 !  
 Sw2(oonfig)#int G0/2  
 Sw2(config-if)#spanning-tree cost 128

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

To meet the requirement, you need to :

- Configure a lower bridge priority on Sw4 e.g. 0

- In order to block Sw2's g0/2, you can configure a high cost value on that port. Sw2's g0/3 will then be selected as root port and this will block Sw2's g0/2.

**Remarks:**

For changing port priority to achieve this, you need to change the port priority in the neighbor switch i.e. Sw4's g0/0 instead of the the port priority of Sw2's g0/2.

#### QUESTION 674

```

Cat3650# show logging
[ ... cut ... ]
*Sep 11 19:06:25.595: 4PM-4-ERR_DISABLE: channel-misconfig error detected on Po1, putting Gi1/0/2
in err-disable state
*Sep 11 19:06:25.606: 4PM-4-ERR_DISABLE: channel-misconfig error detected on Po1, putting Gi1/0/3
in err-disable state
*Sep 11 19:06:25.622: 4PM-4-ERR_DISABLE: channel-misconfig error detected on Po1, putting Po1 in
err-disable state

Cat3650# show etherchannel summary
[ ... cut ... ]
Group Port-channel Protocol Ports
-----+-----+-----+-----+
1      Po1(SD)        -       Gi1/0/2(D)  Gi1/0/3(D)

Cat3650# show interface status err-disabled
Port      Name      Status      Reason      Err-disabled Vlans
Gi1/0/2          err-disabled  channel-misconfig
Gi1/0/3          err-disabled  channel-misconfig
Po1            err-disabled  channel-misconfig

```

Refer to the exhibit. The administrator troubleshoots an EtherChannel that keeps moving to err-disabled. Which two actions must be taken to resolve the issue? (Choose two.)

- A. Ensure that the neighbor interfaces of Gi1/0/2 and Gi1/0/3 are configured as members of the same EtherChannel.
- B. Reload the switch to force EtherChannel renegotiation
- C. Ensure that interfaces Gi1/0/2 and Gi1/0/3 connect to the same neighboring switch,
- D. Ensure that the switchport parameters of Port-channel match the parameters of the port channel on the neighbor switch.
- E. Ensure that the corresponding port channel interface on the neighbor switch is named Port-channel.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The port is error disabled due to the EtherChannel Misconfiguration Guard tries to prevent a loop from occurring e.g. the connecting ports in the neighbor switch is not a member of an EtherChannel. This can occur if the EtherChannel is enabled unconditionally without negotiation.

**Remarks:**

From the output, both Gi1/0/2 and Gi1/0/3 are configured as members of Po1

**QUESTION 675**

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

Which of the following are the characteristics of OSPF (Choose Two)?

- A. sends hello packets every 5 seconds on high-bandwidth links
- B. uses virtual links to link an area that does not have a connection to the backbone
- C. cost is based on interface bandwidth

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The remaining one is the characteristic of EIGRP. OSPF sends Hello packets every 10 seconds for Ethernet link.

**QUESTION 676**

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

Which of the following are the characteristics of EIGRP?

- A. sends hello packets every 5 seconds on high-bandwidth links
- B. uses virtual links to link an area that does not have a connection to the backbone
- C. cost is based on interface bandwidth

**Correct Answer:** A

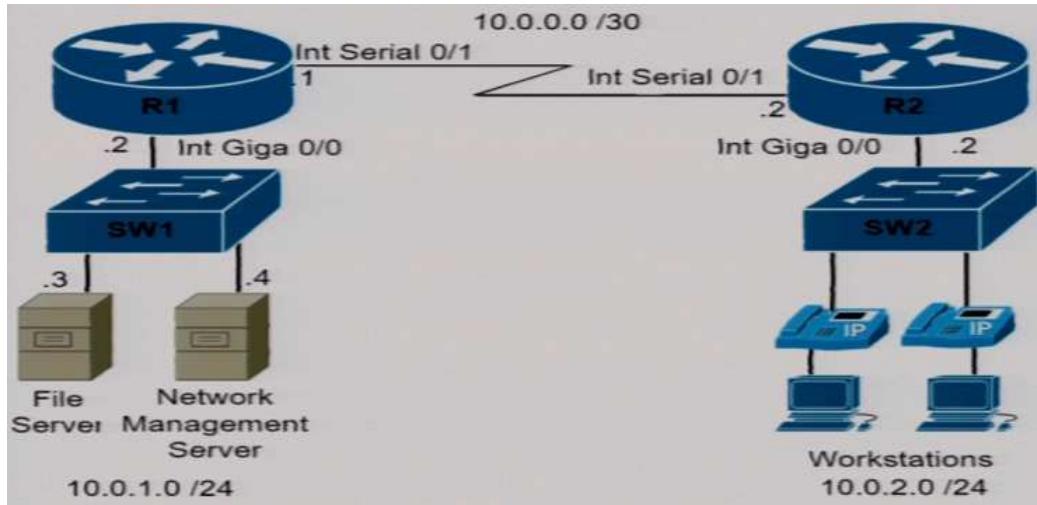
**Section:** (none)

**Explanation**

**Explanation/Reference:**

OSPF sends Hello packets every 10 seconds for Ethernet link.

**QUESTION 677**



An engineer must configure and validate a CoPP policy that allows the network management server to monitor router R1 via SNMP while protecting the control plane. Which two commands or command sets must be used? (Choose two.)

- A. show policy-map control-plane
- B. show quality-of-service profile
- C. show ip interface brief
- D. access-list 150 permit udp 10.0.1.4 0.0.0.0 host 10.0.1.2 eq snmp

```

class-map match-all COPP-management
match access-group 150

policy-map CoPP-policy
class COPP-management
  police 8000 conform-action transmit exceed-action transmit violate-action transmit

control-plane
  Service-policy input CoPP-policy

E. access-list 150 permit udp 10.0.1.4 0.0.0.0 host 10.0.1.2 eq snmp
access-list 150 permit udp 10.0.1.4 0.0.0.0 eq snmp host 10.0.1.2

class-map match-all COPP-management
match access-group 150

policy-map CoPP-policy
class COPP-management
  police 8000 conform-action transmit exceed-action transmit violate-action drop

control-plane
  Service-policy input CoPP-policy

```

**Correct Answer:** AE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In the other incorrect choice, the policy-map has "transmit" in all three actions and this does not protect anything going into the control plane.

#### QUESTION 678

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

Which of the followings are the characteristics of On-Premisis (Choose two)?

- A. Capacity easily scales up or down
- B. Infrastructure requires large and regular investments
- C. It enables users to access resources from anywhere
- D. It requires capacity planning for power and cooling.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 679

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

Which of the followings are the characteristics of Cloud (Choose two)?

- A. Capacity easily scales up or down
- B. Infrastructure requires large and regular investments
- C. It enables users to access resources from anywhere
- D. It requires capacity planning for power and cooling.

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 680**

```
{  
    "method": "GET",  
    "url": "/restconf/api/running/native/interface",  
    "params": {  
        "Accept": "application/vnd.yang.collection+json,  
                  application/vnd.yang.data+json,  
                  application/vnd.yang.datastore+json"  
    },  
    "data": {}  
}
```

Refer to the exhibit. What is the result of the API request?

- A. The information for all interfaces is read from the network appliance.
- B. The "params" variable sends data fields to the network appliance.
- C. The native interface information is read from the network appliance.
- D. The "params" variable reads data fields from the network appliance.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Instead of data, the "params" contains information about the format that the data should be presented in the reply.

**Remarks:**

The keyword "native" in the URL describe the YANG model being used.

**QUESTION 681**

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

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

**Correct Answer: AB**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 682**



Refer to the exhibit Which command set must be applied on R1 to establish a BGP neighborship with R2 and to allow communication from R1 to reach the networks?

- A. router bgp 1200  
 network 209.165.201.0 mask 255.255.255.224  
 neighbor 209.165.202.130 remote-as 1201
- B. router bgp 1200  
 network 209.165.200.224 mask 255.255.255.224  
 neighbor 209.165.202.130 remote-as 1201

- C. router bgp 1200  
   network 209.165.200.224 mask 255.255.255.224  
   neighbor 209.165.201.2 remote-as 1200
- D. router bgp 1200  
   network 209.165.200.224 mask 255.255.255.224  
   neighbor 209.165.202.130 remote-as 1200

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 683

Which Python code snippet must be added to the script to save the returned configuration as a JSON-formatted file?

```
import json
import requests

Creds = ("admin", "S!423554378$Ptx")
Headers = { "Content-Type" : "application/yang-data+json",
            "Accept" : "application/yang-data+json" }

BaseURL = "https://cpe/restconf/data"
URL = baseURL + "/Cisco-IOS-XE-native/interface/GigabitEthernet"
Response = requests.get(URL, auth = Creds, headers = Headers, verify = False)
```

- A. with open("ifaces.json", "w") as OutFile:  
   JSONResponse = json.loads(Response.text)  
   OutFile.write(JSONResponse)
- B. with open("ifaces.json", "w") as OutFile:  
   OutFile.write(Response.json())
- C. with open("ifaces.json", "w") as OutFile:  
   OutFile.write(Response)
- D. with open("ifaces.json", "w") as OutFile:  
   OutFile.write(Response.text)

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In the question, the JSON string result is stored directly to "response" without converting into a JSON object (i.e. without appending .json() on the left of the assignment). Hence the "Response" is storing a raw response object containing various information e.g. data, "url", "status\_code" ... etc.

If you want to get the data from the raw response object "Response", you can use:

- Response.text to get the JSON string representing the data.
- Response.json to get an object representing the data for further processing (e.g. getting a specific piece of data from it e.g.: response.json()['Cisco-IOS-XE-native:interface'][0]['ip']['address'])

Since we just need to save the data as JSON string to the file, we can just write the "Response.text" to the file.

**Remarks:**

json.loads() method is also not required here to parse the JSON string "response.text" into a Python object for processing. For the above raw response object, instead of "json.loads(response.text)", you can simply use "response.json()" to get the same result.

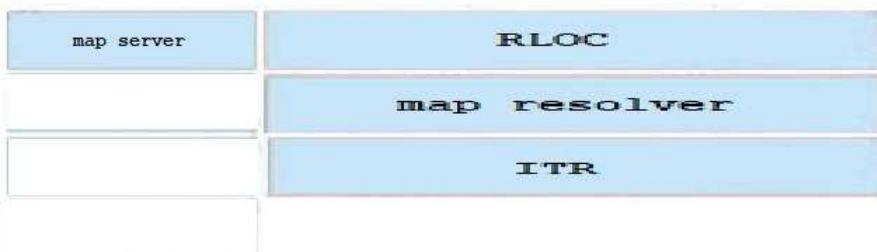
#### QUESTION 684

Drag and drop the LISP components on the left to their descriptions on the right. Not all options are used.

**Select and Place:**

map server	IPv4 or IPv6 address of an egress tunnel router that is Internet facing or network core facing
map resolver	receives map-request messages from ITR and searches for the appropriate ETR by consulting mapping database
RLOC	encapsulates LISP packets coming from inside of the LISP site to destinations outside of the site
ITR	

**Correct Answer:**



**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 685**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 686**

When firewall capabilities are considered, which feature is found only in Cisco next-generation firewalls?

- A. malware protection
- B. stateful inspection
- C. traffic filtering
- D. active/standby availability

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 687**

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

Which of the following are the characteristics of Configuration Management (Choose two)?

- A. This type of technology provides automation across multiple technologies and domains
- B. This type of technology enables consistent configuration of infrastructure resources
- C. Puppet is used for this type of technology
- D. Ansible is used for this type of technology

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Remarks :

Ansible is actually do both (i.e. Configuration Management and Orchestration). It is an open-source Infrastructure as code tool developed by RedHat. It is an automation tool that helps in the automation of many services like cloud provisioning, configuration management, orchestration, application deployment, etc.

Since this is actually a drag and drop question, Ansible should therefore belongs to Orchestration in this question.

**QUESTION 688**

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

Which of the following are the characteristics of Orchestration (Choose two)?

- A. This type of technology provides automation across multiple technologies and domains
- B. This type of technology enables consistent configuration of infrastructure resources
- C. Puppet is used for this type of technology
- D. Ansible is used for this type of technology

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 689**

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

**Select and Place:**

<pre>event manager applet Logging   event timer cron name Logging cron-entry " "     action 2.0 cli command "enable"     action " " cli command "show logging   "       1.0       3.0       redirect         ftp://cisco:cisco@192.168.1.1       0 21 * * 0-4       0 21 * * 1-5       ftp://cisco:cisco@192.168.1.1</pre>		
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

**Correct Answer:**

```

event manager applet Logging
  event timer cron name Logging cron-entry "0 21 * * 0-4"
    action 2.0 cli command "enable"
    action 3.0 cli command "show logging | redirect ftp://cisco:cisco@192.168.1.1"
  1.0
  0 21 * * 1-5
  ftp://cisco:cisco@192.168.1.1

```

Section: (none)

Explanation

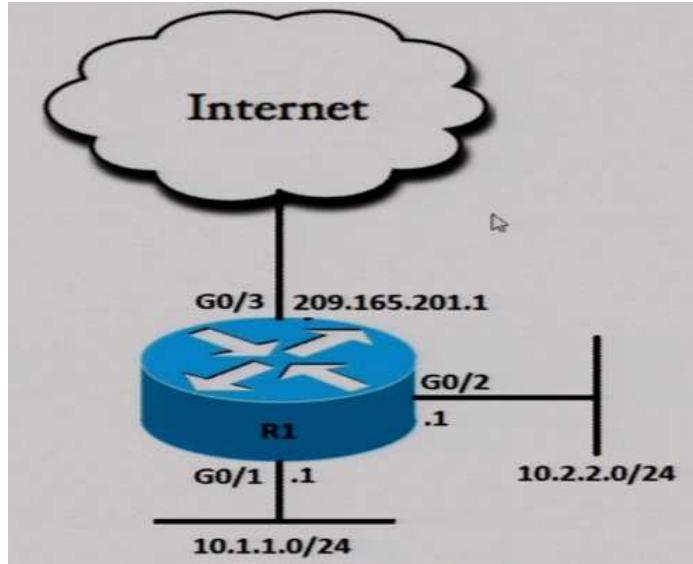
**Explanation/Reference:**

The cron-entry specifies the times for running a scheduled job in a Linux cron job.

- "0 21" means at the time 21:00
- "\*" means any day or any month
- "0-4" means Sunday to Thursday.

For sending the output to a URL, the keyword "redirect" is required after the "pipe" i.e. |

**QUESTION 690**



Refer to the exhibit. An engineer must allow all users in the 10.2.2.0/24 subnet to access the Internet. To conserve address space the public interface address of 209.165.201.1 must be used for all external communication Which command set accomplishes these requirements?

A. access-list 10 permit 10.2.2.0 0.0.0.255

```

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 interface G0/3

```

B. access-list 10 permit 10.2.2.0 0.0.0.255

```

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 interface G0/2 overload

```

C. access-list 10 permit 10.2.2.0 0.0.0.255

```

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 interface G0/3 overload

```

D. access-list 10 permit 10.2.2.0 0.0.0.255

```

interface G0/2
ip nat outside

interface G0/2
ip nat inside

```

```
ip nat inside source list 10 2-9.165.201.1
```

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 691**

What happens when a FlexConnect AP changes to standalone mode?

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

**Correct Answer:** D  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

If a FlexConnect AP should lose its CAPWAP connection to its controller, it goes into Standalone mode. In Standalone mode, any Centrally Switched WLANs are down, but Locally Switched WLANs remain operational. If the Locally Switched WLAN is configured for Central Authentication, the associated clients remain connected when the AP goes into Standalone mode, but will be unable to form new associations. A Locally Switched WLAN that uses Local Authentication remains operational whether the AP is in Standalone or Connected mode.

**Remarks:**

DFS is Dynamic Frequency Selection, which is a function of using 5 GHz Wi-Fi frequencies that are generally reserved for radar, such as military radar, satellite communication, and weather radar. The DFS channels vary from country to country. The main benefit to use DFS channels is to increase the number of Wi-Fi channels. It is legally required Channel Availability Check process to prevent electromagnetic interference the 5 GHz frequency with the radar.

**QUESTION 692**

An engineer must configure a new loopback interface on a router and advertise the interface as a /24 in OSPF. Which command set accomplishes this tasks?

- A. R2(config)#interface Loopback0  
R2(config-if)#ip address 172.22.2.1 255.255.255.0  
R2(config-if)#ip ospf 100 area 0
- B. R2(config)#interface Loopback0  
R2(config-if)#ip address 172.22.2.1 255.255.255.0  
R2(config-if)#ip ospf network point-to-point  
R2(config-if)#ip ospf 100 area 0
- C. R2(config)#interface Loopback0  
R2(config-if)#ip address 172.22.2.1 255.255.255.0  
R2(config-if)#ip ospf network point-to-multipoint  
R2(config-if)#router ospf 100  
R2(config-router)#network 172.22.2.0 0.0.0.255 area 0
- D. R2(config)#interface Loopback0  
R2(config-if)#ip address 172.22.2.1 255.255.255.0  
R2(config-if)#ip ospf network broadcast  
R2(config-if)#ip ospf 100 area 0

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 693**

```
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)
```

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

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

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

Although you can get and parse all data from running-config to obtain the specific setting you required, you can pass a filter in XML format as an additional argument when calling "get\_config()" so that the NETCONF server returns only the data that you required (i.e. less data will be returned).

**QUESTION 694**

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

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 695**

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

Which of the followings are the characteristics of On-Premisis (Choose two)?

- A. Cost for this model are considered CapEx
- B. This model improves elasticity of resources
- C. This model enables complete control of the servers.
- D. This model reduces management overhead by leveraging provider-managed resources.

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 696**

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

Which of the followings are the characteristics of Cloud (Choose two)?

- A. Cost for this model are considered CapEx
- B. This model improves elasticity of resources
- C. This model enables complete control of the servers.
- D. This model reduces management overhead by leveraging provider-managed resources.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 697**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Layer 2 flooding is feature that enables the flooding of broadcast, link-local multicast, and ARP traffic for a given overlay subnet.

Layer 2 flooding should be used selectively, where needed, using small address pool, and it is not enabled by default. Layer 2 flooding works by mapping the overlay subnet to a dedicated multicast group in the underlay. Broadcast, link-local multicast, and ARP traffic are encapsulated in fabric VXLAN and sent to the destination underlay multicast group. PIM ASM is used as the transport mechanism.

**QUESTION 698**

Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.

Which of the followings are characteristics of Chef (Choose two)?

- A. declarative
- B. communicates using knife tool
- C. communications through SSH
- D. procedural

**Correct Answer:** BD

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Knife is Chef's command-line tool to interact with the Chef server. One uses it for uploading cookbooks and managing other aspects of Chef.

	Chef	Puppet	Ansible	SaltStack	Terraform
Cloud		All	All	All	All
Type	Config Mgmt	Config Mgmt	Config Mgmt	Config Mgmt	Orchestration
Infrastructure	Mutable	Mutable	Mutable	Mutable	Immutable
Language	Procedural	Declarative	Procedural	Declarative	Declarative
Architecture	Client/Server	Client/Server	Client only	Client only	Client only
Orchestration					
Lifecycle (state) management	No	No	No	No	Yes
VM provisioning	Partial	Partial	Partial	Partial	Yes
Networking	Partial	Partial	Partial	Partial	Yes
Storage Management	Partial	Partial	Partial	Partial	Yes
Configuration					
Packaging	Yes	Yes	Yes	Yes	Partial <sup>1</sup>
Templating	Yes	Yes	Yes	Yes	Partial <sup>1</sup>
Service provisioning	Yes	Yes	Yes	Yes	Yes

<sup>1</sup> Using CloudInit

#### QUESTION 699

Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.

Which of the followings are characteristics of Saltstack (Choose two)?

- A. declarative
- B. communicates using knife tool
- C. communications through SSH
- D. procedural

**Correct Answer:** AC

**Section:** Selected

**Explanation**

#### Explanation/Reference:

Salt was designed to enable low-latency and high-speed communication for data collection and remote execution in sysadmin environments. The platform is written in Python and uses the push model for executing commands via the SSH protocol.

#### QUESTION 700

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

- A. custom
- B. priority
- C. weighted fair
- D. low latency

**Correct Answer:** B

**Section:** (none)

**Explanation**

#### Explanation/Reference:

#### QUESTION 701

```
Device> enable
Device# configure terminal
Device(config)# monitor session 1 type erspan-source
Device(config-mon-erspan-src)# description source1
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/1 rx
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/4 - 8 tx
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/3
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# erspan-id 100
Device(config-mon-erspan-src-dst)# origin ip address 10.1.0.1
Device(config-mon-erspan-src-dst)# ip prec 5
Device(config-mon-erspan-src-dst)# ip ttl 32
Device(config-mon-erspan-src-dst)# mtu 1700
Device(config-mon-erspan-src-dst)# origin ip address 10.10.0.1
Device(config-mon-erspan-src-dst)# vrf 1
Device(config-mon-erspan-src-dst)# no shutdown
Device(config-mon-erspan-src-dst)# end
```

Refer to the exhibit An engineer must configure an ERSPAN session with the remote end of the session 10.10.0.1. Which commands must be added to complete the configuration?

- A. Device(config)#monitor session 1 type erspan-destination  
Device(config-mon-erspan-src)#source  
Device(config-mon-erspan-src-dst)#origin ip address 10.1.0.1
- B. Device(config)#monitor session 1 type erspan-source  
Device(config-mon-erspan-src)#source  
Device(config-mon-erspan-src-dst)#no origin ip address 10.10.0.1  
Device(config-mon-erspan-src-dst)#ip address 10.10.0.1
- C. Device(config)#monitor session 1 type erspan-source  
Device(config-mon-erspan-src)destination  
Device(config-mon-erspan-src-dst)#no origin ip address 10.10.0.1  
Device(config-mon-erspan-src-dst)#ip destination address 10.10.0.1
- D. Device(config)#monitor session 1 type erspan-source  
Device(config-mon-erspan-src)destination  
Device(config-mon-erspan-src-dst)#no vrf 1

**Correct Answer:** B

**Section: (none)****Explanation****Explanation/Reference:**

For the configuration shown in the exhibit, the IP address of the destination 10.10.0.1 (e.g. the PC running wireshark) is missing. Moreover, you should not configure the destination as the origin IP address in the setting.

Therefore, we need to:

- configure the IP address 10.10.0.1 as destination with the command "ip address 10.10.0.1"
- remove the origin IP address 10.10.0.1

**QUESTION 702**

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

Refer to the exhibit. Which command must be configured for RESTCONF to operate on port 8888?

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

**Correct Answer: A**

**Section: Selected****Explanation****Explanation/Reference:**

All answers are NOT correct.

RESTCONF runs over HTTPS and therefore it is using port 443 by default.

In order to change the port, you need to change the HTTPS port with the command e.g. "ip http secure-port 9443"

The choice A is chosen since it is the closest match.

**QUESTION 703**

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

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

**Correct Answer: C**

**Section: (none)****Explanation****Explanation/Reference:****QUESTION 704**

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

Which of the following are the characteristics of Procedural (Choose two)?

- A. Administrators require deep syntax and context knowledge for the configured entities.
- B. This model states what is wanted but not how it is achieved.
- C. Puppet is a tool that uses this configuration model
- D. This model defines a set of commands that must be executed in a certain order for the system to achieve the desired state.

**Correct Answer: AD**

**Section: Selected****Explanation****Explanation/Reference:****QUESTION 705**

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

Which of the following are the characteristics of Declarative (Choose two)?

- A. Administrators require deep syntax and context knowledge for the configured entities.
- B. This model states what is wanted but not how it is achieved.
- C. Puppet is a tool that uses this configuration model
- D. This model defines a set of commands that must be executed in a certain order for the system to achieve the desired state.

**Correct Answer: BC**

**Section: Selected****Explanation****Explanation/Reference:**

**QUESTION 706**

```

Router A
Interface GigabitEthernet 1/0
ip address 192.168.0.1 255.255.255.0
vrrp priority 120

Router B
Interface GigabitEthernet 1/0
ip address 192.168.0.200 255.255.255.0
vrrp priority 100

Router C
Interface GigabitEthernet 1/0
ip address 192.168.0.3 255.255.255.0
vrrp priority 130

Router D
Interface GigabitEthernet 1/0
ip address 192.168.0.4 255.255.255.0
vrrp priority 90

```

Refer to the exhibit. Which router is elected as the VRRP primary virtual router?

- A. Router A
- B. Router B
- C. Router C
- D. Router D

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 707**

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

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

- A. </>
- B. </>
- C. </>
- D. <rpc message-id="9.0"><notification-off/>

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

All NETCONF requests must end with >>> which denotes an end to the request. Until the >>> sequence is received, the request will not be processed.

**QUESTION 708**

Which A record type should be configured for access points to resolve the IP address of a wireless LAN controller through DNS?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 709**

```

Switch1#show ip int br
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet1  192.168.1.1    YES manual up           up
GigabitEthernet2  172.16.40.10   YES manual administratively down down
Loopback0         172.16.10.10   YES manual up           up

Switch2#show ip int br
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet1  192.168.1.2    YES manual up           up
GigabitEthernet2  172.16.20.10   YES manual up           up
Loopback0         10.10.10.10   YES manual up           up

Switch1(config)#monitor session 1 type erspan-source
Switch1(config-mon-erspan-src)#source interface gigabitethernet1
Switch1(config-mon-erspan-src)#destination
Switch1(config-mon-erspan-src-dst)#erspan-id 110
Switch1(config-mon-erspan-src-dst)#ip address 10.10.10.10
Switch1(config-mon-erspan-src-dst)foreign ip address 172.16.10.10

Switch2(config)#monitor session 1 type erspan-destination
Switch2(config-mon-erspan-dst)#destination interface Gigabitethernet2
Switch2(config-mon-erspan-dst)#source
Switch2(config-mon-erspan-dst-src)#
Switch2(config-mon-erspan-dst-src)#ip address 10.10.10.10

```

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. erspan-id 172.16.10.10
- B. erspan-id 110
- C. origin ip address 172.16.10.10
- D. no shut

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

"origin ip address" is only required on the erspan-source configuration.

#### QUESTION 710

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

Which of the followings are the characteristics of EIGRP (Choose two)?

- A. cost-based metric
- B. Dual Diffusing Update Algorithm
- C. metrics are bandwidth, delay, reliability, load, and MTU
- D. Dijkstra algorithm

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 711

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

Which of the followings are the characteristics of OSPF (Choose two)?

- A. cost-based metric
- B. Dual Diffusing Update Algorithm
- C. metrics are bandwidth, delay, reliability, load, and MTU
- D. Dijktra algorithm

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 712

Which IPv4 packet field carries the QoS IP classification marking?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 713

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 714**

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

- A. standby version 2  
standby 300 priority 110  
standby 300 preempt
- B. standby 300 priority 110  
standby 300 timers 1 110
- C. standby version 2  
standby 300 priority 90  
standby 300 preempt
- D. standby 300 priority 90  
standby 300 preempt

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since the group number is larger than 255, HSRP version 2 must be used.

Moreover, unlike VRRP, HSRP must be configured with preempt (disabled by default) in order to become the active router after boot even if the peer router is already running.

**QUESTION 715**

```
Switch1# show interfaces trunk
! Output omitted for brevity.
Port Mode Encapsulation Status Native
Gi1/0/20 auto 802. trunking 10

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

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

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

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

If one end is configured as "mode auto", the other side must be configured with "mode desirable" or "mode trunk" in order to form a trunk line.

**QUESTION 716**

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

Neighbor      V      AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
192.168.12.2  4      65002     0     0     1     0     0 00:00:15 Idle
R1#show ip interface brief | include 192.168.12
FastEthernet0/0          192.168.12.1  YES NVRAM up                  up

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

Neighbor      V      AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
192.168.12.1  4      65001     0     0     1     0     0 00:01:00 Idle (Admin)
R2#show ip interface brief | include 192.168.12
Ethernet0/0          192.168.12.2  YES NVRAM up                  up
R2#ping 192.168.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

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

- A. Configure no neighbor 192.168.12.1 shutdown under R2 BGP process.

- B. Configure neighbor 192.168.12.1 activate under R2 BGP process.
- C. Configure ip route 1.1.1.1 0.0.0.0 192.168.12.1 on R2.
- D. Configure neighbor 2.2.2.2 remote-as 65002 under R1 BGP process.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

R2 shows the neighbor state for "192.168.12.1" as Idle (Admin). Hence, you need to change it to Active.

#### QUESTION 717

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

Which of the followings are the characteristics of On-Premisis (Choose two)?

- A. easy to scale the capacity up and down
- B. infrastructure requires large and regular investments
- C. highly agile
- D. highly customizable

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

"agile" means able to move quickly and easily.

#### QUESTION 718

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

Which of the followings are the characteristics of Cloud (Choose two)?

- A. easy to scale the capacity up and down
- B. infrastructure requires large and regular investments
- C. highly agile
- D. highly customizable

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

"agile" means able to move quickly and easily.

#### QUESTION 719

<pre>R1#show ip ospf interface Gi0/0 GigabitEthernet0/0 is up, line protocol is up   Internet Address 172.20.0.1/24, Area 0, Attached via Network Statement   Process ID 1, RouterID 172.20.0.1, Network Type   BROADCAST, Cost: 1   Topology-MTID    Cost      Disabled      Shutdown   Topology Name     0          1        no        no Base   Transmit Delay is 1 sec, State DR, Priority 1   Designated Router (ID) 172.20.0.1, Interface address 172.20.0.1   No backup designated router on this network   Timer intervals configured,Hello 10,Dead 40, Wait 40, Retransmit 5   oob-resync timeout 40   No Hellos (Passive interface)   Supports Link-local Signaling (LLS)   Cisco NSF helper support enabled   IETF NSF helper support enabled</pre>	<pre>R2#show ip ospf interface Gi0/0 GigabitEthernet0/0 is up, line protocol is up   Internet Address 172.20.0.2/24, Area 0, Attached via Network Statement   Process ID 1, RouterID 172.20.0.2, Network Type   BROADCAST, Cost: 5   Topology-MTID    Cost      Disabled      Shutdown   Topology Name     0          5        no        no Base   Transmit Delay is 1 sec, State DR, Priority 1   Designated Router (ID) 172.20.0.2, Interface address 172.20.0.2   No backup designated router on this network   Timer intervals configured,Hello 10,Dead 40, Wait 40, Retransmit 5   oob-resync timeout 40   Hello due in 00:00:01   Supports Link-local Signaling (LLS)   Cisco NSF helper support enabled   IETF NSF helper support enabled   Index 1/1/1, flood queue length 0</pre>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Refer to the exhibit. Cisco IOS routers R1 and R2 are interconnected using interface Gi0/0. Which configuration allows R1 and R2 to form an OSPF neighborship on interface Gi0/0?

- A. R1(config)#router ospf 1
 R1(config-router)#no passive-interface Gi0/0
- B. R1(config)#router ospf 1
 R1(config-router)#network 172.20.0.0 0.0.0.255 area 1
- C. R2(config)#router ospf 1
 R2(config-router)#passive-interface Gi0/0
- D. R2(config)#interface Gi0/0
 R2(config-router)#ip ospf cost 1

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

From the exhibit, R1's g0/0 is enabled with OSPF but it is shown as a Passive Interface with No Hellos sending. Hence, you need to set the passive interface setting for the interface.

**QUESTION 720**

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

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

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

**Correct Answer: C****Section: (none)****Explanation****Explanation/Reference:**

In order to insert / modify a rule in an access list, you need to use modify it as a standard / extended named ACL. However, the rule added in the choice using this way is for 172.20.10.0/24 (i.e. not just 172.20.10.1). Hence, it is not the answer.

If you just want to append a new rule at the end, you can just add the rule normally.

**QUESTION 721**

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

Which of the following are the characteristics of MAC Address Table (Choose two)?

- A. used to make Layer 2 forwarding decisions
- B. used to build IP routing table
- C. records MAC address, port of arrival, VLAN and time stamp
- D. stores ACL, QoS and other upper-layer information

**Correct Answer: AC****Section: (none)****Explanation****Explanation/Reference:****QUESTION 722**

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

Which of the following are the characteristics of TCAM Table (Choose two)?

- A. used to make Layer 2 forwarding decisions
- B. used to build IP routing table
- C. records MAC address, port of arrival, VLAN and time stamp
- D. stores ACL, QoS and other upper-layer information

**Correct Answer: BD****Section: (none)****Explanation****Explanation/Reference:****QUESTION 723**

```

GigabitEthernet0/1 is up, line protocol is up
Internet Address 192.168.50.1/24, Area 0, Attached via Interface Enable
Process ID 1, Router ID 192.168.50.1, Network Type BROADCAST, Cost: 1
Topology-MTID      Cost      Disabled      Shutdown      Topology Name
          0           1        no          no          Base
Enabled by interface config, including secondary ip addresses
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.50.1, Interface address 192.168.50.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
    cobb-resync timeout 40
    Hello due in 00:00:07
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/2/2, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 1 msec, maximum is 1 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

```

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

- A. R1(config)#router ospf 1  
R1(config-router)#network 192.168.50.0 0.0.0.255 area 0
- B. R1(config)#interface Gi0/1  
R1(config-if)#ip ospf enable  
R1(config-if)#ip ospf network broadcast  
R1(config-if)#no shutdown
- C. R1(config)#interface Gi0/1  
R1(config-if)#ip ospf 1 area 0  
R1(config-if)#no shutdown
- D. R1(config)#router ospf 1  
R1(config-router)#network 192.168.50.0 0.0.0.255 area 0  
R1(config-router)#no passive-interface Gi0/1

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since there is a line "Enabled by interface config" (line number 6) in the exhibit, the OSPF interface is configured by interface command.

#### QUESTION 724

Based on the routers API output in JSON format below, which Python code will display the value of the "role" key?

```
{
  "response": [
    {
      "family": "Routers",
      "macAddress": "00:c8:8b:80:bb:00",
      "hostname": "BorderA",
      "uptime": "5 days, 1:22:33:44",
      "lastUpdated": "2000-01-01 11:22:33"
    }
  ]
}
```

- A. json\_data = json.loads(response.text)  
print(json\_data[response][0][hostname])
- B. json\_data = json.loads(response.text)  
print(json\_data["response"]["family"]["hostname"])
- C. json\_data = response.json()  
print(json\_data["response"][family][hostname])
- D. json\_data = response.json()  
print(json\_data["response"][0]["hostname"])

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The data in "response" is enclosed by "[]" which is a List in Python. Therefore, you need to specify a "0" to get the first element before you can access the "hostname" in this element. Moreover, the field name has to be enclosed by "".

#### QUESTION 725

```

flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow monitor FLOW-MONITOR-1
record v4_r1
exit
!
sampler SAMPLER-1
mode random 1 out-of 2
exit
!
ip cef
!
interface GigabitEthernet 0/0/0
 ip address 172.16.6.2 255.255.255.0

```

Refer to the exhibit. Which command set must be added to the configuration to analyze 50 packets out of every 100?

\_r

```
, interface Gigabitfihernet W0
ip flaw monitor FLOW-MONITOR-'i sampler SAMPLER-'t input
```

- A. sampler SAMPLER-1
 

```
no mode random 1-out-of 2
      mode percent 50
```
- B. interface GigabitEtherntet Gi0/0/0
 

```
ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```
- C. flow monitor FLOW-MONITOR-1
 

```
record v4_r1
      sampler SAMPLER-1
```
- D. interface GigabitEtherntet Gi0/0/0
 

```
ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

**Correct Answer:** B

**Section:** (none)

**Explanation**

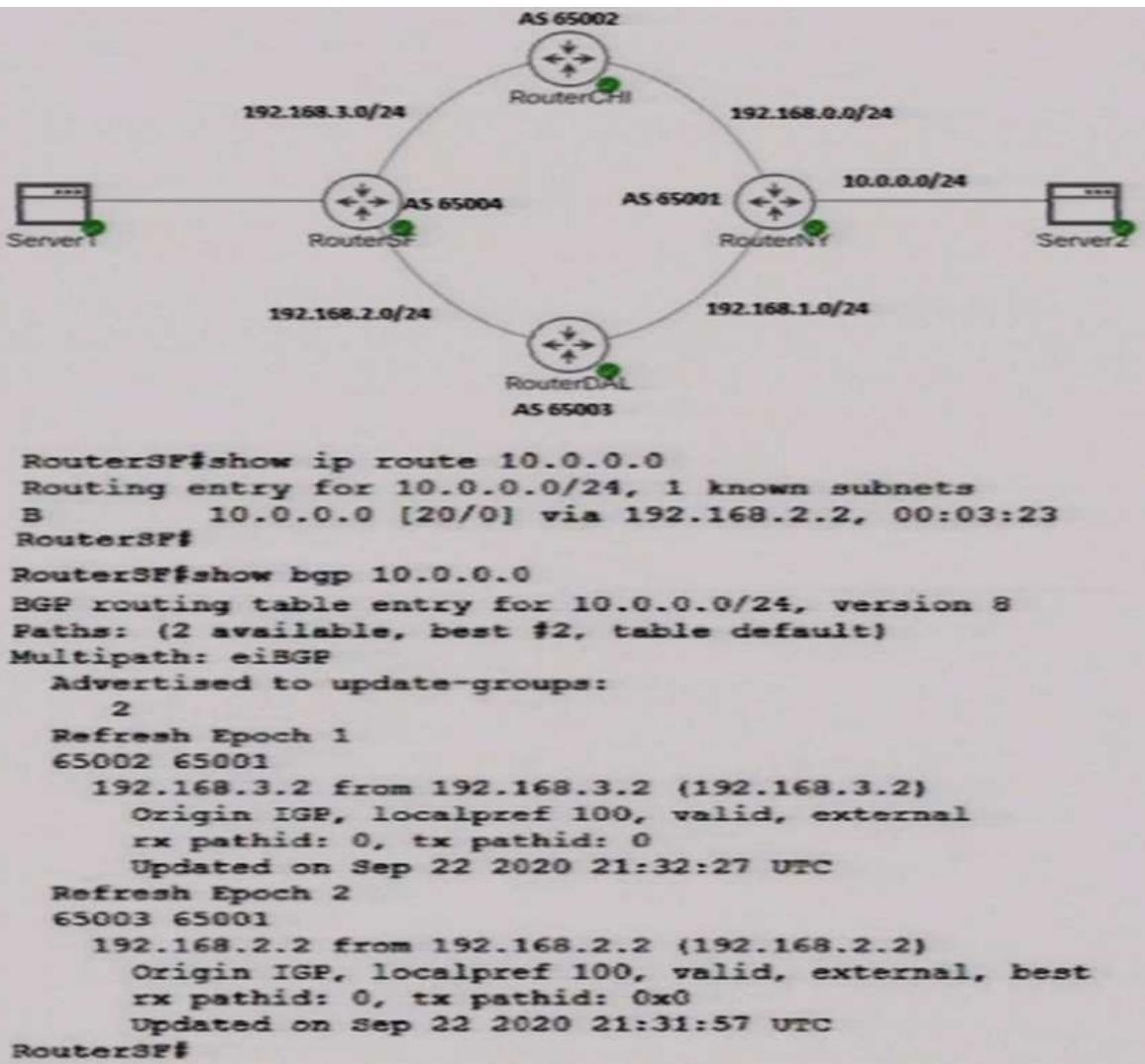
**Explanation/Reference:**

Since both flow monitor and sampler exists in the current configuration and match the requirement, you just need to apply them.

**Remarks:**

Note that you cannot specify sampler within a flow monitor configuration and you cannot specify flow within the sampler configuration.

**QUESTION 726**



Refer to the exhibit. After configuring the BGP network, an engineer verifies that the path between Server1 and Server2 is functional. Why did RouterSF choose the route from RouterDAL instead of the route from RouterCHI?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

BGP path is selected according to the following order:

Next hop reachable?	continue if "yes"
Local Preference	higher wins
AS path	shorter wins
Origin Type	IGP over EGP over incomplete
MED	lower wins
eBGP, iBGP	eBGP wins
Network exit	nearest wins
Age of route	older wins
Router ID	lower wins
Neighbor IP	lower wins

From the information in "show bgp 10.0.0.0", both paths have the same number of ASes i.e. 2

From the information in "show bgp 10.0.0.0", both paths have the same origin i.e. "IGP".

No information is shown for metric and therefore it is assumed that the two paths have the same default MED i.e. 0.

Both paths are learnt from AS other than 65004 therefore both are the same i.e. learnt from eBGP.

Since there is no information about IGP cost to NextHop and therefore it is assumed that they are the same.

From the information in "show bgp 10.0.0.0", the second path i.e. the one learnt from 650003 has a older updated time than the first path i.e. the one learnt from 65002. Hence it is probably the cause of choosing the second path i.e. through RouterDAL.

From the information in "show bgp 10.0.0.0", the second path i.e. the one learnt from RouterDAL has a lower Router ID 192.168.2.2 than the first path i.e. the one learnt from RouterCHI. Hence, if the time learnt is the same, it is the factor to choose the second path i.e. through RouterDAL.

For the choices:

The choice about Static route is not a valid answer since "sh ip route" shows a "B" in the routing entry i.e. learnt from BGP instead of static.

The choice that BGP is not running in RouterCHI is not a valid answer since a BGP path is actually learnt from RouterCHI although it is not selected as "Best". Since there is no information about metric in the "sh ip route" and there is no choice about selection by oldest path / age, the only valid answer is the one mentioning about lower RouterID.

#### QUESTION 727

Drag and drop the characteristics from the left onto the switching architectures on the right.  
Which are the characteristics of Process Switching (Choose two)?

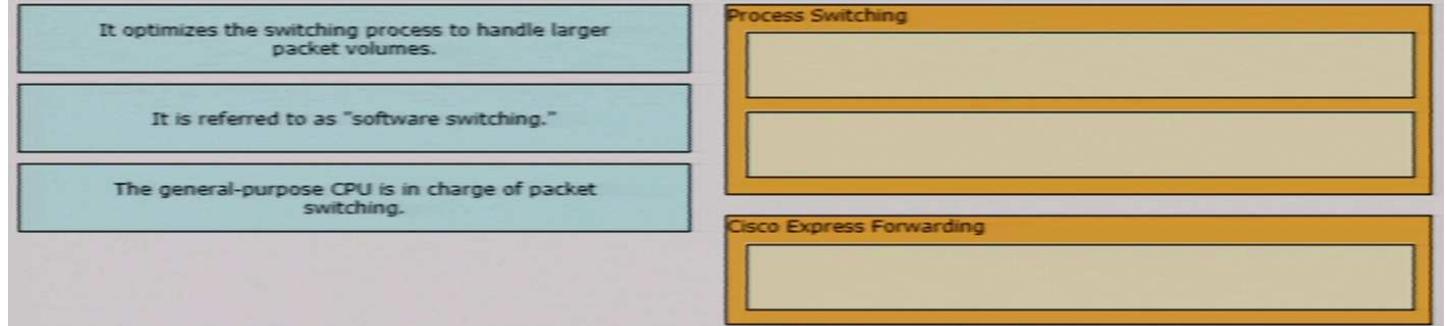
- A. It optimizes the switching process to handle larger packet volumes.
- B. It is referred to as "software switching."
- C. The general-purpose CPU is in charge of packet switching.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 728

Drag and drop the characteristics from the left onto the switching architectures on the right.  
Which is the characteristic of Cisco Express Forwarding?

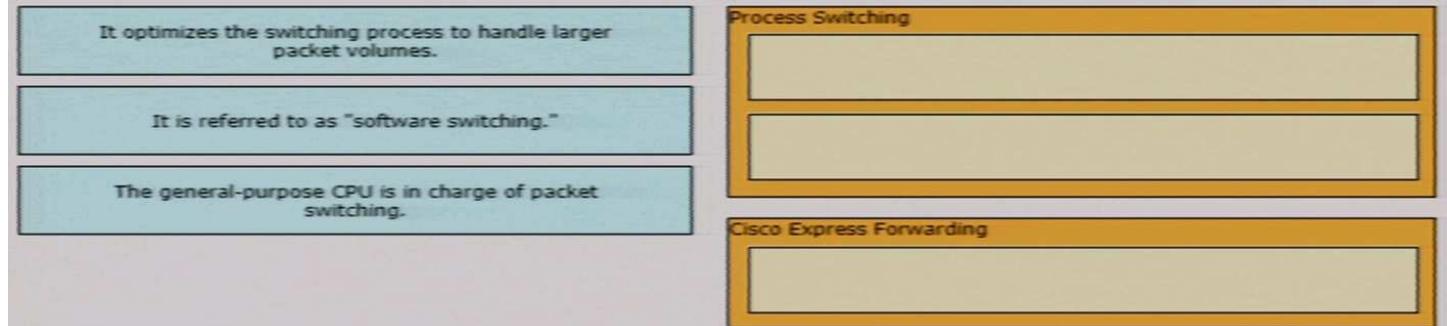
- A. It optimizes the switching process to handle larger packet volumes.
- B. It is referred to as "software switching."
- C. The general-purpose CPU is in charge of packet switching.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 729

In Cisco DNA Center, what is the integration API?

- A. southbound consumer-facing RESTful API, which enables network discovery and configuration management
- B. westbound interface, which allows the exchange of data to be used by ITSM, IPAM and reporting
- C. an interface between the controller and the network devices, which enables network discovery and configuration management
- D. northbound consumer-facing RESTful API, which enables network discovery and configuration management

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

#### Events and Notifications (Eastbound)

The Cisco DNA Center platform provides the ability to establish a notification handler when specific events are triggered, such as Cisco DNA Assurance and Automation (SWIM) events.

This mechanism enables external systems to take actions in response to an event. For example, a custom application could execute a software upgrade action in response to notification of network devices that are out of compliance.

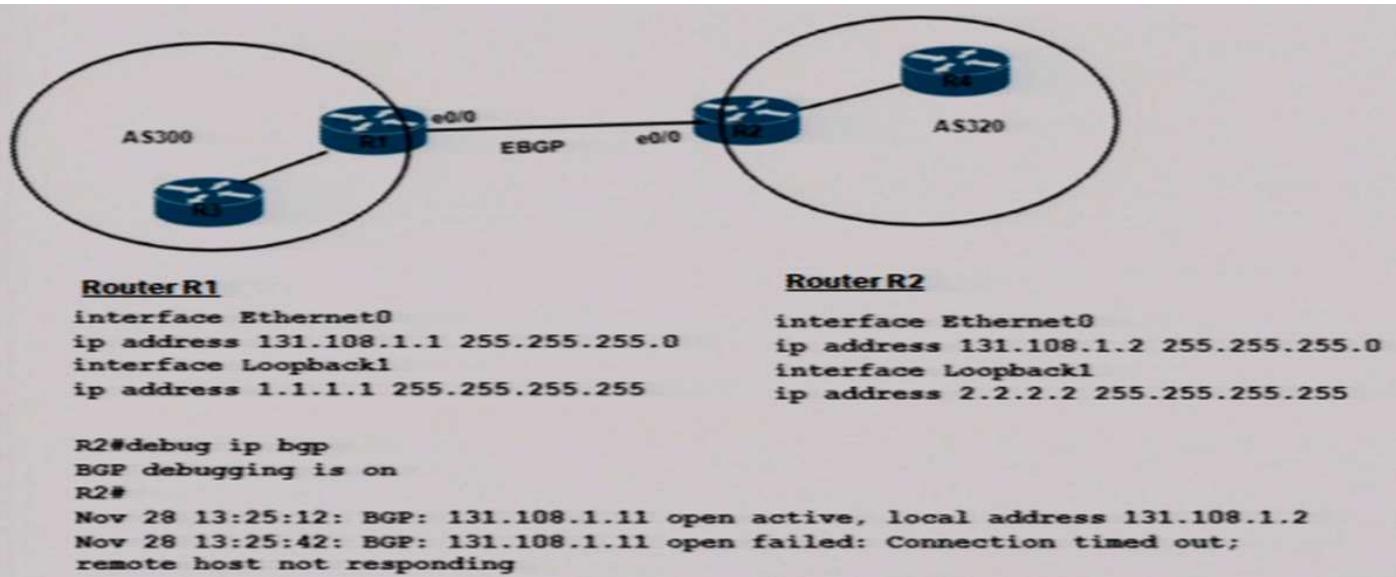
Notifications may also be triggered by events internal DNA Center events. For example, Assurance events can be customized for IT Service Management incidents.

#### Integration API (Westbound)

Integration capabilities are part of Westbound interfaces. To meet the need to scale and accelerate operations in modern data centers, IT operators require intelligent, end-to-end work flows built with open APIs. The Cisco DNA Center platform provides mechanisms for integrating Cisco DNA Assurance workflows and data with third-party IT Service Management (ITSM) solutions.

Therefore the choice mentioning "westbound" is the answer.

#### QUESTION 730



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

- A. R2
 

```
router bgp 320
neighbor 131.108.1.11 remote-as 300
R1
router bgp 300
neighbor 131.108.1.2 remote-as 320
```
- B. R2
 

```
router bgp 300
neighbor 131.108.1.1 remote-as 320
R1
router bgp 320
neighbor 131.108.1.2 remote-as 300
```
- C. R2
 

```
router bgp 320
neighbor 131.108.1.1 remote-as 300
R1
router bgp 300
neighbor 131.108.1.2 remote-as 320
```
- D. R2
 

```
router bgp 320
neighbor 1.1.1.1 remote-as 300
R1
router bgp 300
neighbor 2.2.2.2 remote-as 320
```

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

From the debugging, R1 is trying to make connection to 131.108.1.11 but failed. It seems that the neighbor configured in R1 is 131.108.1.11 but R2 actually has the IP address 131.108.1.2.

You can either change the IP address of R2 or change the neighbor command in R1.

Since no choice involved the changing of IP address, you should choose one with a valid neighbor configuration for R1 i.e.

R1

```
router bgp 300
neighbor 131.108.1.2 remote-as 320
```

Only one choice contains the above commands and therefore it is the answer.

**QUESTION 731**

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

R1#ping vrf CUST-A 192.168.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R1#show ip arp 192.168.12.2
R1#
```

Refer to the exhibit. A network engineer checks connectivity between two routers. The engineer can ping the remote endpoint but cannot see an ARP entry. Why is there no ARP entry?

- A. Interface FastEthernet0/0 is configured in VRF CUST-A, so the ARP entry is also in that VRF.
- B. When VRPs are used, ARP protocol is disabled in the global routing table.
- C. When VRPs are used, ARP protocol must be enabled in each VRF.

- D. The ping command must be executed in the global routing table.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

```
Router#sh ip arp vrf ?  
WORD  VPN Routing/Forwarding instance name
```

Note that the keyword "vrf" is only available for the command after a VRF is created in the router.

**QUESTION 732**

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

Which are the characteristics of On-Premises (Choose two)?

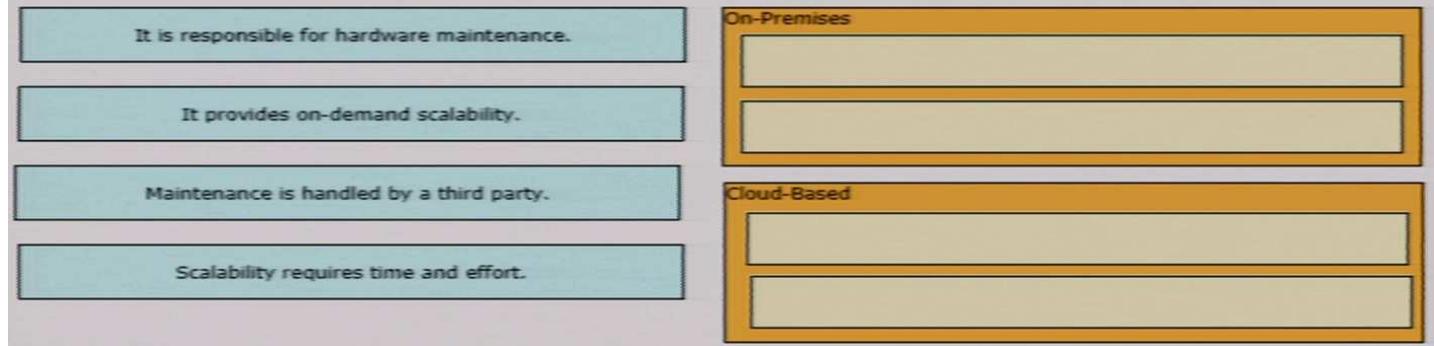
- A. It is responsible for hardware maintenance.
- B. It provides on-demand scalability.
- C. Maintenance is handled by a third party.
- D. Scalability requires time and effort.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 733**

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

Which are the characteristics of Cloud-Based (Choose two)?

- A. It is responsible for hardware maintenance.
- B. It provides on-demand scalability.
- C. Maintenance is handled by a third party.
- D. Scalability requires time and effort.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 734**

Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.

Which are the characteristics of Chef (Choose two)?

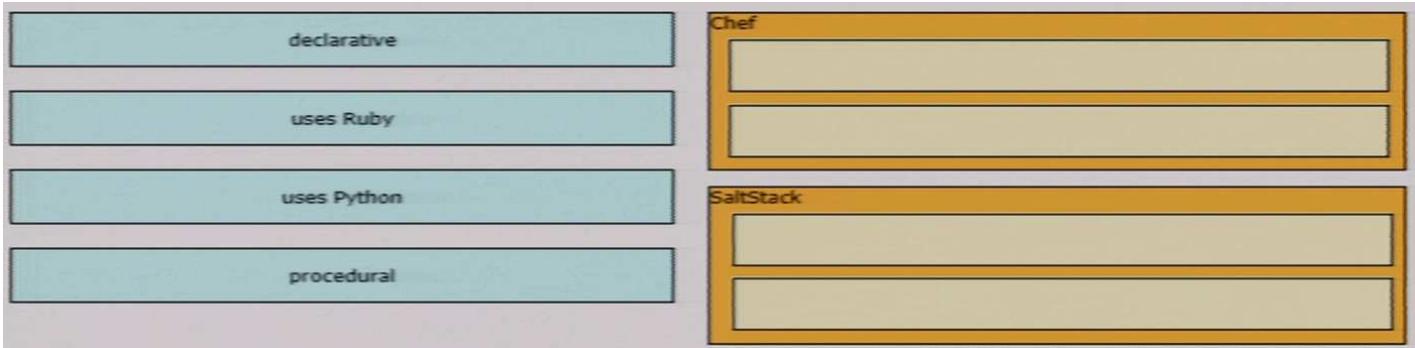
- A. declarative
- B. uses Ruby
- C. uses Python
- D. procedural

**Correct Answer:** BD

**Section:** Selected

**Explanation**

**Explanation/Reference:**



Metrics	Chef	Puppet	Ansible	Saltstack
Availability	✓	✓	✓	✓
Ease of Setup	Not very easy	Not very easy	Easy	Not very easy
Management	Not very easy	Not very easy	Easy	Easy
Scalability	Highly Scalable	Highly Scalable	Highly Scalable	Highly Scalable
Configuration language	DSL(Ruby)	DSL(PuppetDSL)	YAML(Python)	YAML(Python)
Interoperability	High	High	High	High
Pricing (upto 100 nodes)	\$13700	\$11200-\$19900	\$10,000	\$15,000(approx.)

	Chef	Puppet	Ansible	SaltStack	Terraform
Cloud		All	All	All	All
Type	Config Mgmt	Config Mgmt	Config Mgmt	Config Mgmt	Orchestration
Infrastructure	Mutable	Mutable	Mutable	Mutable	Immutable
Language	Procedural	Declarative	Procedural	Declarative	Declarative
Architecture	Client/Server	Client/Server	Client only	Client only	Client only
Orchestration					
Lifecycle (state) management	No	No	No	No	Yes
VM provisioning	Partial	Partial	Partial	Partial	Yes
Networking	Partial	Partial	Partial	Partial	Yes
Storage Management	Partial	Partial	Partial	Partial	Yes
Configuration					
Packaging	Yes	Yes	Yes	Yes	Partial <sup>1</sup>
Templating	Yes	Yes	Yes	Yes	Partial <sup>1</sup>
Service provisioning	Yes	Yes	Yes	Yes	Yes

<sup>1</sup> Using CloudInit

### QUESTION 735

Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.  
Which are the characteristics of SaltStack (Choose two)?

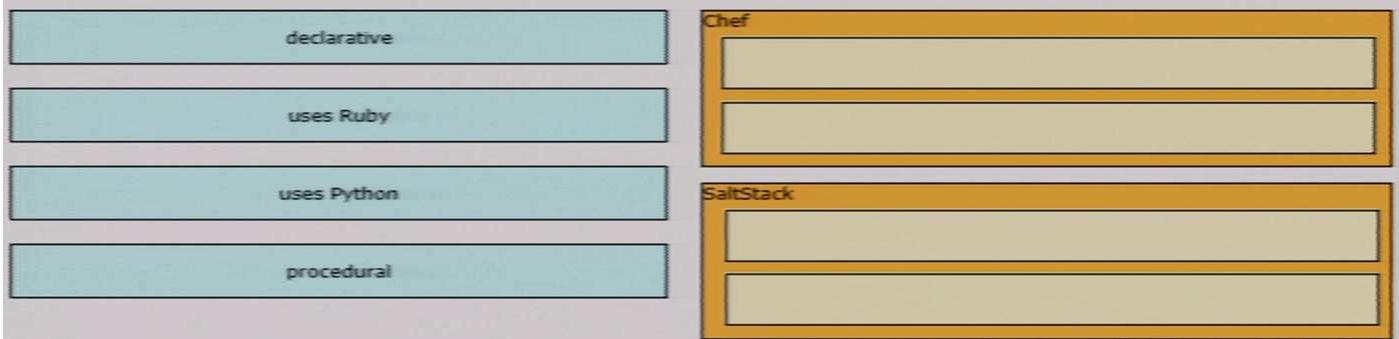
- A. declarative
- B. uses Ruby
- C. uses Python
- D. procedural

Correct Answer: AC

Section: Selected

Explanation

Explanation/Reference:



Metrics	Chef	Puppet	Ansible	Saltstack
Availability	✓	✓	✓	✓
Ease of Setup	Not very easy	Not very easy	Easy	Not very easy
Management	Not very easy	Not very easy	Easy	Easy
Scalability	Highly Scalable	Highly Scalable	Highly Scalable	Highly Scalable
Configuration language	DSL(Ruby)	DSL(PuppetDSL)	YAML(Python)	YAML(Python)
Interoperability	High	High	High	High
Pricing (upto 100 nodes)	\$13700	\$11200-\$19900	\$10,000	\$15,000(approx.)

	Chef	Puppet	Ansible	SaltStack	Terraform
Cloud		All	All	All	All
Type	Config Mgmt	Config Mgmt	Config Mgmt	Config Mgmt	Orchestration
Infrastructure	Mutable	Mutable	Mutable	Mutable	Immutable
Language	Procedural	Declarative	Procedural	Declarative	Declarative
Architecture	Client/Server	Client/Server	Client only	Client only	Client only
Orchestration					
Lifecycle (state) management	No	No	No	No	Yes
VM provisioning	Partial	Partial	Partial	Partial	Yes
Networking	Partial	Partial	Partial	Partial	Yes
Storage Management	Partial	Partial	Partial	Partial	Yes
Configuration					
Packaging	Yes	Yes	Yes	Yes	Partial <sup>1</sup>
Templating	Yes	Yes	Yes	Yes	Partial <sup>1</sup>
Service provisioning	Yes	Yes	Yes	Yes	Yes

<sup>1</sup> Using CloudInit

#### QUESTION 736

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

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

Number of channel-groups in use: 1
Number of aggregators: 1
```

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

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

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

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

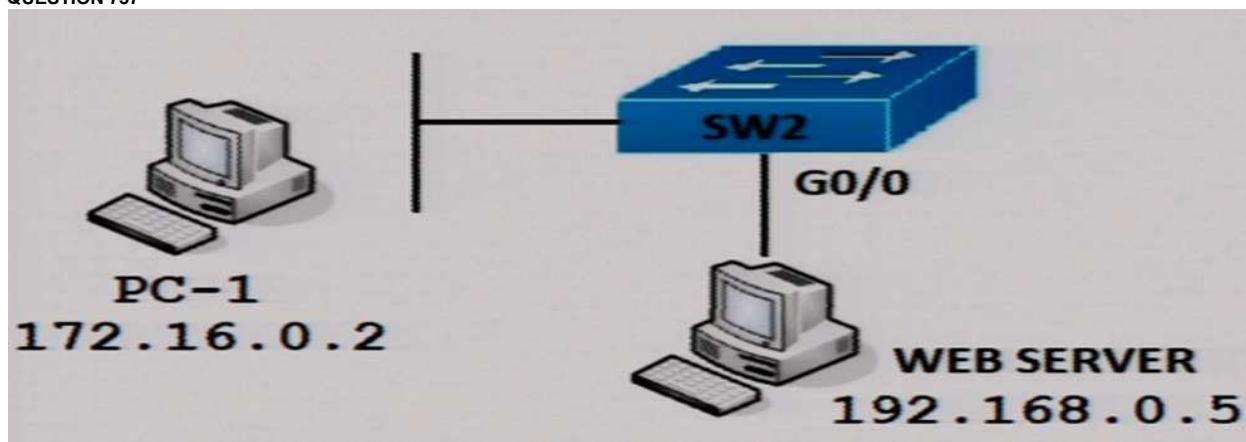
#### Explanation/Reference:

When forcing the ports to use EtherChannel in S1, no negotiation will occur. Hence S2 cannot negotiate an EtherChannel using PAgP with S1. Hence you need to change the setting in S1 to use PAgP e.g. "mode desirable".

Although the port channel is forced with "mode on" instead of through negotiation it can also be in Down state. For example, when error occur due to receiving BPDU from both underlying ports which err-disabled the underlying ports e.g.:

%PM-4-ERR\_DISABLE: channel-misconfig (STP) error detected on Po1, putting Fa0/1 in err-disable state  
%PM-4-ERR\_DISABLE: channel-misconfig (STP) error detected on Po1, putting Fa0/2 in err-disable state

**QUESTION 737**



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

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

**Correct Answer: A**

Section: (none)

Explanation

**Explanation/Reference:**

For inbound traffic entering g0/0, the web traffic is has a source 192.168.0.5:8080 and a destination 172.16.0.2:<some random port>. Hence the rule should be "permit tcp host 192.168.0.5 eq 8080 host 172.16.0.2"

**QUESTION 738**

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#427427300$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:")

with open("ifaces.json", "w") as f:
    f.write(updatedConfig)
```

- A. OutFile = open("ifaces.json","w")  
OutFile.write(UpdatedConfig)  
OutFile.close()
- B. OutFile = open("ifaces.json","w")  
json.dump(UpdatedConfig,OutFile)  
OutFile.close()
- C. OutFile = open("ifaces.json","w")  
OutFile.write(Response.json())  
OutFile.close()
- D. OutFile = open("ifaces.json","w")  
OutFile.write(Response.text)  
OutFile.close()

**Correct Answer: A**

Section: (none)

Explanation

**Explanation/Reference:**

In the last statement of the script:

- Response.text contains a JSON string representing the interface data.
- .replace() is then called to replace the IPv6 address in the above JSON string.
- The replaced JSON string is stored in "UpdatedConfig".

Since "UpdatedConfig" is already the replaced JSON string containing the changed interface configuration, you can just write it to a file directly with ".write(UpdatedConfig)"

Note that the changed configuration is just stored in the file "ifaces.json", the script does not send it to the router to make the change.

**QUESTION 739**

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

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

From the output:

- It shows Virtual IP address is 10.1.1.1
- It shows "Active router is 10.1.1.2, priority 255" and "Priority 100 (default 100)". Since local router is 100 but the active router is 255, local device does NOT have higher priority.
- It shows "Hello time 3 sec, hold time 10 sec" therefore takeover only occurs after 10 seconds (i.e. NOT more than 5 seconds).
- It shows "Hello time 3 sec, hold time 10 sec" which are default values therefore it is NOT custom values.

For the choice about higher IP address and same HSRP priority, the new router seems to take over to become the active router after a delay of 5 seconds (due to "Preemption enabled, delay min 5 sec"). However, this is only true if:

- The new router is configured with "standby 1 preempt" (whether the standby router configuration pre-empt setting shown in the exhibit is irrelevant).
- The router is running an IOS that will perform pre-empt with a higher IP address. Most IOS versions only consider the factor of IP address in initial election (i.e. no router has been elected as Active yet).

However, since there is no other choice that is correct. This is also included as the suggested answer.

**QUESTION 740**

```
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
```

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Error about retransmitting DBD often related to MTU problem.

**QUESTION 741**

```
interface GigabitEthernet1
ip address 10.10.10.1 255.255.255.0
!
access-list 10 permit 10.10.10.1
!
monitor session 10 type erspan-source
source interface G1
destination
  erspan-id 10
  ip address 192.168.1.1
!
```

Which command filters the ERSPAN session packets only to interface GtgbabitEthernet1?

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

**Correct Answer:** C

**Section:** (none)

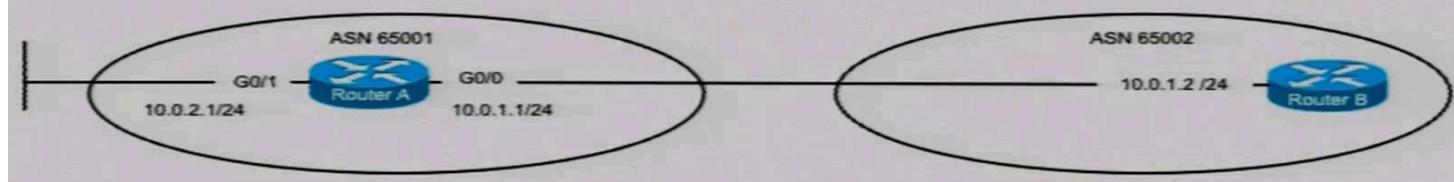
**Explanation**

**Explanation/Reference:**

You can perform filtering by "filter" command with an ACL.

```
filter {ip access-group {standard-access-list | expanded-access-list | acl-name} | ipv6 access-group acl-name | mac access-group acl-name} | vlan vlan-ID [, -]}
```

**QUESTION 742**



An engineer must configure an eBGP neighborship to Router B on Router A. The network that is connected to G0/1 on Router A must be advertised to Router B. Which configuration should be applied?

- A. router bgp 65002  
neighbor 10.0.1.2 remote-as 65002  
network 10.0.2.0 255.255.255.0
- B. router bgp 65001  
neighbor 10.0.1.2 remote-as 65002  
redistribute static
- C. router bgp 65001  
neighbor 10.0.1.2 remote-as 65002  
network 10.0.2.0 255.255.255.0
- D. router bgp 65001  
neighbor 10.0.1.2 remote-as 65002  
network 10.0.1.0 255.255.255.0

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since you need to configure RouterA, the AS number should be 65001 i.e. "router bgp 65001". For advertising the connected network of interface g0/1 "10.0.2.1/24", you need "network 10.0.2.0 mask 255.255.255.0".

Since the connected network is not a static route and all other choices are missing the keyword "mask". The one with "router bgp 65001" and "network 10.0.2.0 255.255.255.0" is selected as the answer.

**QUESTION 743**

What is provided to the Client to identify the authenticated session in subsequent API calls after authenticating to the Cisco DNA Center API?

- A. client X.509 certificate
- B. authentication token
- C. session cookie
- D. username and password

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Cisco DNA Center accepts REST requests from authenticated users only. To authenticate to Cisco DNA Center, you must submit your user credentials. Successful authentication returns an authorization token that you can use to issue subsequent requests.

**QUESTION 744**

What is one difference between the RIB and the FIB?

- A. The FIB contains routing prefixes, and the RIB contains the Layer 2 and Layer 3 information necessary to make a forwarding decision.
- B. The RIB is known as the CEF table, and the FIB is known as the routing table.
- C. The RIB works at the data plane, and the FIB works at the control plane.
- D. The RIB keeps all routing information received from peers, and the FIB keeps the minimum information necessary to make a forwarding decision.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 745**

What is the output of this code?

```
def get_credentials():
    creds={'username':'admin123456789','password':'7e3aea76f118'}
    return(creds.get('password'))

print(get_credentials())
```

- A. 7e3aea76f118
- B. get\_credentials
- C. password
- D. username: password

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

When getting from the key "username", it contains the value "admin123456789"

When getting from the key "password", it contains the value "7e3aea76f118"

Hence, the function get\_credentials() will return "7e3aea76f118" and this value will be printed.

**QUESTION 746**

Which notification method is used by the Intent API Event Management Domain?

- A. GET Event Count
- B. GET Event Series
- C. GET Subscriptions
- D. GET Events

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The Intent API Event Management Domain includes the following:

Event Methods:

GET Event Count: Return the number of defined Events.

GET Events: Obtain Event definition(s).

Subscription Methods:

POST Subscription: Create one or more new event subscriptions.

GET Subscriptions: Read information about one or more event subscriptions.

PUT Subscription: Update one or more existing event subscriptions.

DELETE Subscription: Delete one or more event subscriptions.

GET Subscription Count: Get the number of existing subscriptions.

Synchronous Notification / Event-Series Methods:

GET Event Series (Notification) Count: Return a count of Event occurrences matching request filter criteria.

GET Event Series (Notification) Content: Get Event occurrence information matching request filter criteria.

**QUESTION 747**

Why would a customer implement an on-premises solution instead of a cloud solution?

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

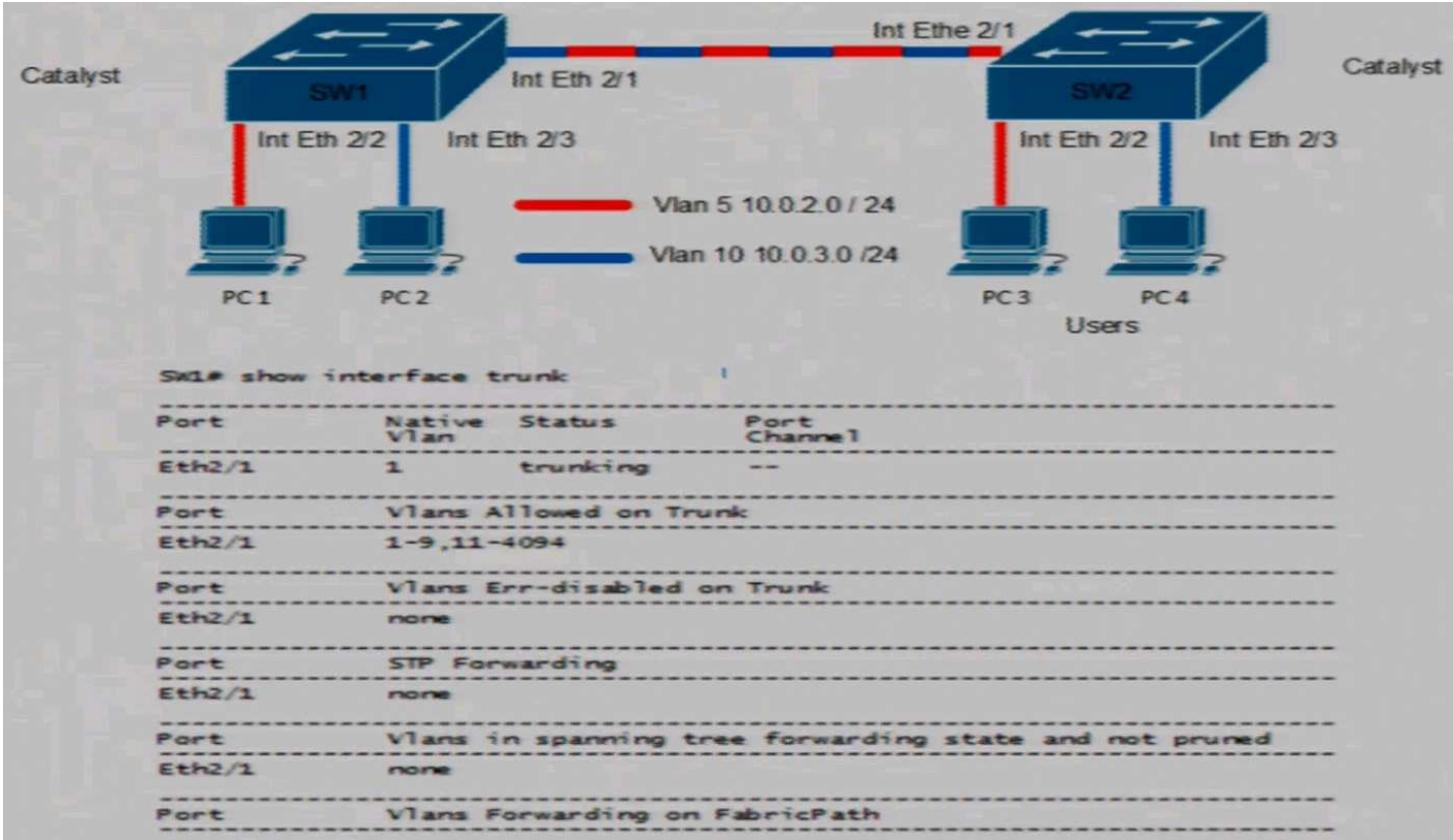
**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 748**



PC 2 cannot communicate with PC 4. Which configuration resolves this issue?

- A. SW1(config)# interface Gigabitethernet 2/1  
SW1(config-if)# switchport trunk allowed vlan add 10
- B. SW1(config)# interface Gigabitethernet 2/1  
SW1(config-if)# switchport mode trunk
- C. SW1(config)# interface Gigabitethernet 2/1  
SW1(config-if)# switchport mode access  
SW1(config-if)# switchport access vlan 10
- D. SW1(config)# interface Gigabitethernet 2/1  
SW1(config-if)# switchport vlan mapping 10 10

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

From the command output, only VLANs "1-9,11-4096" are allowed in the trunk link e2/1. Since PC2 and PC4 are connected with blue lines i.e. VLAN 10, you need to add VLAN 10 to the allowed VLAN.

**QUESTION 749**

The Gig0/0 interface of two routers is directly connected with a 1G Ethernet link. Which configuration must be applied to the interface of both routers to establish an OSPF adjacency without maintaining a DR/BDR relationship?

- A. interface Gig0/0  
ip ospf network point-to-multipoint
- B. interface Gig0/0  
ip ospf network broadcast
- C. interface Gig0/0  
ip ospf network point-to-point
- D. interface Gig0/0  
ip ospf network non-broadcast

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The simplest way to form OSPF neighbors between two and only two directly connected neighbors without the use of DR is "point-to-point".

**QUESTION 750**

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

**Select and Place:**

```

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

```

deny      access-list-seq-rule      dst-any      ip

Correct Answer:

```

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

```

[ ]      [ ]      [ ]      [ ]

Section: Selected  
Explanation

**Explanation/Reference:**

Remarks :

A similar configuration in XML format:

```

<ip>
  <access-list>
    <ios-acl:extended>
      <ios-acl:name>ato </ios-acl:name>
      <ios-acl:access-list-seq-rule>
        <ios-acl:sequence>111111</ios-acl:sequence>
        <ios-acl:ace-rule>
          <ios-acl:action>deny</ios-acl:action>
          <ios-acl:protocol>ip</ios-acl:protocol>
          <ios-acl:any/>
          <ios-acl:dst-any/>
        </ios-acl:ace-rule>
      </ios-acl:access-list-seq-rule>
    </ios-acl:extended>

  </access-list>
</ip>

```

#### QUESTION 751

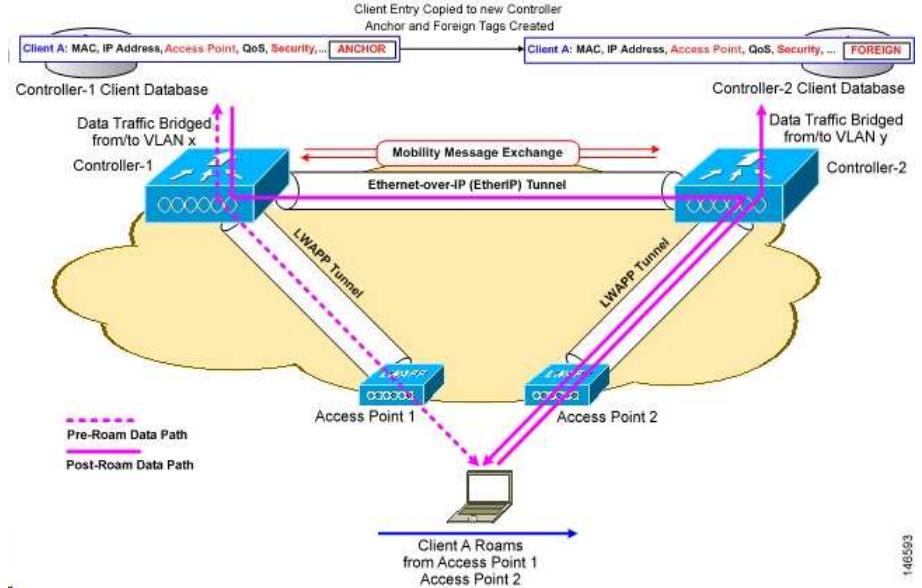
A large campus network has deployed two wireless LAN controllers to manage the wireless network. WLC1 and WLC2 have been configured as mobility peers. A client device roams from AP1 on WLC1 to AP2 on WLC2, but the controller's client interfaces are on different VLANs. How do the wireless LAN controllers handle the inter-subnet roaming?

- A. WLC1 marks the client with an anchor entry in its own database. The database entry is copied to the new controller and marked with a foreign entry on WLC2.
- B. WLC2 marks the client with an anchor entry in its own database. The database entry is copied to the new controller and marked with a foreign entry on WLC1.
- C. WLC1 marks the client with a foreign entry in its own database. The database entry is copied to the new controller and marked with an anchor entry on WLC2.
- D. WLC2 marks the client with a foreign entry in its own database. The database entry is copied to the new controller and marked with an anchor entry on WLC1.

Correct Answer: A

Section: (none)

Explanation

**Explanation/Reference:****QUESTION 752**

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

- biometric authentication
- nonrepudiation feature
- password hash
- SSL certificates

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

SSL certificate can verify identity of a target device and it ensures that you are connecting to the target device not someone else's device in the middle.

**QUESTION 753**

Which technology provides an overlay fabric to connect remote locations utilizing commodity data paths and improves network performance, boosts security, and reduces costs?

- InfiniBand
- VXLAN
- SD-WAN
- VTEP

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 754**

```
from ncclient import manager
```

```
with manager.connect(host=host, port=830, username=user, hostkey_verify=False) as m:
    c = m.get_config(source='running').data_xml
    with open("%s.xml" % host, 'w') as f:
        f.write(c)
```

What is generated by the script?

- the routing table
- the running configuration
- the cdp neighbors
- the router processes

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Remarks:

The "open()" and "write()" in the script stores the running configuration gathered into an XML file.

**QUESTION 755**

Which language defines the structure or modeling of data for NETCONF and RESTCONF?

- A. YANG
- B. XML
- C. JSON
- D. YAML

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 756**

What is a characteristic of traffic shaping?

- A. can be applied in both traffic directions
- B. causes TCP retransmits when packets are dropped
- C. drops out-of-profile packets
- D. queues out-of-profile packets until the buffer is full

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 757**

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

What are the characteristics of FIB? (Choose two.)

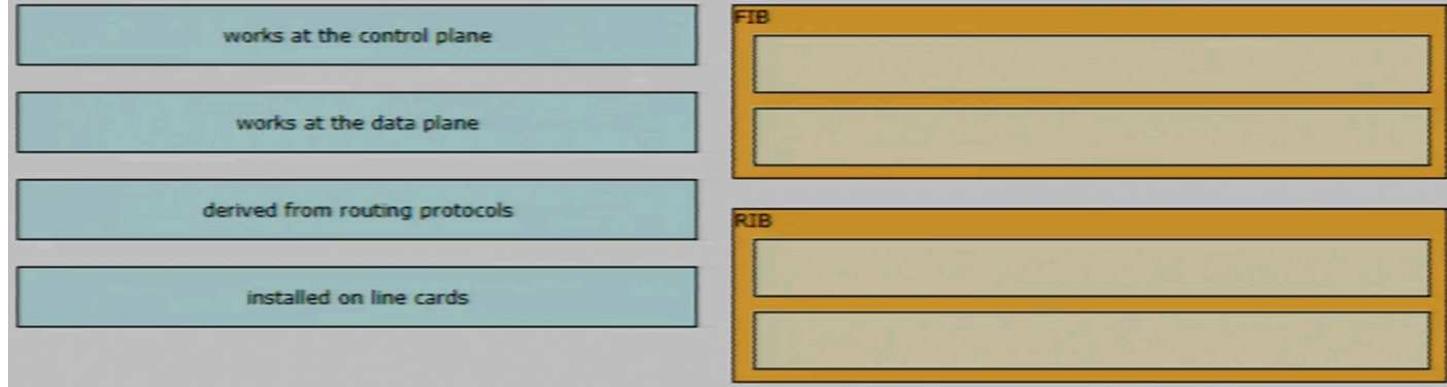
- A. works at the control plane
- B. works at the data plane
- C. derived from routing protocols
- D. installed on line cards

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 758**

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

What are the characteristics of RIB? (Choose two.)

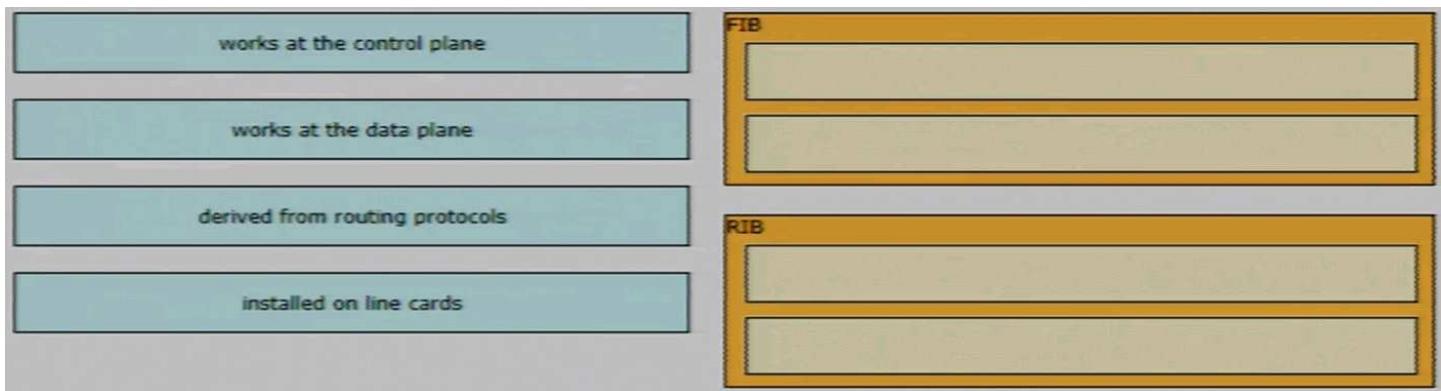
- A. works at the control plane
- B. works at the data plane
- C. derived from routing protocols
- D. installed on line cards

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 759

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

When DHCP servers are programmed to offer WLAN Controller IP addresses as Option 43 for Cisco Aironet LAPs, the sub-option TLV block is defined in this way:  
Type - 0xf1 (decimal 241).

Length - Number of controller IP addresses \* 4.

Value - List of the WLC management interfaces, typically translated to hexadecimal values.

#### QUESTION 760

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In order to authenticate over the network, you need to use RADIUS (or TACACS+).

#### QUESTION 761

<pre> Ethernet II, Src: ca:01:3c:cc:00:00 (ca:01:3c:cc:00:00), Dst:    Internet Protocol Version 4, Src: 10.1.1.132 (10.1.1.132), Dst:      Header checksum: 0xccf3 [validation disabled]     Source: 10.1.1.132 (10.1.1.132)     Destination: 224.0.0.10 (224.0.0.10)     [Source GeoIP: Unknown]     [Destination GeoIP: Unknown]  Cisco EIGRP   Version: 2   Opcode: Hello (5)   Checksum: 0xcd34 [correct]   Flags: 0x00000000   Sequence: 0   Acknowledge: 0   Virtual Router ID: 0 (Address-Family)   Autonomous System: 100   Authentication MDS     Type: Authentication (0x0002)     Length: 40     Type: MDS (2)     Length: 16     Key ID: 1     Key Sequence: 0     Nullpad: 0000000000000000     Digest: 58a4118e96f5888f6e10bd1b537618a2    Parameters     Type: Parameters (0x0001)     Length: 12     K1: 1     K2: 0     K3: 1     K4: 1     K5: 0     K6: 0     Hold Time: 15   </pre>	<pre> Ethernet II, Src: ca:02:58:e4:00:00 (ca:02:58:e4:00:00), Dst:    Internet Protocol Version 4, Src: 10.1.1.133 (10.1.1.133), Dst:      Header checksum: 0xccf2 [validation disabled]     Source: 10.1.1.133 (10.1.1.133)     Destination: 224.0.0.10 (224.0.0.10)     [Source GeoIP: Unknown]     [Destination GeoIP: Unknown]  Cisco EIGRP   Version: 2   Opcode: Hello (5)   Checksum: 0xffc7 [correct]   Flags: 0x00000000   Sequence: 0   Acknowledge: 0   Virtual Router ID: 0 (Address-Family)   Autonomous System: 100   Authentication MDS     Type: Authentication (0x0002)     Length: 40     Type: MDS (2)     Length: 16     Key ID: 0     Key Sequence: 0     Nullpad: 0000000000000000     Digest: 9a5868fec6d13f7569504a1381b6afb6    Parameters     Type: Parameters (0x0001)     Length: 12     K1: 1     K2: 0     K3: 1     K4: 1     K5: 0     K6: 0     Hold Time: 10   </pre>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

An engineer configures EIGRP but the routers fail to form a neighborship. What is the reason for the failure?

- A. The hold timers do not match.
- B. The MD5 digests do not match.
- C. The key IDs do not match.
- D. The K-values are invalid.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

For EIGRP neighbors, they do not need to have the same hold timers or use the same key IDs for the password / MD5 digest.

From the output, the K values of the two routes match. However, their MD5 digests do not match: one has a digest starting with "5" but the other has a different digest starting with "9".

#### QUESTION 762

Which configuration filters out DOT1X messages in the format shown below from being sent toward Syslog server 10.15.20.33?

Nov 20 13:37:13.446: %DOT1X-5-FAIL: Authentication failed for client (e04f.645f.ab3e) on Interface GigabitEthernet0/1 AuditSessionID 0A0649B4000003292688001F

- A. logging discriminator DOT1X facility drops DOT1X  
logging host 10.15.20.33 discriminator DOT1X
- B. logging discriminator DOT1X msg-body drops DOT1X  
logging host 10.15.20.33 discriminator DOT1X
- C. logging discriminator DOT1X mnemonics includes DOT1X  
logging host 10.15.20.33 discriminator DOT1X
- D. logging discriminator DOT1X mnemonics includes DOT1X  
logging host 10.15.20.33 discriminator DOT1X

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

You need a logging discriminator that drop a message if it contains the word "DOT1X" i.e.

logging discriminator XXX mnemonics drops DOT1X

logging host 10.15.20.33 discriminator XXX

The "XXX" above is the name of the logging discriminator. You can use any name you like as long as you use the same name in the two commands above.

#### QUESTION 763

What is a characteristic of a Type 2 hypervisor?

- A. It is completely independent of the operating system.
- B. Its main task is to manage hardware resources between different operating systems.
- C. It is installed on an operating system and supports other operating systems .
- D. It eliminates the need for an underlying operating system.

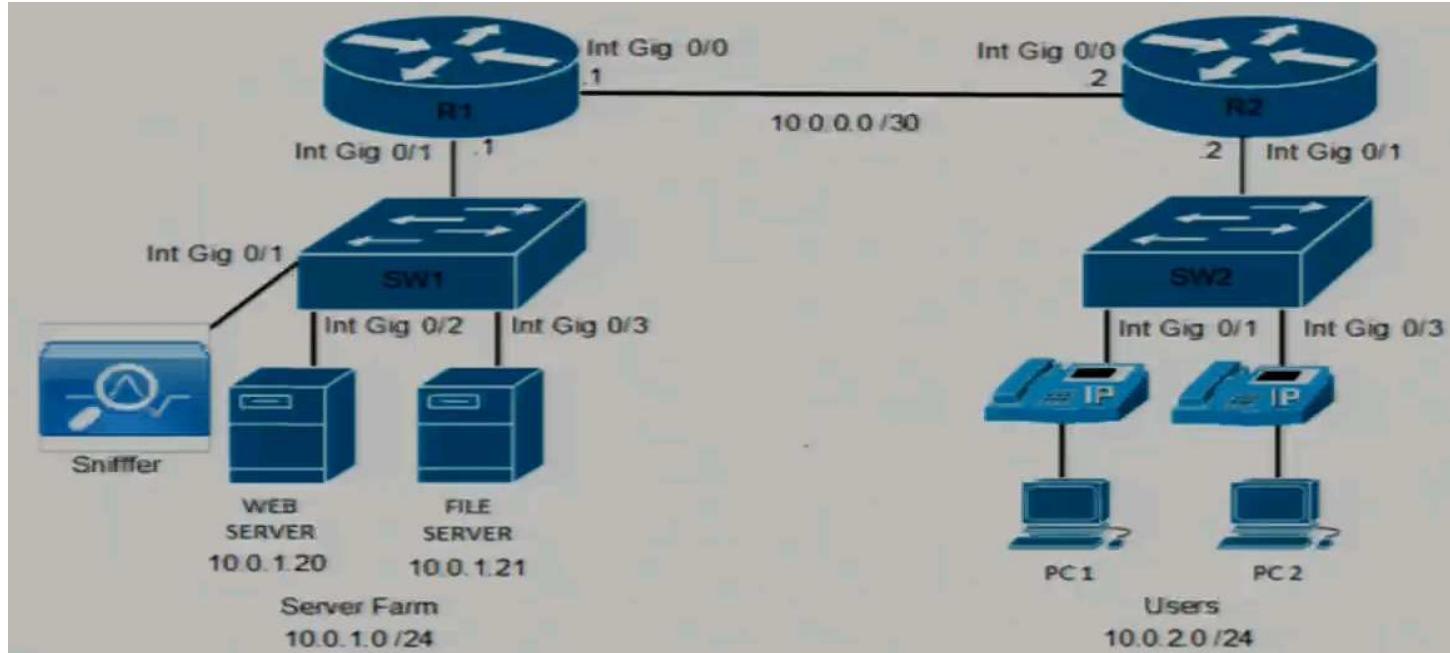
**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 764



A network engineer is troubleshooting an issue with the file server based on reports of slow file transmissions. Which two commands or command sets are required in switch SW1 to analyze the traffic from the file server with a packet analyzer? (Choose two.)

- A. SW1#show ip route
- B. SW1(config)# monitor session 1 source interface gigabitethernet0/1  
SW1(config)# monitor session 1 destination interface gigabitethernet0/3 encapsulation replicate
- C. SW1#show vlan
- D. SW1#show monitor
- E. SW1(config)# monitor session 1 source interface gigabitethernet0/3  
SW1(config)# monitor session 1 destination interface gigabitethernet0/1 encapsulation replicate

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since the file server is connected to SW1's g0/3 and the sniffer is connected to SW1's g0/1, you need to configure a SPAN session with source interface g0/3 and with destination interface g0/1.

From the diagram, since only one network 10.0.1.0/24 is specified on the left side of the diagram (i.e. Server Farm), SW1 is probably configured as a Layer 2 switch without IP routing. Hence, instead of using "sh ip route", you should use "show vlan" to find out if there is any layer 2 problem in SW1.

**QUESTION 765**

Which LISP component decapsulates messages and forwards them to the map server responsible for the egress tunnel routers?

- A. Proxy ETR
- B. Router Locator
- C. Ingress Tunnel Router
- D. Map Resolver

**Correct Answer:** D

**Section:** (none)

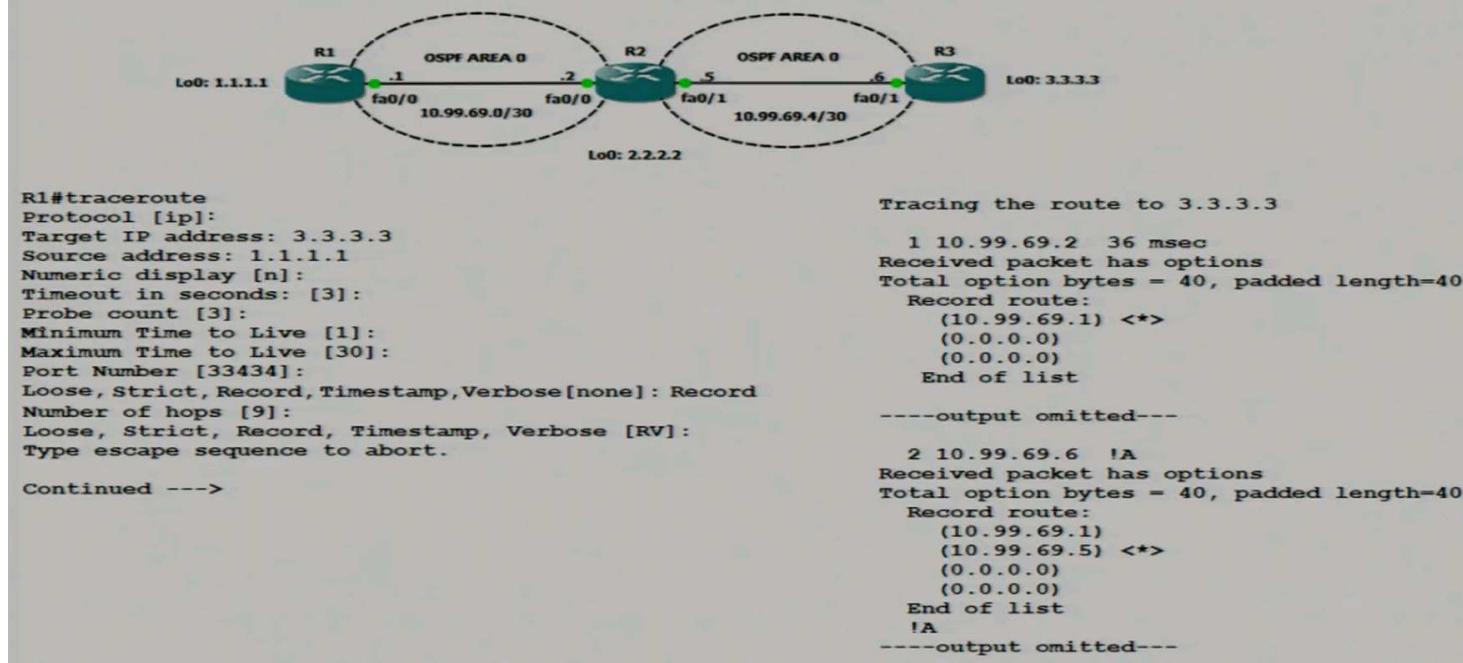
**Explanation**

**Explanation/Reference:**

Map resolver (MR): The MR performs the following functions:

- Receives MAP requests, which are encapsulated by ITRs.
- Provides a service interface to the ALT router, de-encapsulates MAP requests, and checks the Map Server (MS) to locate the proper ETR response to the requests.
- Sends negative MAP replies in response to MAP requests for non-LISP sites.

**QUESTION 766**



The traceroute fails from R1 to R3. What is the cause of the failure?

- A. An ACL applied inbound on loopback0 of R2 is dropping the traffic.
- B. An ACL applied inbound on fa0/1 of R3 is dropping the traffic.
- C. Redistribution of connected routes into OSPF is not configured.
- D. The loopback on R3 is in a shutdown state.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The "!A" response found in the output from traceroute command indicates that a response of Administratively Prohibited has been received. This usually means that the traceroute packet is blocked by e.g. an access list.

Since the Administratively Prohibited response is sent to the source of the packet, it is the traceroute packet sourced from R1 that is being blocked. Hence, the access list denying the packet is being applied to R3's f0/1 for blocking inbound traffic.

**QUESTION 767**

What is an advantage of utilizing data models in a multivendor environment?

- A. improving communication security with binary-encoded protocols
- B. removing the distinction between configuration and runtime state data
- C. lowering CPU load incurred to managed devices
- D. facilitating a unified approach to configuration and management

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 768**

Drag and drop the characteristics from the left onto the deployment models on the right.  
Which are the characteristics of Cloud (Choose two)?

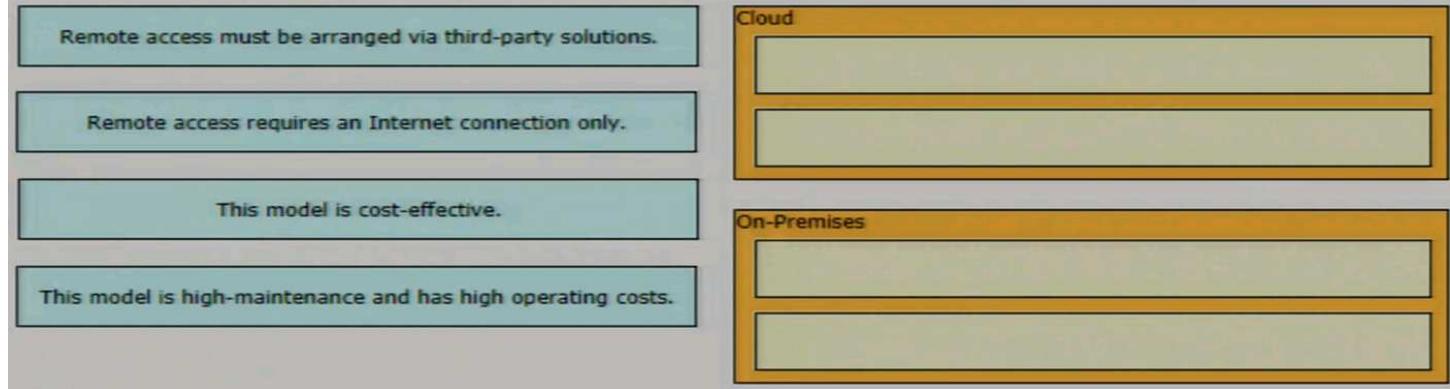
- A. Remote access must be arranged via third-party solutions.
- B. Remote access requires an Internet connection only.
- C. This model is cost-effective.
- D. This model is high-maintenance and has high operating costs.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 769**

Drag and drop the characteristics from the left onto the deployment models on the right.  
Which are the characteristics of On-Premises (Choose two)?

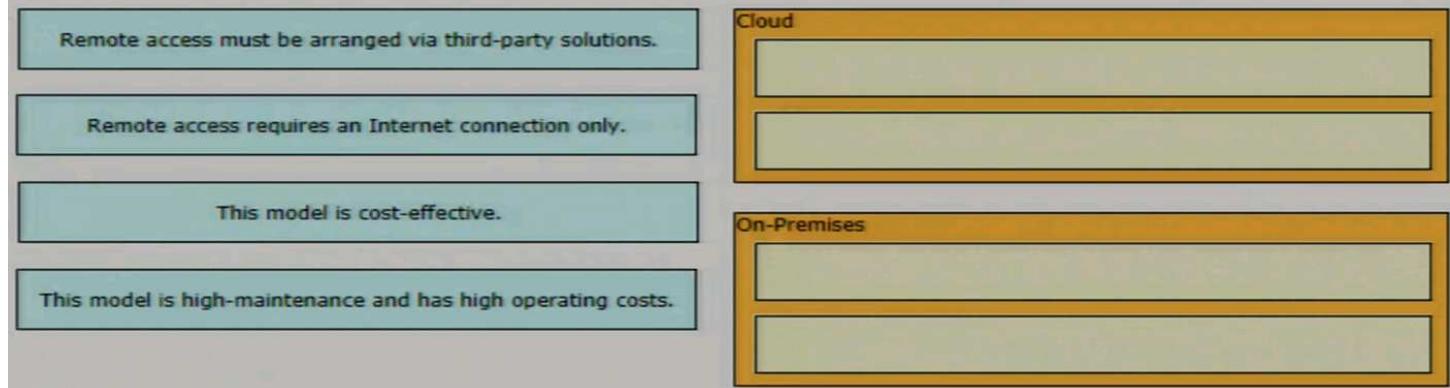
- A. Remote access must be arranged via third-party solutions.
- B. Remote access requires an Internet connection only.
- C. This model is cost-effective.
- D. This model is high-maintenance and has high operating costs.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



For remote access, Cloud Service Provider usually provide many solutions for you to access your subscribed services easily.

**QUESTION 770**

```

interface Ethernet0/0
    ipaddress 10.1.1.1 255.255.255.252
    ip natoutside
!
interface Ethernet0/0
    ipaddress 10.10.10.1 255.255.255.0
    ip natinside
!
ip nat inside source static 10.10.10.10 10.0.3.10

```

Which address type is 10.10.10.10 configured for?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

The first IP in the command i.e. 10.10.10.10 is "inside local" and the second IP in the command i.e. 10.0.3.10 is "inside global".

```

R1(config)#ip nat inside source static ?
  A.B.C.D  Inside local  IP address
  esp      IPSec-ESP (Tunnel mode) support
  network   Subnet translation
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol

R1(config)#ip nat inside source static 10.10.10.10 ?
  A.B.C.D  Inside global  IP address
  interface Specify interface for global address

```

**QUESTION 771**

How do EIGRP and OSPF differ?

- A. EIGRP sends full routing updates, and OSPF sends partial updates.
- B. EIGRP uses query packets to request routing information, and OSPF uses LSU packets.
- C. EIGRP sends partial routing updates and OSPF sends full updates.
- D. EIGRP sends unicast routing updates, and OSPF sends multicast routing updates.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Other choices are surely wrong since:

both EIGRP and OSPF can send partial updates.

EIGRP can either send unicast or multicast updates.

For the remaining choice, EIGRP can use query packets to request routing information. OSPF can also request routing information using LSR (Link-State Request). This choice is chosen although it specifies "LSU" instead of "LSR".

**QUESTION 772**

What is a benefit of using segmentation with TrustSec?

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

With Cisco TrustSec, a network administrator can implement extensive network segmentation and endpoint access controls without modifying network topology (e.g. additional VLANs) and rule administration, which greatly simplifies IT engineering and operations.

Since the question is asking about benefits provided by segmentation, the choice mentioning firewall rules should be the answer since the configuration of rules does not depend on the physical network topology.

**QUESTION 773**

What does the Cisco DNA Center Authentication API provide?

- A. list of global issues that are logged in Cisco DNA Center
- B. access token to make calls to Cisco DNA Center
- C. client health status
- D. list of VLAN names

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 774

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

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

**Correct Answer:** AC

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Edge Node provides first-hop services for Users / Devices connected to a Fabric

- Responsible for Identifying and Authenticating Endpoints (e.g. Static, 802.1X, Active Directory)
- Register specific Endpoint ID info (e.g. /32 or /128) with the Control-Plane Node(s)
- Provide an Anycast L3 Gateway for the connected Endpoints (same IP address on all Edge nodes)
- Performs encapsulation / de-encapsulation of data traffic to and from all connected Endpoints

**Remarks:**

Entry & Exit points for data traffic going Into & Out of a Fabric are provided by Broader Nodes.

#### QUESTION 775

Which Python library is used to work with YANG data models via NETCONF?

- A. Postman
- B. requests
- C. cURL
- D. ncclient

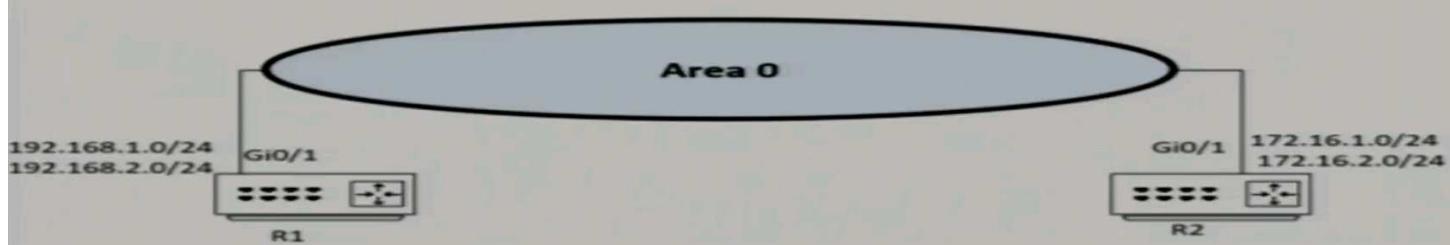
**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 776



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

- A. R1
 

```
router ospf 0
network 192.168.1.0 255.255.255.0 area 0
network 192.168.2.0 255.255.255.0 area 0
```
- B. R2
 

```
router ospf 0
network 172.16.1.0 0.0.0.255 area 0
network 172.16.2.0 0.0.0.255 area 0
```
- C. R1
 

```
router ospf 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
```
- D. R2
 

```
router ospf 0
network 172.16.1.0 255.255.255.0 area 0
network 172.16.2.0 255.255.255.0 area 0
```
- E. R2
 

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

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

OSPF network command officially requires wildcard masks.

Remarks:

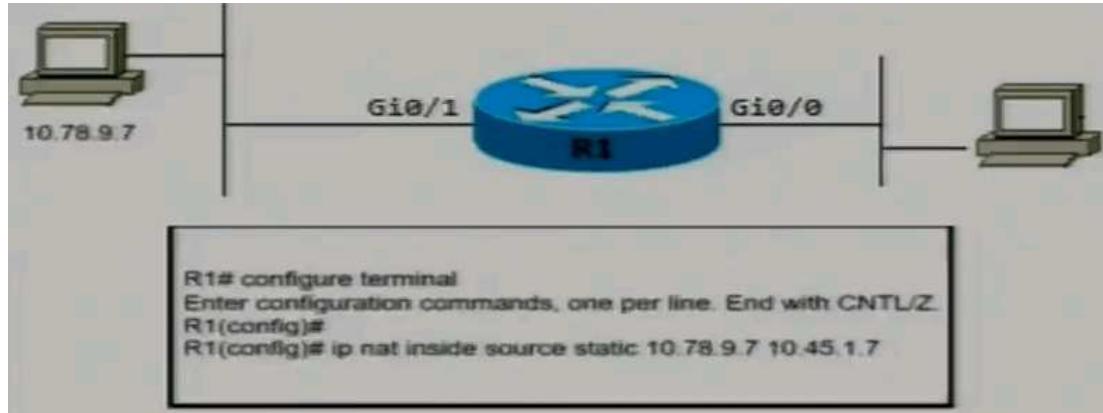
Actually there are two problems in this question:

1. Process ID "0" is NOT allowed.

```
R2(config)#router ospf 0
^
% Invalid input detected at '^' marker.
```

```
R2(config)#router ospf ?
<1-65535> Process ID
```

2. Most IOS accepts network mask in the "network" command of OSPF and converts it to wildcard mask for entering into running configuration automatically.

**QUESTION 777**

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

- A. R1(config)# interface GigabitEthernet 0/0  
R1(config)# ip pat inside

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

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

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

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

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

- D. R1(config)# interface GigabitEthernet 0/0  
R1(config)# ip pat outside

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Since "10.78.9.7" is inside local address of a host in the inside network, the interface connecting to it i.e. "g0/1" should be configured with "ip nat inside". Hence, the other interface i.e. "g0/0" should be configured with "ip nat outside".

Note that there is no valid command starting with "ip pat ....".

```
R2(config-if)#ip pat ?
% Unrecognized command
```

**QUESTION 778**

What is a concern when implementing virtual switching in a hypervisor?

- virtual CPU data bus bandwidth limitations
- packet forwarding across multiple virtual collision domains
- incorrect duplex, speed, and negotiation configuration for virtual interfaces
- broadcast domain isolation meeting corporate security policies

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 779**

```

<?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>
]]>]]>

```

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The use of "<nc:get>" is to read data and a "filter" section is included to get the IP address information of g1 only.

**QUESTION 780**

Which device is responsible for finding EID-to-RLOC mappings when traffic is sent to a LISP-capable site?

- A. egress tunnel router
- B. ingress tunnel router
- C. map server
- D. map resolver

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The function of the LISP MR is to accept encapsulated Map-Request messages from ingress tunnel routers (ITRs), decapsulate those messages, and then forward the messages to the MS responsible for the egress tunnel routers (ETRs) that are authoritative for the requested EIDs.

An ITR is responsible for finding EID-to-RLOC mappings for all traffic destined for LISP-capable sites. When the ITR receives a packet destined for an EID, it first looks for the EID in its mapping cache. If the ITR finds a match, it encapsulates the packet inside a LISP header with one of its RLOCs as the IP source address and one of the RLOCs from the mapping cache entry as the IP destination. The ITR then routes the packet normally. If no entry is found in the ITR's mapping cache, the ITR sends a Map-Request message to one of its configured map resolvers and then discards the original packet.

**QUESTION 781**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Cisco DNA Center allows you to designate software images and SMUs as golden. A golden software image or SMU is a validated image that meets the compliance requirements for the particular device type.

**QUESTION 782**

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

- A. interface GigabitEthernet0/0  
ip address 10.10.10.2 255.255.255.0  
vrrp 65 ip 10.10.10.1  
vrrp 65 priority 110
- B. interface GigabitEthernet0/0  
ip address 10.10.10.1 255.255.255.0  
vrrp 65 ip 10.10.10.1  
standby 65 priority 100  
standby 65 preempt
- C. interface GigabitEthernet0/0  
ip address 10.10.10.2 255.255.255.0  
standby 65 ip 10.10.10.1  
standby 65 track 1 decrement 10  
standby 65 preempt
- D. interface GigabitEthernet0/0  
ip address 10.10.10.2 255.255.255.0  
vrrp 65 ip 10.20.20.1  
vrrp 65 track 1 decrement 100  
vrrp 65 preempt  
vrrp 65 authentication \$3#5621280826

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since the question is about VRRP, the choices with "standby" command are NOT correct. Moreover, the IP address in the physical interface should be in the same subnet as the Virtual IP address (e.g. 10.10.10.2/24 and 10.20.20.1 is NOT in the same subnet.)

Note that "preempt" is enabled by default in VRRP and therefore there is **no need** to configure the "vrrp 65 preempt" command.

**QUESTION 783**

How do cloud deployments compare to on-premises deployments?

- A. Cloud deployments provide a better user experience across world regions, whereas on-premises deployments depend upon region-specific conditions.
- B. Cloud deployments mandate a secure architecture, whereas on-premises deployments are inherently unsecure.
- C. Cloud deployments are inherently unsecure, whereas a secure architecture is mandatory for on-premises deployments.
- D. Cloud deployments must include automation infrastructure, whereas on-premises deployments often lack the ability for automation.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 784**

```
access-list 1 permit 172.16.1.0 0.0.0.255
ip nat inside source list 1 interface gigabitethernet0/0 overload
```

Refer to the exhibit. The inside and outside interfaces in the NAT configuration of this device have been correctly identified. What is the effect of this configuration?

- A. static NAT
- B. NAT64
- C. dynamic NAT
- D. PAT

**Correct Answer:** D

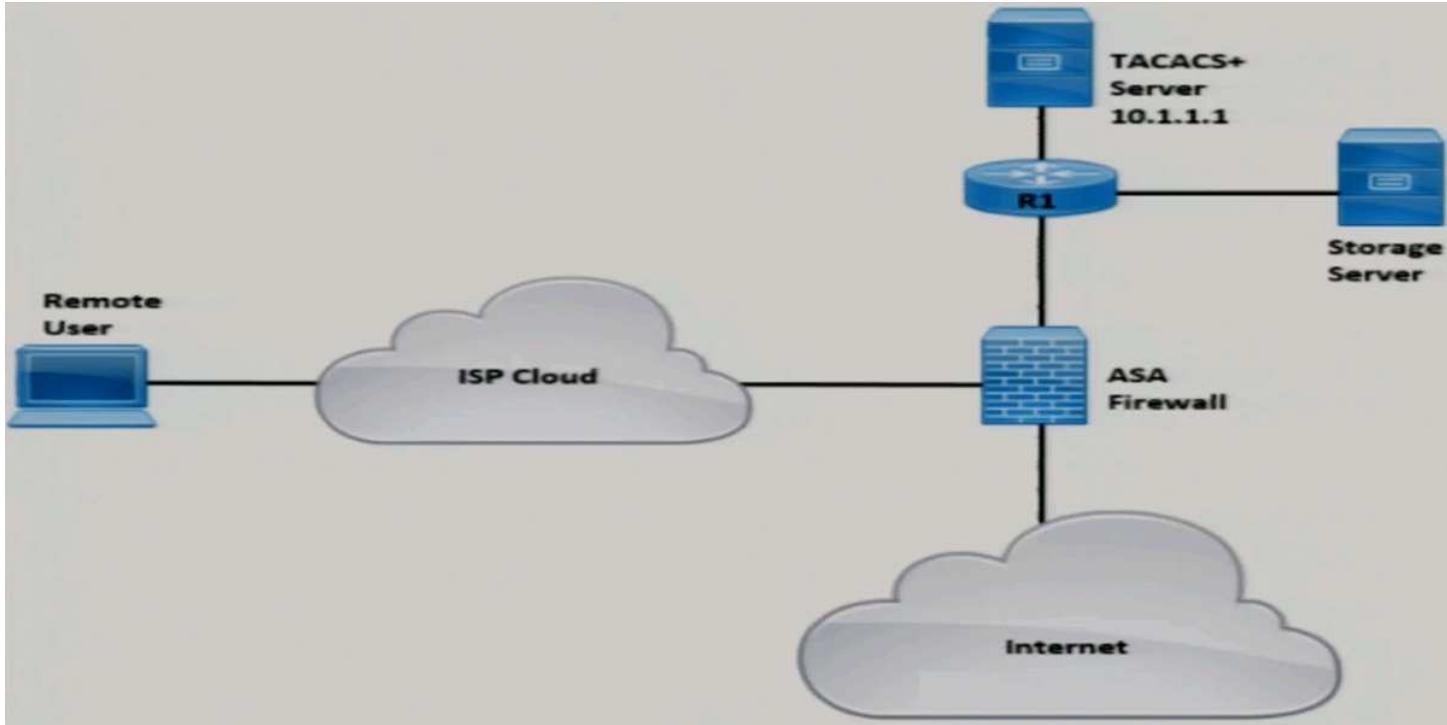
**Section:** (none)

**Explanation**

**Explanation/Reference:**

The keyword "overload" make the configuration become a Port Address Translation setting.

**QUESTION 785**



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

- A. ciscoasa(config)# access-list HTTP\_AUTH extended permit udp any any eq http  
ciscoasa(config)# aaa authentication listener http outside port 43
- B. ciscoasa(config)# access-list MAIL\_AUTH extended permit udp any any eq http  
ciscoasa(config)# aaa authentication listener http outside redirect
- C. ciscoasa(config)# access-list MAIL\_AUTH extended permit tcp any any eq http  
ciscoasa(config)# aaa authentication listener http inside port 43
- D. ciscoasa(config)# access-list MAIL\_AUTH extended permit tcp any any eq www  
ciscoasa(config)# aaa authentication listener http inside redirect

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The question is about configuring a Cisco ASA firewall for Network Access Authentication. According to a Cisco documentation, the sample configuration for authenticating all inside HTTP traffic and SMTP traffic:

```

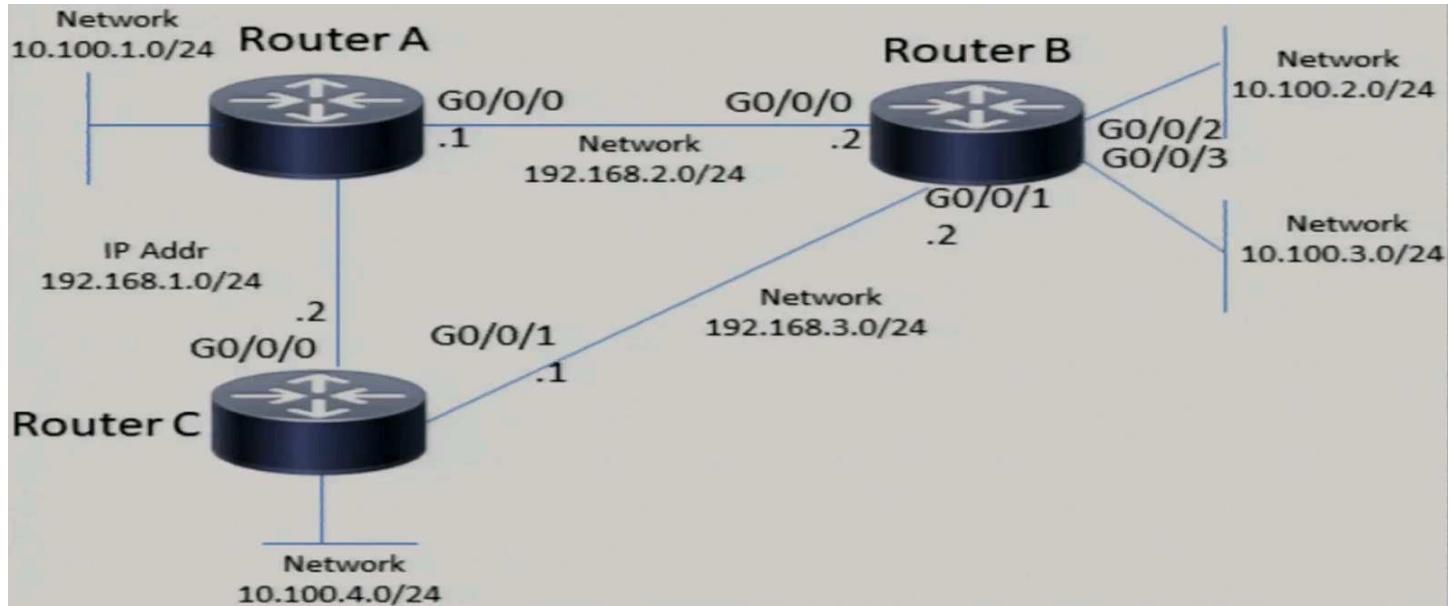
hostname(config)# aaa-server AuthOutbound protocol tacacs+
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthOutbound (inside) host 10.1.1.1
hostname(config-aaa-server-host)# key TACPlusUauthKey
hostname(config-aaa-server-host)# exit
hostname(config)# access-list MAIL_AUTH extended permit tcp any any eq smtp
hostname(config)# access-list MAIL_AUTH extended permit tcp any any eq www
hostname(config)# aaa authentication match MAIL_AUTH inside AuthOutbound
hostname(config)# aaa authentication listener http inside redirect

```

The correct answer can be chosen by checking the last command in the choices.

Moreover, the other choices are also NOT correct since the keyword for port 80 is "www" (i.e. NOT "http").

**QUESTION 786**



Refer to the exhibit. A network administrator must configure router B to allow traffic only from network 10.100.2.0 to networks outside of router B. Which configuration must be applied?

- A. RouterB(config)# access-list 101 permit ip 10.100.3.0 0.0.0.255 any  
 RouterB(config)# access-list 101 deny any  
 RouterB(config)# int g0/0/0  
 RouterB(config-if)# ip access-group 101 out  
 RouterB(config)# int g0/0/1  
 RouterB(config-if)# ip access-group 101 out
- B. RouterB(config)# access-list 101 permit ip 10.100.2.0 0.0.0.255 any  
 RouterB(config)# access-list 101 deny any  
 RouterB(config)# int g0/0/0  
 RouterB(config-if)# ip access-group 101 out
- C. RouterB(config)# access-list 101 permit ip 10.100.2.0 0.0.0.255 any  
 RouterB(config)# access-list 101 deny any  
 RouterB(config)# int g0/0/2  
 RouterB(config-if)# ip access-group 101 in
- D. RouterB(config)# access-list 101 permit ip 10.100.2.0 0.0.0.255 any  
 RouterB(config)# int g0/0/0  
 RouterB(config-if)# ip access-group 101 out  
 RouterB(config)# int g0/0/1  
 RouterB(config-if)# ip access-group 101 out

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

For this question, you need to block 10.100.3.0/24 from accessing all networks except 10.100.2.0/24

You can configure ACL in two ways:

- Configure an ACL with a single rule to allow traffic from 10.100.3.0/24 to 10.100.2.0/24 and apply it to the interface g0/0/3 in the inbound direction.
- Configure an ACL with a single rule to allow traffic from 10.100.2.0/24 to any and apply it to the interface g0/0/0 and g0/0/1 in the outbound direction.

**QUESTION 787**

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

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

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 788**

```

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

```

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

- A. ip route vrf Customer1 172.16.1.1 255.255.255.255 172.16.1.1 global  
ip route vrf Customer2 192.168.1.200 255.255.255.0 192.168.1.1 global
  - B. ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customer1  
ip route vrf Customer2 192.168.1.200 255.255.255.255 192.168.1.1 Customer2
  - C. ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customer2  
ip route vrf Customer2 192.168.1.200 255.255.255.255 192.168.1.1 Customer1
  - D. ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 global  
ip route vrf Customer2 192.168.1.200 255.255.255.255 192.168.1.1 global
- ip route 192.168.1.0 255.255.255.0 Vlan10  
ip route 172.16.1.0 255.255.255.0 Vlan20

**Correct Answer:** D

**Section:** (none)

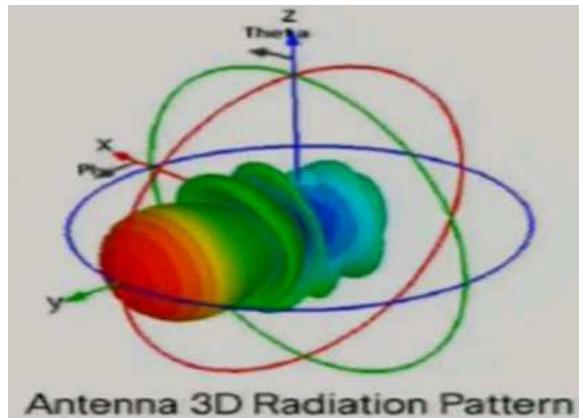
**Explanation**

**Explanation/Reference:**

For inter-vrf routing, you need to configure static route in each VRF through global.

Since you need to allow any hosts in Customer2, you need to configure a static route for 172.16.1.0/24 in vrf Customer1 (i.e. not the IP address 172.16.1.1/32 of the router).

**QUESTION 789**



Refer to the exhibit. Which type of antenna does the radiation pattern represent?

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

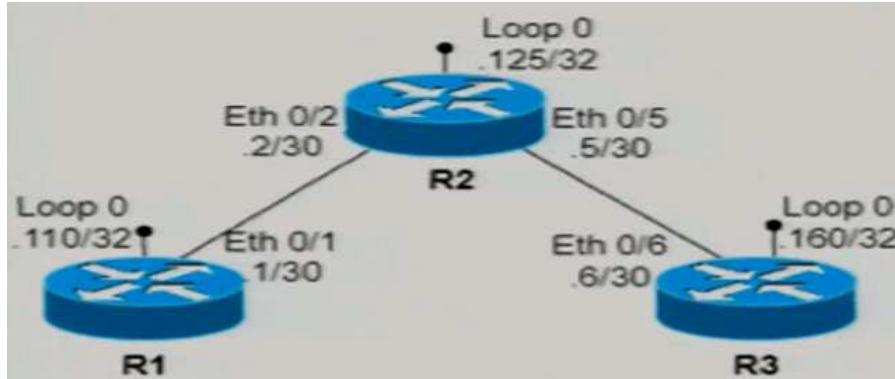
**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 790**



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

A. R1

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

R2

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

R3

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

B. R1

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

R3

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

C. R1

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

R3

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

D. R1

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

R3

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

For building GRE tunnel between R1 and R3, you just need to configure tunnel interfaces in these two routers.

For all the choices, the tunnel is configured using loopback 0 of the two routers. Hence, the tunnel sources are loopback0 and:

For tunnel interface in R1, the tunnel destination is R3's loopback0 i.e. x.y.z.160

For tunnel interface in R3, the tunnel destination is R1's loopback0 i.e. x.y.z.110

**QUESTION 791**



```
R1# show run int tunnel 0
Building configuration...
Current configuration : 127 bytes
!
interface Tunnel0
ip address 192.168.1.1 255.255.255.252
tunnel source FastEthernet1/0
tunnel destination 200.1.1.1
end
```

```
R2# show run int tunnel 0
Building configuration...
Current configuration : 125 bytes
!
interface Tunnel0
ip address 192.168.1.2 255.255.255.252
tunnel destination 100.1.1.1
end
```

```
R1#show interfaces tunnel 0
Tunnel0 is up, line protocol is up
Hardware is Tunnel
Internet address is 192.168.1.1/30
MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 100.1.1.1 (FastEthernet1/0), destination
200.1.1.1
Tunnel Subblocks:
src-track:
Tunnel0 source tracking subblock associated with
FastEthernet1/0
Set of tunnels with source FastEthernet1/0, 1 member
(includes iterators), on interface
<OK>
Tunnel protocol/transport GRE/IP
Key disabled, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
Tunnel transport MTU 1476 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
```

Refer to the exhibit. Which GRE tunnel configuration command is missing on R2?

- A. tunnel source 200.1.1.1
- B. tunnel source 172.16.1.0
- C. tunnel source 192.168.1.2
- D. tunnel destination 200.1.1.1

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

From the configuration in R1 and R2, the tunnel is formed using the interfaces connecting to the public Internet. For R2, the tunnel interface is missing the "tunnel source" which should be configured with either "Fa1/0" or "200.1.1.1".

**QUESTION 792**

```
list = [1,2,3,4]
list[3] = 10
print(list)
```

What is the value of the variable list after the code is run?

- A. [1, 2, 10]
- B. [1, 2, 3, 10]
- C. [1, 2, 10, 4]
- D. [1, 10, 10, 10]

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

In Python, the element in a list can be referenced by an index number starting from 0.

Hence in the list "list":

- element with index "0" is 1
- element with index "1" is 2
- element with index "2" is 3
- element with index "3" is 4

By changing the element with index "3" to the value 10, the output will be therefore [1, 2, 3, 10].

**QUESTION 793**

```
def main():
    print("The answer is " + str(magic(5)))

def magic(num):
    try:
        answer = num + 2 * 10
    except:
        answer = 100
    return answer

main()
```

What is displayed when the code is run?

- A. The answer is 25
- B. The answer is 5
- C. The answer is 70
- D. The answer is 100

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

When main() function is called, the words "The answer is " is printed with a String converted from the result from calling the function magic() with value 5. When calling the function magic() with value 5. 5 is assigned to the parameter "num". Then since "\*" i.e. multiple should be evaluated before "+" i.e. add. The answer will have the value  $5 + 20 = 25$ .

Since no error occurs in the calculation, the line under "except" is not executed. The value 25 stored in answer will be returned to the main() function and converted into the string "25" for printing.

#### QUESTION 794

Drag and drop the characteristics from the left onto the deployment models on the right. Not all options are used.  
Which are the characteristics of Cloud? (Choose two)

- A. longer deployment cycle
- B. shared ownership and accessibility
- C. complete control and accessibility
- D. requires purpose built applications
- E. quick and scalable deployment

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 795

Drag and drop the characteristics from the left onto the deployment models on the right. Not all options are used.  
Which are the characteristics of On-Prem? (Choose two)

- A. longer deployment cycle
- B. shared ownership and accessibility
- C. complete control and accessibility
- D. requires purpose built applications
- E. quick and scalable deployment

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 796

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

- A. Router(config)#ip sla 1  
Router(config)#udp-jitter 192.0.2.115 65051
- B. Router(config)#ip sla 1  
Router(config)#udp jitter 239.1.1.1 65051 end-point list List source-ip 192.168.1.1
- C. Router(config)#ip sla 1  
Router(config)#udp-jitter 192.0.2.115 65051 num-packets 20
- D. Router(config)#ip sla 1  
Router(config)#udp jitter 10.0.0.1 source-ip 192.168.1.1

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

```
R1(config-ip-sla)#udp-jitter ?
  Hostname or A.B.C.D Destination IP address or hostname

R1(config-ip-sla)#udp-jitter 192.0.2.115 ?
<1-65535> Port Number. Recommended ports greater than 1023. For codec
options recommended port range is an Even Port range between
16384-32767 or 49152-65535

R1(config-ip-sla)#udp-jitter 192.0.2.115 65051 ?
  codec      codec type to be configured
  control    Enable or disable control packets
  interval   Inter Packet Interval
  num-packets Number of Packets to be transmitted
  source-ip  Source address
  source-port Source Port
<cr>
```

Since "num-packets" is optional, the shorter one (i.e. without "num-packets") is selected as the suggested answer.

Note that you can also use a multicast address "239.1.1.1" in the configuration but you will only be allowed to configure "endpoint-list" as follows:

```
R1(config-ip-sla)#udp-jitter 239.1.1.1 65051 ?
  endpoint-list Endpoint list configuration
```

However, the one in the choices has two list names "list" and "List" specified which makes it invalid.

```
udp-jitter 239.1.1.1 65051 endpoint-list list List source-ip 192.168.1.1
R1(config-ip-sla)#$239.1.1.1 65051 endpoint-list list List source-ip 192.168.1.$
  udp-jitter 239.1.1.1 65051 endpoint-list list List source-ip 192.168.1.1
   ^
% Invalid input detected at '^' marker.
```

```
R1(config-ip-sla)#

```

#### QUESTION 79

Drag and drop the characteristics from the left onto the routing protocol they describe on the right.  
Which are the characteristics of EIGRP? (Choose three)

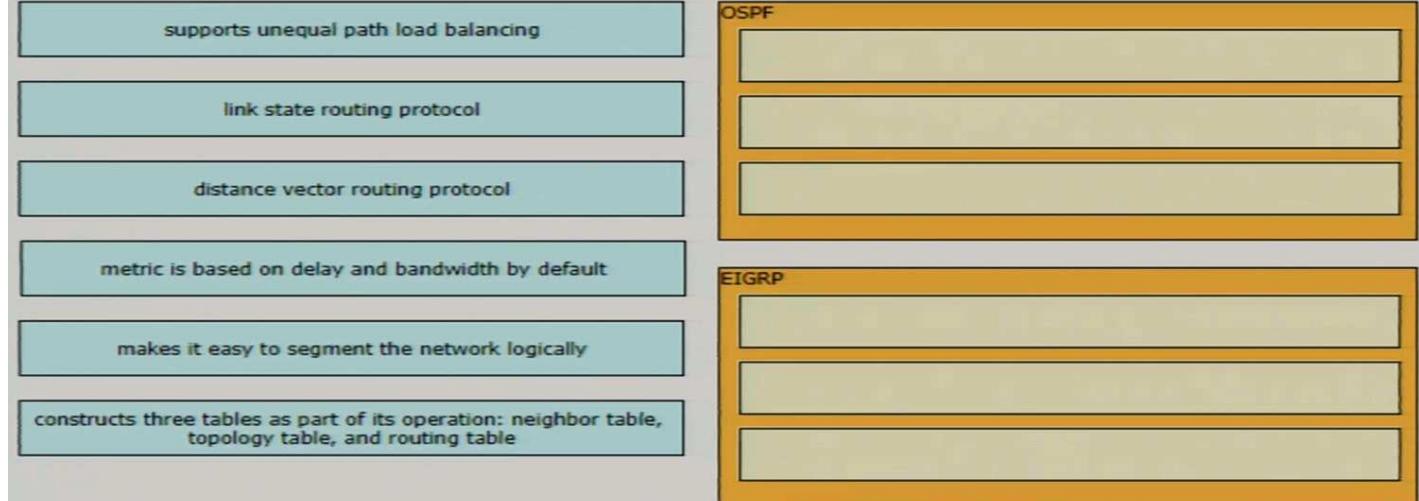
- A. supports unequal path load balancing
- B. link state routing protocol
- C. distance vector routing protocol
- D. metric is based on delay and bandwidth by default
- E. makes it easy to segment the network logically
- F. constructs three tables as part of its operation: neighbor table, topology table,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

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 798

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

Which are the characteristics of OSPF? (Choose three)

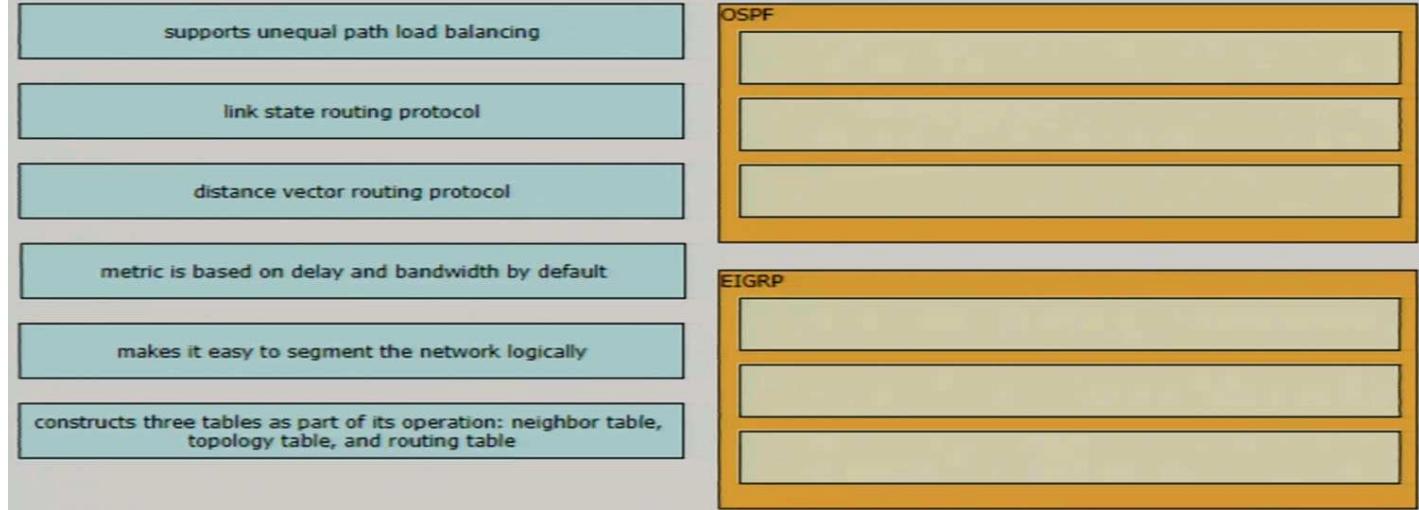
- A. supports unequal path load balancing
- B. link state routing protocol
- C. distance vector routing protocol
- D. metric is based on delay and bandwidth by default
- E. makes it easy to segment the network logically
- F. constructs three tables as part of its operation: neighbor table, topology table,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

**Correct Answer:** BEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**



Although the term "topology table" is often used in EIGRP, it can be used in OSPF:

## OSPF Router Tables / Databases

- OSPF maintains three databases which are used to create three tables.

Database	Table	Description
Adjacency Database	Neighbor Table	<ul style="list-style-type: none"><li>• List of all neighbors routers to which a router has established bidirectional communication.</li><li>• This table is unique for each router.</li><li>• Can be viewed using the show ip ospf neighbor command.</li></ul>
Link-state Database	Topology Table	<ul style="list-style-type: none"><li>• List of information about all other routers in the network.</li><li>• The database shows the network topology.</li><li>• All routers within an area have identical link-state databases.</li><li>• Can be viewed using the show ip ospf database command.</li></ul>
Forwarding Database	Routing Table	<ul style="list-style-type: none"><li>• List of routes generated when an algorithm is run on the link-state database.</li><li>• Each router's routing table is unique and contains information on how and where to send packets to other routers.</li><li>• Can be viewed using the show ip route command.</li></ul>

Chapter 3

©2007 - 2010 Cisco Systems, Inc. All rights reserved.

CCNA Study Guide

9

Therefore both EIGRP and OSPF maintains those three tables. However, since all slots in EIGRP has been used, the entry "constructs three tables as part of its operation: neighbor table, topology table, and routing table" are therefore entered under OSPF.

### QUESTION 799

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

Which are the descriptions of OSPF? (Choose two.)

- A. supports unequal cost path load balancing
- B. link state
- C. advanced distance vector
- D. supports only equal cost path load balancing

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 800**

Drag and drop the descriptions from the left onto the routing protocol they describe on the right.  
Which are the descriptions of EIGRP? (Choose two.)

- A. supports unequal cost path load balancing
- B. link state
- C. advanced distance vector
- D. supports only equal cost path load balancing

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 801**

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

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

**Correct Answer:** A

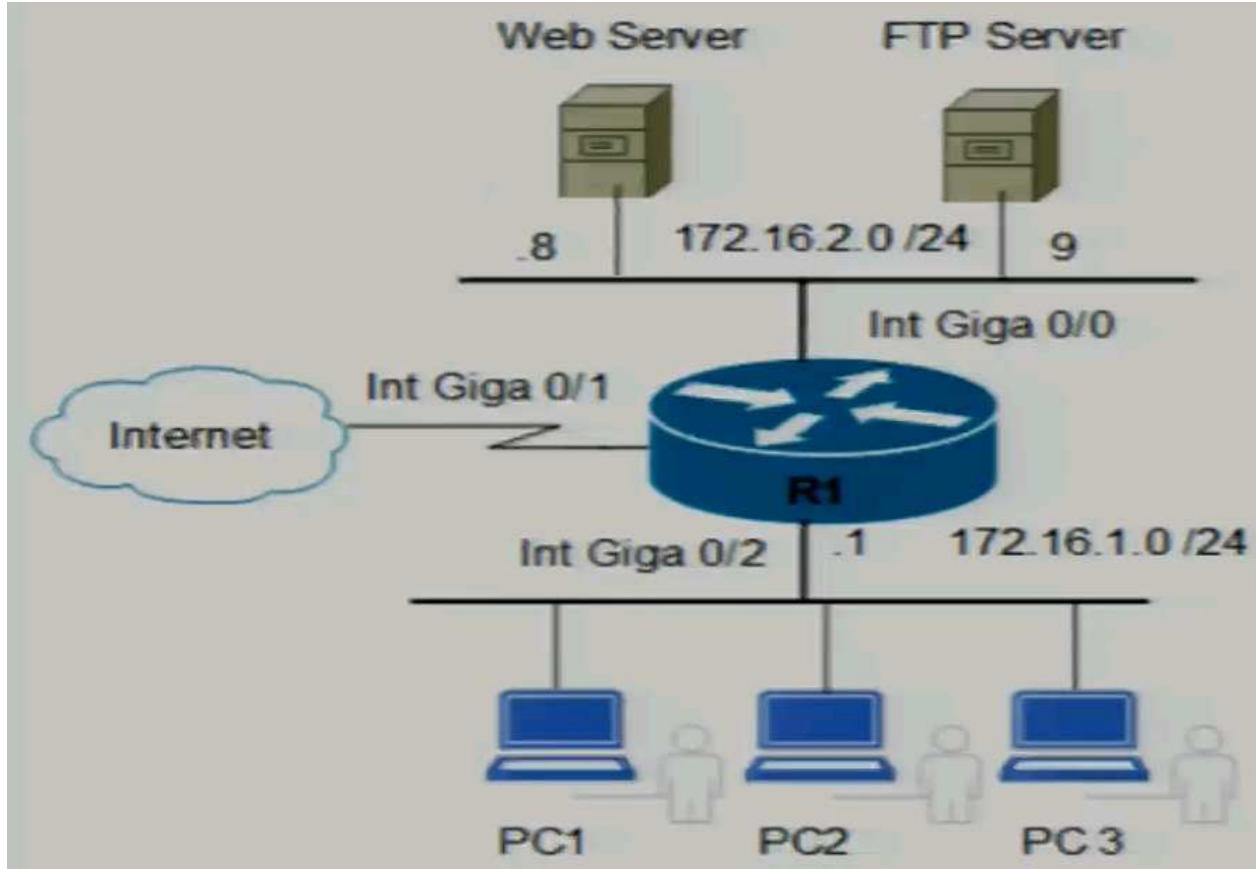
**Section:** (none)

**Explanation**

**Explanation/Reference:**

For CEF, a line card with special processor can use CEF to forward packets without going through the main processor.

**QUESTION 802**



An engineer must allow the FTP traffic from users on 172.16.1.0 /24 to 172.16.2.0 /24 and block all other traffic. Which configuration must be applied?

- A. R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255  
R1(config)# access-list 120 permit udp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255  
R1(config)# interface giga 0/2  
R1(config-if)# ip access-group 120 out
- B. R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 20  
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 21  
R1(config)# interface giga 0/2  
R1(config-if)# ip access-group 120 in
- C. R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255  
R1(config)# interface giga 0/2  
R1(config-if)# ip access-group 120 in
- D. R1(config)# access-list 120 deny any any  
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 21  
R1(config)# interface giga 0/0  
R1(config-if)# ip access-group 120 out

**Correct Answer:** B

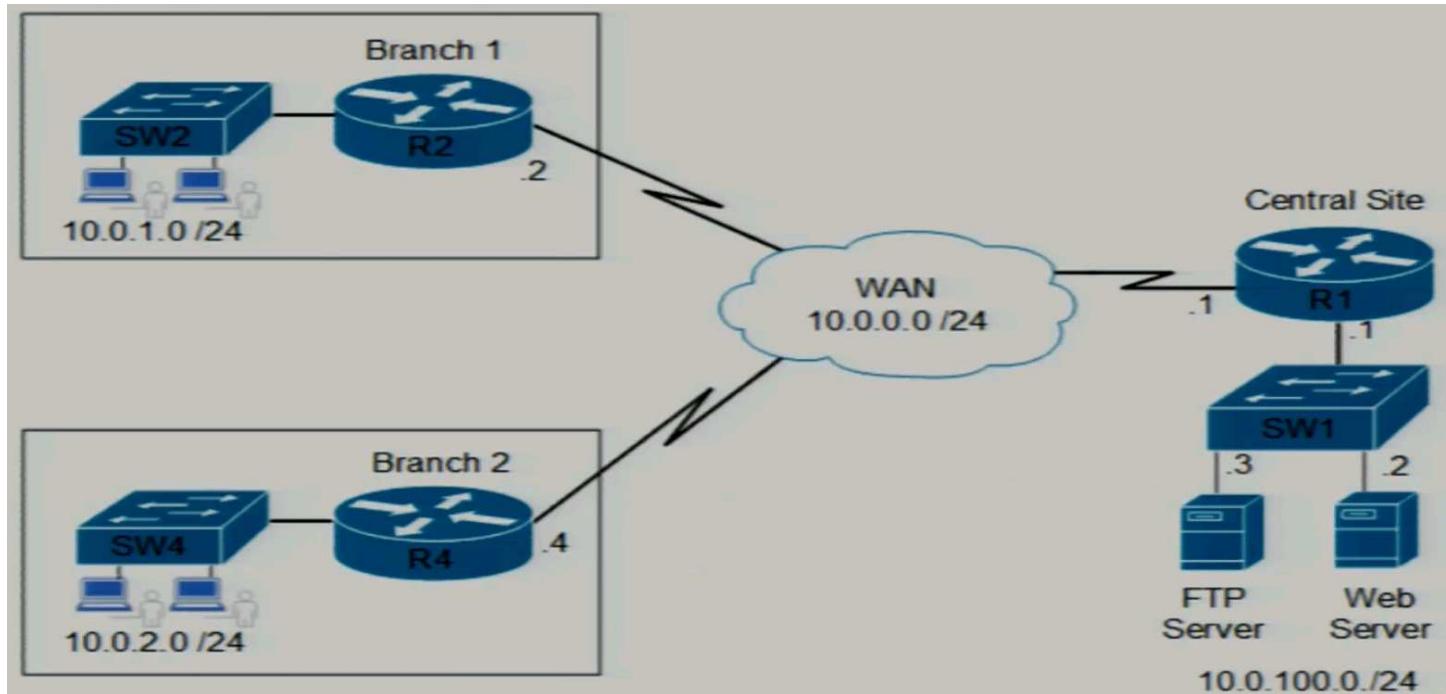
**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since the FTP server is in 172.16.2.0/24, traffic for TCP port 20 and 21 to that network should be allowed. When configuring the IP address 172.16.2.0/24 and port numbers 20 / 21 as destination in an ACL, the ACL can be applied to inbound direction of g0/2 or outbound direction of g0/0.

**QUESTION 803**



A network engineer must monitor the response time from the branch offices to the central site. Which command set configures and activates the IPSLA feature in the R4 router?

- A. ip sla 35  
  icmp-echo 10.0.100.3 source-ip 10.0.0.4  
  frequency 300  
  ip sla schedule 35 life forever start-time now
- B. ip sla 35  
  icmp-echo 10.0.0.4 source-ip 10.0.100.3  
  request-data-size 64  
  ip sla schedule 35 life forever start-time now
- C. ip sla 35  
  icmp-echo 10.0.0.4 source-ip 10.0.100.3  
  history buckets-kept 300  
  ip sla schedule 35 life forever start-time now
- D. ip sla 35  
  icmp-echo 10.0.0.1 source-ip 10.0.100.1  
  timeout 300  
  ip sla schedule 35 life forever start-time now

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

When using IP SLA to monitor traffic in R4 from Branch 4 to the central site, the target should be an IP address in central site and the source should be an IP address of R4.

**QUESTION 804**

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

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

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

**Correct Answer:** B

**Section:** (none)

## Explanation

### Explanation/Reference:

For either SPAN or RSPAN, you can use multiple source interfaces or multiple VLANs as source. However, you can't mix interfaces and VLANs. Since monitor session 1 has already been configured with interfaces as sources, you cannot add a VLAN as source to this session.

```
Switch(config)#monitor session 1 source vlan 10
% Cannot add VLANs as sources for SPAN session 1
Switch(config)#+
```

## QUESTION 805

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

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

**Correct Answer:** C

**Section:** Selected

**Explanation**

### Explanation/Reference:

Although both Basic Auth and OAuth 2.0 can be used to restrict access to HTTP services, only OAuth 2.0 is an authorization framework.

## QUESTION 806

Which action limits the total amount of memory and CPU that is used by a collection of VMs?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

### Explanation/Reference:

A resource pool is a logical abstraction for the virtual machines that can be used to manage resources.

## QUESTION 807

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

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

**Correct Answer:** B

**Section:** Selected

**Explanation**

### Explanation/Reference:

The AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN tagging, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on the returned RADIUS attributes from the AAA server.

## QUESTION 808

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

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

### Explanation/Reference:

## QUESTION 809

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

- A. Microsoft Word macro attack
- B. DDoS

- C. email phishing
- D. SQL injection
- E. ransomware

**Correct Answer:** AE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 810

Which technology enables a redundant supervisor engine to take over when the primary supervisor engine fails?

- A. graceful restart
- B. SSO
- C. NSF
- D. FHRP

**Correct Answer:** B

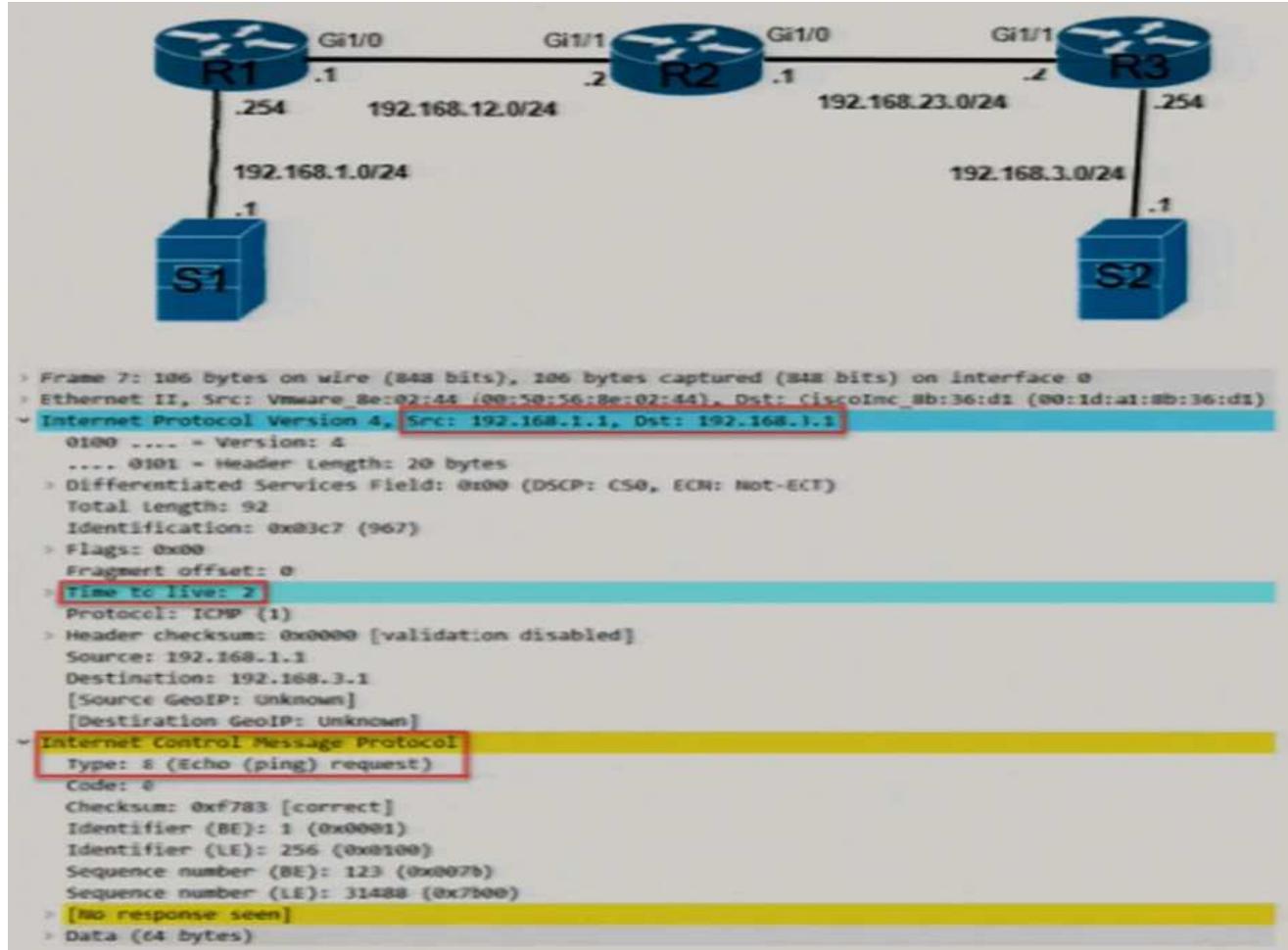
**Section:** (none)

**Explanation**

**Explanation/Reference:**

SSO establishes one of the supervisor engines as active while the other supervisor engine is designated as standby, and then SSO synchronizes information between them. A switchover from the active to the redundant supervisor engine occurs when the active supervisor engine fails, or is removed from the switch, or is manually shut down for maintenance. This type of switchover ensures that Layer 2 traffic is not interrupted. Cisco NSF always runs with SSO and provides redundancy for Layer 3 traffic. NSF works with SSO to minimize the amount of time that a network is unavailable to its users following a switchover. The main purpose of NSF is to continue forwarding IP packets following a supervisor engine switchover. Hence the primary feature for switchover is provided by SSO.

#### QUESTION 811



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

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

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since S1 issues an ICMP echo request packet with TTL of value 2:

- The packet reaches R1 and R1 subtracts 1 from the TTL. R1 then forwards the packet with TTL of value 1 to R2.
- The packet reaches R2 and R2 subtracts 1 from the TTL. Since the TTL becomes 0, the TTL expires.
- R2 sends back a TTL exceeded message.

**QUESTION 812**

```
enable secret cisco
```

```
aaa new-model
```

```
tacacs server ise-1
address 10.1.1.1
key cisco123!
```

```
tacacs server ISE-2
address 10.2.2.1
key cisco123!
```

```
aaa group server tacacs+ ISE-Servers
server name ise-1
server name ise-2
```

A network engineer must configure the router to use the ISE-Servers group for authentication. If both ISE servers are unavailable, the local username database must be used. If no usernames are defined in the configuration, then the enable password must be the last resort to log in. Which configuration must be applied to achieve this result?

- A. aaa authentication login error-enable  
aaa authentication login default group enable local ISE-Servers
- B. aaa authentication login default group enable local ISE-Servers
- C. aaa authentication login default group ISE-Servers local enable
- D. aaa authorization exec default group ISE-Servers local enable

**Correct Answer: C****Section: (none)****Explanation****Explanation/Reference:****QUESTION 813**

```
Delete + https://192.168.42.105/restconf/data/ietf-interfaces:interfaces/interface=Loopback100
```

Send ▾

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

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

**Correct Answer: B****Section: (none)****Explanation****Explanation/Reference:**

The response code "204 No Content" means that the server successfully processed request; no content is being returned. This is normal since some operations do not return any data after successful completion.

**QUESTION 814**

A network engineer is designing a QoS policy for voice and video applications. Which software queuing feature provides strict-priority servicing?

- A. Link Fragmentation
- B. Automatic QoS
- C. Low Latency Queuing
- D. Class-Based Weighted Fair Queuing

**Correct Answer: C****Section: (none)****Explanation****Explanation/Reference:****QUESTION 815**

```
from pythonping import ping
import paramiko
import sys

s= "%s %s" % (sys.argv[1], '')
s1=s.replace(' ', '')
ip= s1
t= "%s %s" % (sys.argv[2], '')
r= ping(s1, count=7)
r1= r.success()
if r1 != True:
    exit()
client= paramiko.SSHClient()
client.load_system_host_keys()
client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
client.connect(ip, port= 22, username= usr, password= pswd)
stdin, stdout, stderr = client.exec_command(t + '\n')
time.sleep(3)
print(t)
for u in stdout:
    print(u)
client.close()
```

Which action results from executing the Python script?

- A. SSH to the IP address that is manually entered on that device
- B. display the unformatted output of a command that is entered on that device
- C. display the output of a command that is entered on that device in a single line
- D. display the output of a command that is entered on that device

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

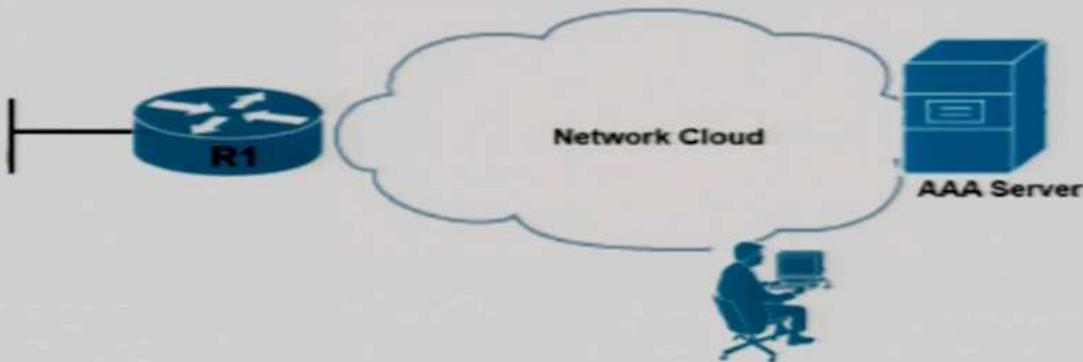
The script accepts manually entered two arguments: The 1st one is the IP address of the target and the 2nd one is a command for running in the target.

Detailed operations are:

- Ping the IP address.
- If ping is successful, make an SSH connection to the same IP address.
- Run the specified command in the SSH connection.
- Wait 3 seconds and then print the command.
- Then print all lines in the output obtained from the command as is.

Actually all choices can be correct. However, display unformatted output seems to be the best answer.

**QUESTION 816**



```

Router1$ ssh -s admin@192.168.20.3 -p 830 netconf
admin@192.168.20.3's password: cisco123

<?xml version="1.0" encoding="UTF-8"?>
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<capabilities>
<capability>urn:ietf:params:netconf:base:1.0</capability>
<capability>urn:ietf:params:netconf:base:1.1</capability>
<capability>urn:ietf:params:netconf:capability:writable-
running:1.0</capability>
<capability>urn:ietf:params:netconf:capability>xpath:1.0</capability>
<capability>urn:ietf:params:netconf:capability:validate:1.0</capability>
<capability>urn:ietf:params:netconf:capability:validate:1.1</capability>
<capability>urn:ietf:params:netconf:capability:rollback-on-
error:1.0</capability>
--snip--
</capabilities>
<session-id>2870</session-id></ hello>]]>]]>

Use < ^C > to exit

```

An engineer tries to log in to router R1. Which configuration enables a successful login?

- A. R1# aaa new-model  
aaa authorization exec default local  
enable aaa admin privilege 15
- B. R1#netconf-yang  
username admin privilege 15 secret cisco123  
aaa new-model  
aaa authorization exec default local
- C. R1#username admin privilege 15  
aaa authorization exec default local
- D. R1# username admin privilege 15  
aaa authorization exec default local  
netconf-yang

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Basic Configuration of a Catalyst 3850 Running Cisco-XE 16.3.3 Software to Support NETCONF/YANG Data Modeling  
netconf-yang  
username ciscol privilege 15 password 0 ciscol

If it is desired to enable AAA (authentication, authorization, and accounting). The following configuration can be used.  
netconf-yang  
username ciscol privilege 15 password 0 ciscol  
aaa new-model  
aaa authorization exec default local

**QUESTION 817**

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

- A. deep packet inspection
- B. virtual private network
- C. stateful inspection
- D. packet filtering
- E. application awareness

**Correct Answer:** AE

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 818**

What is the purpose of the weight attribute in an EID-to-RLOC mapping?

- A. It determines the administrative distance of LISP generated routes in the RIB.
- B. It indicates the preference for using LISP over native IP connectivity.
- C. It identifies the preferred RLOC address family.
- D. It indicates the load-balancing ratio between ETRs of the same priority.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The weight (value from 0 and 100) assigned to the locator. Used in order to determine how to load-share traffic between multiple locators when the priorities assigned to multiple locators are the same. The value represents the percentage of traffic to be load-shared.

**QUESTION 819**

What is a benefit of YANG modules?

- A. tightly coupled models with encoding to improve performance
- B. easier multivendor interoperability provided by common or industry models
- C. avoidance of ecosystem fragmentation by having fixed modules that cannot be changed
- D. single protocol and model coupling to simplify maintenance and support

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 820**

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. FlexConnect
- B. fabric
- C. local
- D. bridge

**Correct Answer:** C

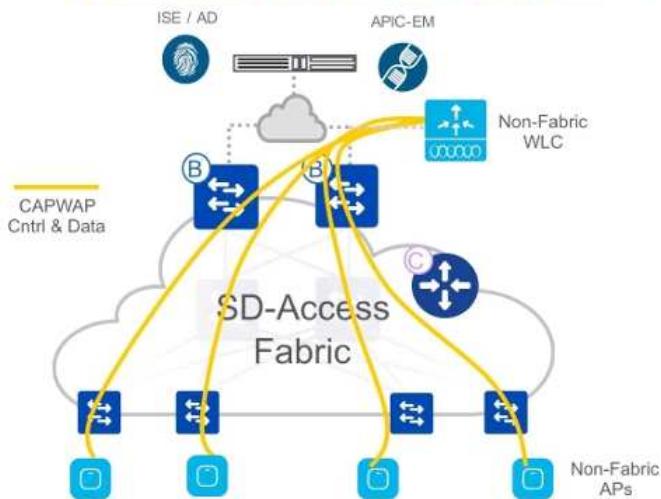
**Section:** Selected

**Explanation**

**Explanation/Reference:**

Wireless OTT is the traditional wireless carried on top of the SD-Access fabric. This mode is important as a migration step for customers who decide to implement SD-Access first on the wired network and then plan the wireless integration.

### CUWN wireless Over The Top (OTT)



Another reason that Wireless OTT is also required when there are many old APs that do not support SDAcces.

Since there is no change in the configuration and operation of APs, they are running in local mode for connecting to the WLC as before.

**QUESTION 821**

```

CPE# debug ip nat

"Jun 28 19:14:41.463: NAT: Entry assigned id 11
"Jun 28 19:14:41.463: NAT*: s=10.0.1.1->198.51.100.5, d=203.0.113.8 [59922]NAT: dyn flow info
download suppressed for flow 11
"Jun 28 19:14:41.463: NAT*: s=203.0.113.8, d=198.51.100.5->10.0.1.1 [53790]NAT: dyn flow info
download suppressed for flow 11
[...]
"Jun 28 19:14:46.147: NAT: Entry assigned id 13
"Jun 28 19:14:46.147: NAT*: s=10.0.2.1->198.51.100.6, d=203.0.113.8 [60095]NAT: dyn flow info
download suppressed for flow 13
"Jun 28 19:14:46.148: NAT*: s=203.0.113.8, d=198.51.100.6->10.0.2.1 [32109]NAT: dyn flow info
download suppressed for flow 13
[...]
"Jun 28 19:14:50.462: %IPNAT-4-ADDR_ALLOC_FAILURE: Address allocation failed for 10.0.3.1,
pool NAT might be exhausted
"Jun 28 19:14:50.462: NAT: translation failed (A), dropping packet s=10.0.3.1 d=203.0.113.8

CPE# show ip nat translation
Pro Inside global   Inside local   Outside local   Outside global
tcp 198.51.100.5:61082 10.0.1.1:61082 203.0.113.8:23  203.0.113.8:23
— 198.51.100.5      10.0.1.1      —                —
tcp 198.51.100.6:15350 10.0.2.1:15350 203.0.113.8:23  203.0.113.8:23
— 198.51.100.6      10.0.2.1      —                —

CPE# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic, 2 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Ethernet0/1
Hits: 234 Misses: 0
CEF Translated packets: 234, CEF Punted packets: 7
Expired translations: 2
Dynamic mappings:
  — Inside Source
    [Id: 1] access-list NAT pool NAT refcount 4
    pool NAT: id 1, netmask 255.255.255.0
      start 198.51.100.5 end 198.51.100.6
      type generic, total addresses 2, allocated 2 (100%), misses 7
nat-limit statistics:
  max entry: max allowed 0, used 0, missed 0
Outside global interfaces count: 1

```

Refer to the exhibit. An administrator troubleshoots Intermittent connectivity from internal hosts to an external public server. Some internal hosts can connect to the server while others receive an ICMP Host Unreachable message, and these hosts change over time. What is the cause of this issue?

- A. The NAT pool netmask is excessively wide.
- B. The NAT ACL and NAT pool share the same name.
- C. The translation does not use address overloading.
- D. The NAT ACL does not match all internal hosts.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In the debug messages, the last two lines shows that pool NAT might be exhausted.

In the output of "sh ip nat statistics", the pool NAT has a start address "192.168.51.100.5" and an end address "192.168.51.100.6". In the output of "sh ip nat translation", these two IP addresses have already been used by two different hosts.

Hence, the probable cause is that "overload" is not included in the NAT configuration.

**QUESTION 822**

Drag and drop the characteristics from the left onto the deployment models on the right.

Which is the characteristic of Cloud?

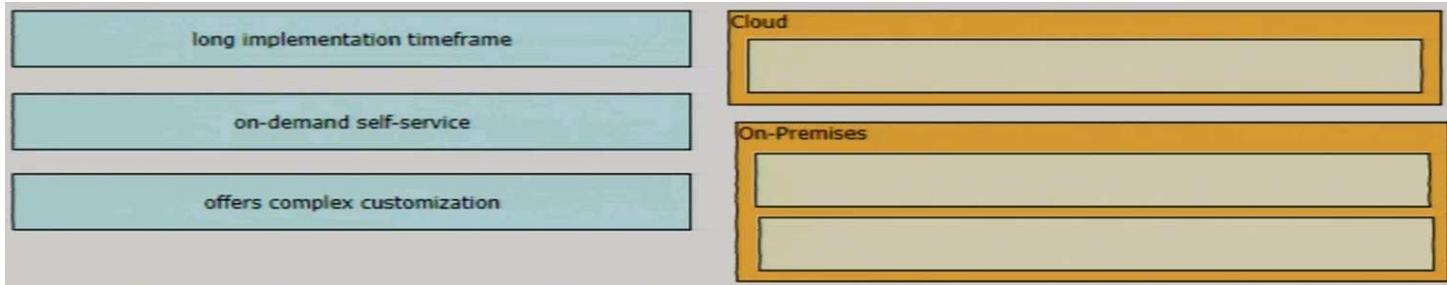
- A. long implementation timeframe
- B. on-demand self-service
- C. offers complex customization

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 823**

Drag and drop the characteristics from the left onto the deployment models on the right.  
Which are the characteristic of On-Premises? (Choose two.)

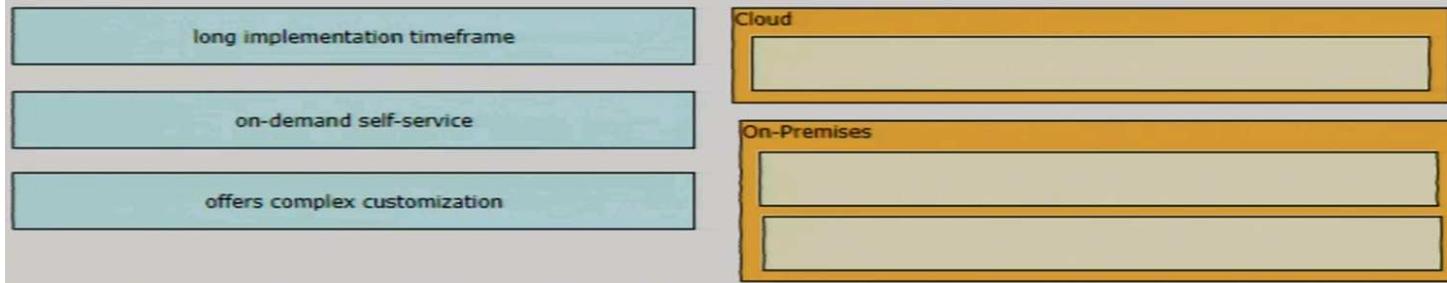
- A. long implementation timeframe
- B. on-demand self-service
- C. offers complex customization

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 824**

```
ip sla 100
  udp-echo 10.10.10.15 6336
    frequency 30
```

Refer to the exhibit. An engineer has configured an IP SLA for UDP echos. Which command is needed to start the IP SLA to test every 30 seconds and continue until stopped?

- A. ip sla schedule 100 life forever
- B. ip sla schedule 100 start-time now life forever
- C. ip sla schedule 100 start-time now life 30
- D. ip sla schedule 30 start-time now life forever

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Note that testing every 30 second is defined in the SLA with "frequency". Hence "ip sla schedule" only needs to specify the SLA number, the start-time and its lifetime.

**QUESTION 825**

In a Cisco SD-WAN deployment, which action is the vSmart controller responsible for?

- A. distribute policies that govern data forwarding performed within the Cisco SD-WAN fabric
- B. handle, maintain, and gather configuration and status for nodes within the Cisco SD-WAN fabric
- C. gather telemetry data from WAN Edge routers
- D. onboard WAN Edge nodes into the Cisco SD-WAN fabric

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 826**

Which two methods are used to interconnect two Cisco SD-Access Fabric sites? (Choose two.)

- A. fabric Interconnect
- B. SD-Access transit
- C. SAN transit
- D. IP-based transit
- E. wireless transit

**Correct Answer:** BD

**Section: (none)****Explanation****Explanation/Reference:**

A fabric domain can consist of one or more fabric sites and transit site. Multiple fabric sites are connected to each other using a transit site. There are two types of transit sites:

SD-Access transit: Enables a native SD-Access (LISP, VXLAN, CTS) fabric, with a domain-wide control plane node for intersite communication.

IP-based transit: Leverages a traditional IP-based (VRF-LITE, MPLS) network, which requires remapping of VRFs and SGTs between sites.

**QUESTION 827**

A company recently decided to use RESTCONF instead of NETCONF, and many of their NETCONF scripts contain the operation <edit-config> (operation="create"). Which RESTCONF operation must be used to replace these statements?

- A. GET
- B. PUT
- C. POST
- D. CREATE

**Correct Answer: C**

**Section: Selected****Explanation****Explanation/Reference:**

The following table shows the Protocol operations that the Cisco NX-OS RESTCONF Agent supports:

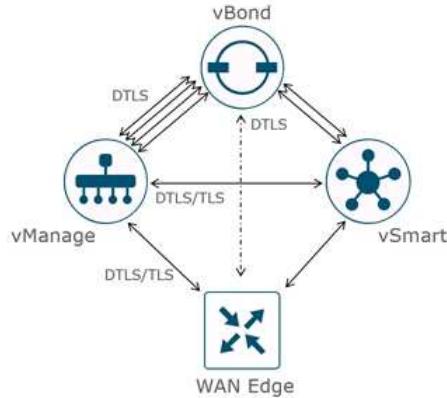
RESTCONF	NETCONF Equivalent
OPTIONS	NETCONF: none
HEAD	NETCONF: none
GET	NETCONF: <get-config>, <get>
POST	NETCONF: <edit-config> (operation="create")
PUT	NETCONF: <edit-config> (operation="create/replace")
PATCH	NETCONF: <edit-config> (operation="merge")
DELETE	NETCONF: <edit-config> (operation="delete")

**QUESTION 828**

What is a characteristic of Cisco SD-WAN?

- A. uses control plane connections between routers
- B. requires manual secure tunnel configuration
- C. operates over DTLS/TLS authenticated and secured tunnels
- D. uses unique per-device feature templates

**Correct Answer: C**

**Section: (none)****Explanation****Explanation/Reference:****QUESTION 829**

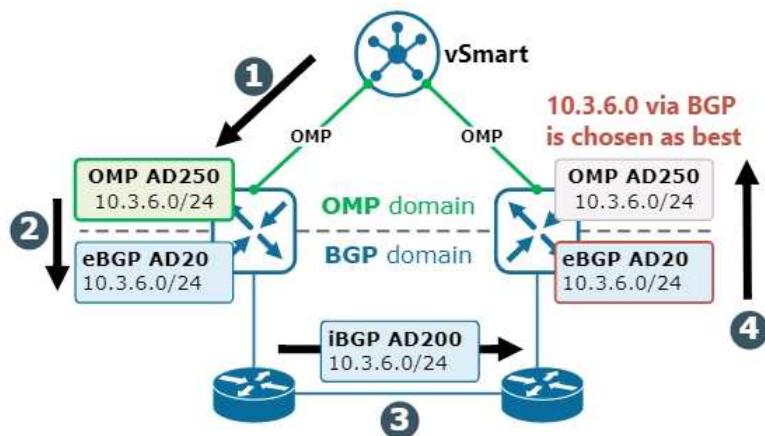
Which function is performed by vSmart in the Cisco SD-WAN architecture?

- A. execution of localized policies
- B. redistribution between OMP and other routing protocols
- C. aggregation and distribution of VPN routing information
- D. facilitation of NAT detection and traversal

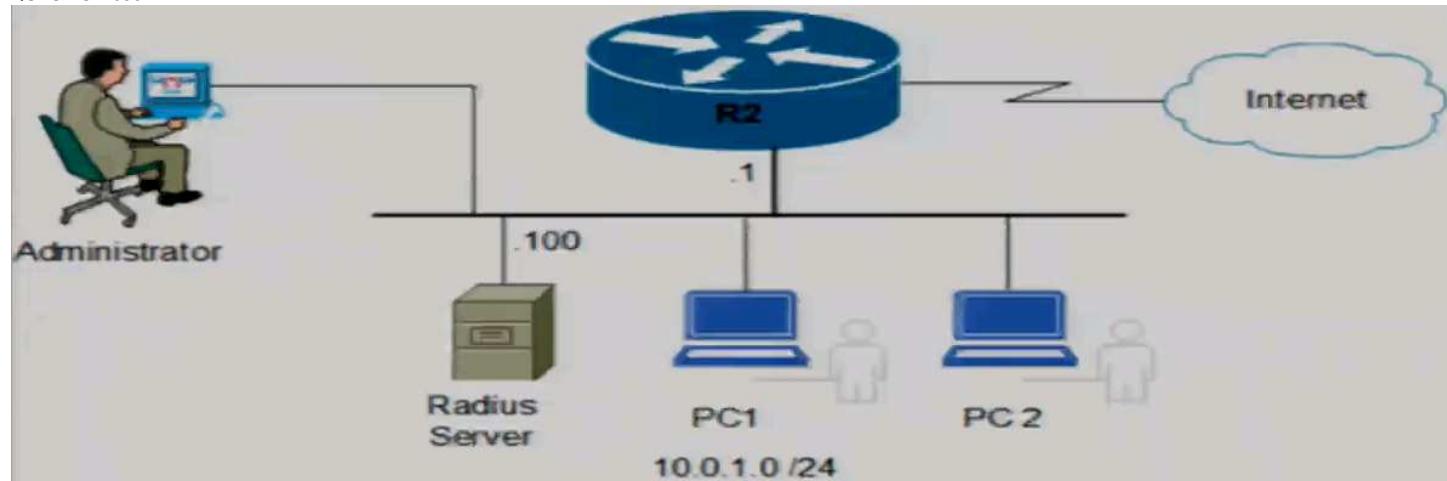
**Correct Answer: C**

**Section: (none)****Explanation****Explanation/Reference:**

Centralized policy is provisioned on the centralized Cisco vSmart Controllers in the overlay network. The localized policy is provisioned on Cisco vEdge devices. vSmart only communicate OMP with vEdge devices. Redistribution between OMP and other routing protocols (e.g. BGP) is performed in vEdge devices.



QUESTION 830



Refer to the exhibit. An engineer must save the configuration of router R2 using the NETCONF protocol. Which script must be used?

- A. 

```
<?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>
```
- B. 

```
<?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>
```
- C. 

```
<?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>
```
- D. 

```
<?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-state">
        <ncm:capabilities/>
      </ncm:netconf-state>
    </filter>
  </get>
</rpc>
```

Correct Answer: A  
 Section: (none)  
 Explanation

**Explanation/Reference:**

The running configuration can be saved to the startup configuration on the Catalyst 3850 by sending this YANG formatted NETCONF RPC message to the Catalyst 3850 via NETCONF.

```
<?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="cisco/yang/cisco-ia">
</rpc>
```

**QUESTION 831**

Drag and drop the snippets onto the blanks within the code to construct a script that blocks a MAC address.

**Select and Place:**

```
event manager applet mac_block
event timer [ ] time 10
action 01 cli command "enable"
action 02 cli command "terminal length 0"
action 03 cli command "show mac address-table address 0050.7966.6800"
action 04 regexp " [ ] "
action 05 if $_regexp_result eq [ ] t match
action 06 cli command "configure terminal"
action 07 cli command "interface $Ports"
action 08 cli command "shutdown"
action 09 end
```

**Correct Answer:**

```
event manager applet mac_block
event timer [ watchdog ] time 10
action 01 cli command "enable"
action 02 cli command "terminal length 0"
action 03 cli command "show mac address-table address 0050.7966.6800"
action 04 regexp " [ (Gl...) ] "
action 05 if $_regexp_result eq [ 1 ] t match
action 06 cli command "configure terminal"
action 07 cli command "interface $Ports"
action 08 cli command "shutdown"
action 09 end
```

**Section: Selected****Explanation****Explanation/Reference:****Explanations:**

```
R1(config-applet)#event timer ?
absolute    Absolute timer event
countdown   Countdown timer event
cron        Cron timer event
watchdog    Watchdog timer event
```

R1(config-applet)#

The “regexp” action finds the interface name that corresponds to the specified MAC address. The interface name found will be stored. If the result of the “regexp” action shows that a match is found (i.e. the built-in variable “\$\_regexp\_result” is 1), the interface name stored will be used for shutting down the interface.

**Reference:**

Something is missing in the action 04 in the question, it should specify that it uses the last CLI command result (i.e. \$cli\_result) as input and it stores the matching result in bracket (i.e. “()”) in the variable “Ports” e.g.:

```
action 04 regexp " <blank for filling> " $cli_result match Ports
```

**QUESTION 832**

When is GLBP preferred over HSRP?

- A. When encrypted hellos are required between gateways in a single group.
- B. When the gateway routers are a mix of Cisco and non-Cisco routers.
- C. When clients need the gateway MAC address to be the same between multiple gateways.
- D. When the traffic load needs to be shared between multiple gateways using a single virtual IP.

**Correct Answer: D****Section: (none)****Explanation****Explanation/Reference:****QUESTION 833**

```

pl1 = [
    ...
<get-config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <source>
        <running/>
    </source>
    <filter>
        <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
            <ip>
                <access-list>
                    <extended xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-acl">
                        <name>flp</name>
                    </extended>
                </access-list>
            </ip>
        </native>
    </filter>
</get-config>
...
]

with manager.connect(host=c54, port=830, username=c14,
                     password=c24, timeout=90, hostkey_verify=False) as m:
    for rpc in pl1:
        r1 = m.dispatch(et.fromstring(rpc))
        d1 = xmltodict.parse(r1.xml)[['rpc-reply'][['data'][['native'][['ip']
            ['access-list'][['extended'][['access-list-seq-rule']]]]]]]

```

What is achieved by this Python script?

- A. It converts access list statements to a human-readable format.
- B. It displays access list statements on a terminal screen.
- C. It configures access list statements.
- D. It reads access list statements into a dictionary list.

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

"xmltodict" converts the XML data of the access list obtained from the host "c54" into a dictionary list.

**QUESTION 834**

What is a capability of the Cisco DNA Center southbound API?

- A. It adds support for managing non-Cisco devices from Cisco DNA Center.
- B. It sends webhooks from Cisco DNA Center when alerts are triggered.
- C. It allows administrators to make API calls to Cisco DNA Center.
- D. It connects to ITSM services such as ServiceNow.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Southbound—Multivendor Support APIs/SDK

The Cisco DNA Center Multivendor SDK allows partners to add support for managing non-Cisco devices directly from Cisco DNA Center. This tool provides the ability to build "device packs" customized for the level of automation and reporting that each new device allows. Once built, this capability permits basic device visibility, monitoring and Command Runner compatibility, and enables a non-Cisco device to be identified properly in inventory.

**QUESTION 835**

Which solution simplifies management of secure access to network resources?

- A. 802.1AE to secure communication in the network domain
- B. ISE to automate network access control leveraging RADIUS AV pairs
- C. RFC 3580-based solution to enable authenticated access leveraging RADIUS and AV pairs
- D. TrustSec to logically group internal user environments and assign policies

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 836**

What does the destination MAC on the outer MAC header identify in a VXLAN packet?

- A. the next hop
- B. the remote spine
- C. the remote switch
- D. the leaf switch

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 837**

Where is the wireless LAN controller located in a mobility express deployment?

- A. The wireless LAN controller is embedded into the access point.
- B. The wireless LAN controller exists in a server that is dedicated for this purpose.
- C. The wireless LAN controller exists in the cloud.
- D. There is no wireless LAN controller in the network.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Cisco Mobility Express is a virtual wireless LAN controller integrated on 802.11ac Wave 2 access points (Cisco Aironet ® 4800, 3800, 2800, 1850, 1830, 1815, 1560, and 1540 Series).

**QUESTION 838**

An engineer plans to use Python to convert text files that contain device information to JSON. Drag and drop the code snippets from the bottom onto the blanks in the code to construct the request. Not all options are used.

**Select and Place:**

```
import json
input_file = 'raw-data.txt'
dictionary_1 = {}
fields = ['Device_type', 'IP_Address', 'IOS_type', 'Username', 'Password']

l = 1
for line in text:
    description = list(line.strip().split(None, 4))
    print(description)
    Device_Number = 'Device' + str(l)
    i = 0
    dictionary_2 = {}
    while i < len(fields):
        dictionary_2[fields[i]] = description[i]
        i = i + 1
    dictionary_1[Device_Number] = dictionary_2
    l = l + 1

json.dump(dictionary_1, out_file, indent=4)
```

**Output of Python Code**

```
switch ios 10.1.1.1 user1 pass1
router ios-xr 10.1.1.2 user2 pass2
nexus-9k nx-os 10.1.1.3 user3 pass3
```

**raw-data.txt**

```
{
  "Device1": {
    "Device_type": "switch",
    "IOS_type": "ios",
    "IP_Address": "10.1.1.1",
    "Username": "user1",
    "Password": "pass1"
  },
  "Device2": {
    "Device_type": "router",
    "IOS_type": "ios-xr",
    "IP_Address": "10.1.1.2",
    "Username": "user2",
    "Password": "pass2"
  },
  "Device3": {
    "Device_type": "nexus-9k",
    "IOS_type": "nx-os",
    "IP_Address": "10.1.1.3",
    "Username": "user3",
    "Password": "pass3"
  }
}
```

out\_file.close()

out\_file = open ("Json-Output.json", "w")

with open(raw-data) as text:

with open(input\_file) as text:

**Correct Answer:**

```

import json
input_file = 'raw-data.txt'
dictionary_1 = {}
fields = ['Device type', 'IP Address', 'IOS type', 'Username', 'Password']
with open(input_file) as text:
    i = 1
    for line in text:
        description = list(line.strip().split(None, 4))
        print(description)
        Device_Number = 'Device' + str(i)
        i = 0
        dictionary_2 = {}
        while i < len(fields):
            dictionary_2[fields[i]] = description[i]
            i = i + 1
        dictionary_1[Device_Number] = dictionary_2
        i = i + 1
out_file = open ("Json-Output.json", "w")
json.dump(dictionary_1, out_file, indent=4)
out_file.close()

```

#### Output of Python Code

```

switch ios 10.1.1.1 user1 pass1
router ios-xr 10.1.1.2 user2 pass2
nexus-9k nx-os 10.1.1.3 user3 pass3

```

#### raw-data.txt

```

{
    "Device1": {
        "Device_type": "switch",
        "IOS_type": "ios",
        "IP_Address": "10.1.1.1",
        "Username": "user1",
        "Password": "pass1"
    },
    "Device2": {
        "Device_type": "router",
        "IOS_type": "ios-xr",
        "IP_Address": "10.1.1.2",
        "Username": "user2",
        "Password": "pass2"
    },
    "Device3": {
        "Device_type": "nexus-9k",
        "IOS_type": "nx-os",
        "IP_Address": "10.1.1.3",
        "Username": "user3",
        "Password": "pass3"
    }
}

```

with open(raw-data) as text:

Section: (none)

Explanation

Explanation/Reference:

#### QUESTION 839

Drag and drop the snippets onto the blanks within the code to construct a script that configures a loopback interface with an IP address. Not all options are used.

Select and Place:

```

"@message-id": "101",
"edit-config": {
    [
        {
            "running": null
        },
        "config": {
            "native": {
                "interface": {
                    "Loopback": [
                        [
                            [
                                "ip": {
                                    "address": [
  [
  [
  "address": "10.10.10.10",
  "mask": "255.255.255.255"
  ]
  ]
                                    ]
                                }
                            ]
                        ]
                    }
                }
            }
        }
    ]
}

```

"mask":

"fixed":

"name": "100"

"primary":

"config":

"target":

Correct Answer:

```
    "@message-id": "101",
    "edit-config": {
        "target": {
            "running": null
        },
        "config": {
            "native": {
                "interface": {
                    "Loopback": {
                        "name": "100"
                    },
                    "ip": {
                        "address": {
                            "primary": {
                                "address": "10.10.10.10",
                                "mask": "255.255.255.255"
                            }
                        }
                    }
                }
            }
        }
    }
}
```

Section: (none)

Explanation

Explanation/Reference:

#### QUESTION 840

Which statement describes the Cisco SD-Access plane functionality for fabric-enabled wireless?

- A. Control plane traffic and data plane traffic are sent to the WLC through VXLAN.
- B. The control plane traffic is sent to the WLC through CAPWAP tunnels, and the data plane traffic is sent from the AP to the fabric edge switch through VXLAN.
- C. Control plane traffic and data plane traffic are sent to the WLC through CAPWAP tunnels.
- D. The control plane traffic is sent to the WLC through VXLAN, and the data plane traffic is sent to the WLC through CAPWAP tunnels.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

#### QUESTION 841

When a branch location loses connectivity, which Cisco FlexConnect state rejects new users but allows existing users to function normally?

- A. Authentication-Local / Switch-Local
- B. Authentication-Down / Switch-Local
- C. Authentication-Down / Switching-Down
- D. Authentication-Central / Switch-Local

Correct Answer: B

Section: Selected

Explanation

Explanation/Reference:

With respect to client authentication (open, shared, EAP, web authentication, and NAC) and data packets, the WLAN can be in any one of the following states depending on the configuration and state of controller connectivity:

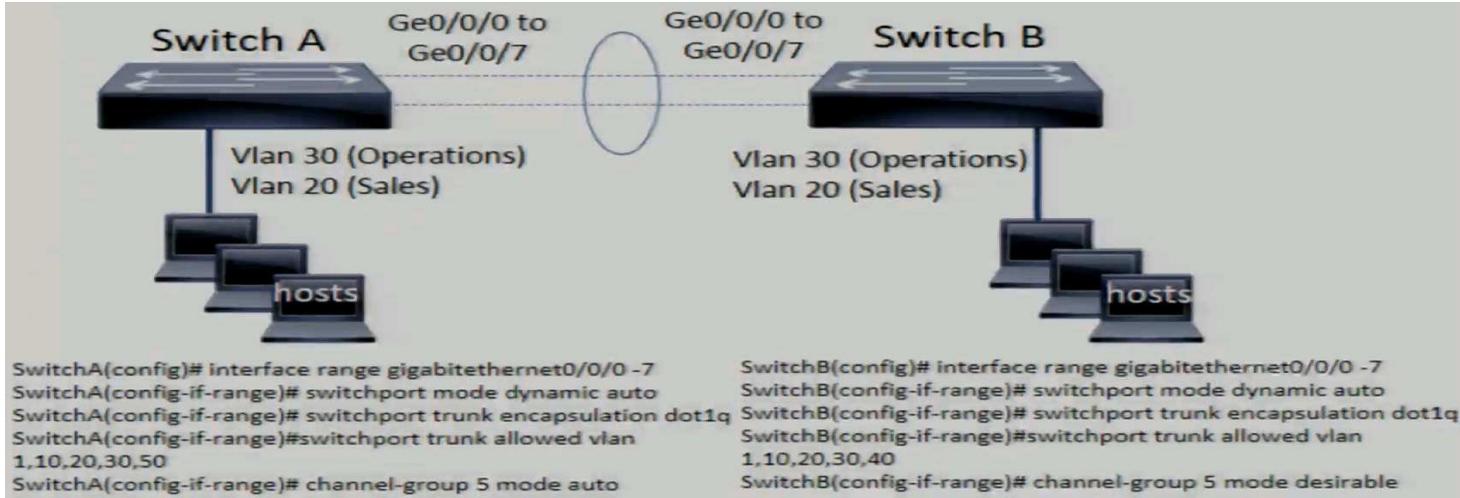
**central authentication, central switching**—In this state, the controller handles client authentication, and all client data is tunneled back to the controller. This state is valid only in connected mode.

**local authentication, local switching**—In this state, the FlexConnect access point handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode.

**authentication down, switch down**—In this state, the WLAN disassociates existing clients and stops sending beacon and probe requests. This state is valid in both standalone mode and connected mode.

**authentication down, local switching**—In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive. This state is valid only in standalone mode.

#### QUESTION 842



Users in the Operations VLAN on Switch A are unable to communicate with users in the Operations VLAN on Switch B. Which action resolves the issue?

- A. Set the EtherChannel mode to LACP on Switch A.
- B. Set the switchport mode to dynamic desirable on Switch B.
- C. Set the EtherChannel mode to PAgP on Switch B.
- D. Configure the same allowed VLAN list on Switch A and Switch B.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The two switches can negotiate to form EtherChannel using PAgP due to the "auto" and "desirable" in the settings of their "channel-group" commands. However, they cannot negotiate trunk since both are set to "dynamic auto" in the "switch-port" commands. Hence, you need to set one of the switch to "dynamic desirable" in the "switch-port" command

**QUESTION 843**

Which unit of measure is used to measure wireless RF SNR?

- A. dBi
- B. dBm
- C. mW
- D. dB

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

SNR (Signal-to-Noise Ratio) is a ratio based value that evaluates your signal based on the noise being seen. It is usually expressed in decibels (db).

**QUESTION 844**

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 greater than or equal to 999.
- D. A value not equal to 999.

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 845**

```

line vty 0 4
  exec-timeout 120 0
  login local
line vty 5 15
  exec-timeout 30 0
  login local

```

An engineer must update the existing configuration to achieve these results:

- Only administrators from the 192.168.1.0/24 subnet can access the vty lines.
- Access to the vty lines using clear-text protocols is prohibited.

Which command set should be applied?

- A. access-list 1 permit 192.168.1.0 255.255.255.0  
line vty 0 15  
access-class 1 in  
transport input telnet rlogin
- B. access-list 1 permit 192.168.1.0 0.0.0.255  
line vty 0 15  
access-class 1 in  
transport input telnet ssh
- C. access-list 1 permit 192.168.1.0 0.0.0.255  
line vty 0 15  
access-class 1 in  
transport input none
- D. access-list 1 permit 192.168.1.0 0.0.0.255  
line vty 0 15  
access-class 1 in  
transport input ssh

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 846

Drag and drop the characteristics from the left onto the corresponding switching architectures on the right.  
Which are the characteristics of RIB? (Choose three.)

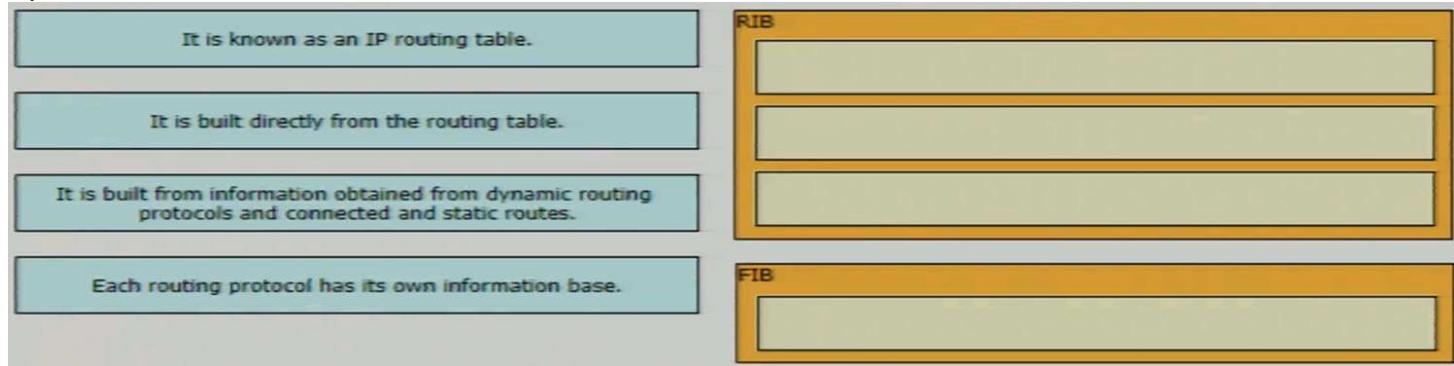
- A. It is known as an IP routing table.
- B. It is built directly from the routing table.
- C. It is built from information obtained from dynamic routing protocols and connected and static routes.
- D. Each routing protocol has its own information base.

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 847

Drag and drop the characteristics from the left onto the corresponding switching architectures on the right.  
Which are the characteristics of FIB?

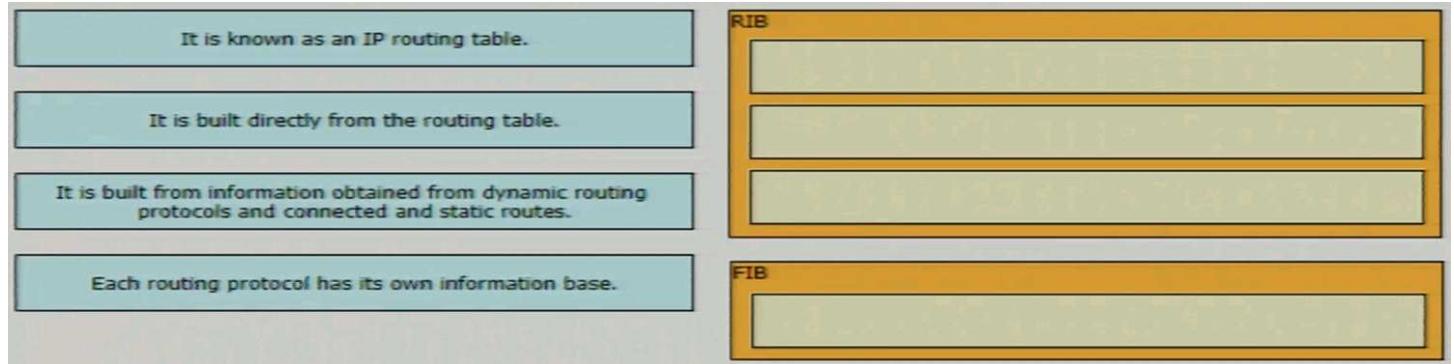
- A. It is known as an IP routing table.
- B. It is built directly from the routing table.
- C. It is built from information obtained from dynamic routing protocols and connected and static routes.
- D. Each routing protocol has its own information base.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 848

An engineer must configure a router to allow users to run specific configuration commands by validating the user against the router database. Which configuration must be applied?

- A. aaa authorization exec default local
- B. aaa authorization network default local
- C. aaa authentication network default local
- D. aaa authentication exec default local

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 849**

```
import sqlite3
a= sqlite3.connect('/home/sdwan-lab/user.sqlite3')
b= a.cursor()
c= "select user from monitor_branch where loopbackip=''" + str(ip[i]) + "'"
d= b.execute(c)
e= b.fetchall()
usr= str(e[0])
usr= usr.replace("('','")
usr= usr.replace("',')","")
```

What does this Python script do?

- A. writes the username for a specific IP address into a light database
- B. enters the RADIUS username for a specific IP address
- C. enters the TACACS+ username for a specific IP address
- D. reads the username for a specific IP address from a light database

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 850**

What do Chef and Ansible have in common?

- A. They rely on a declarative approach
- B. They use YAML as their primary configuration syntax
- C. They are clientless architectures
- D. They rely on a procedural approach

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 851**

Which two advanced security features are available in next-generation firewalls but were not provided by standard firewalls? (Choose two.)

- A. stateful traffic inspection
- B. network telemetry
- C. remote access VPN
- D. intrusion prevention
- E. application control

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 852**

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

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 853**

Which tunnel type allows clients to perform a seamless Layer 3 roam between a Cisco AireOS WLC and a Cisco IOS XE WLC?

- A. Ethernet over IP
- B. VPN
- C. Mobility
- D. IPsec

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

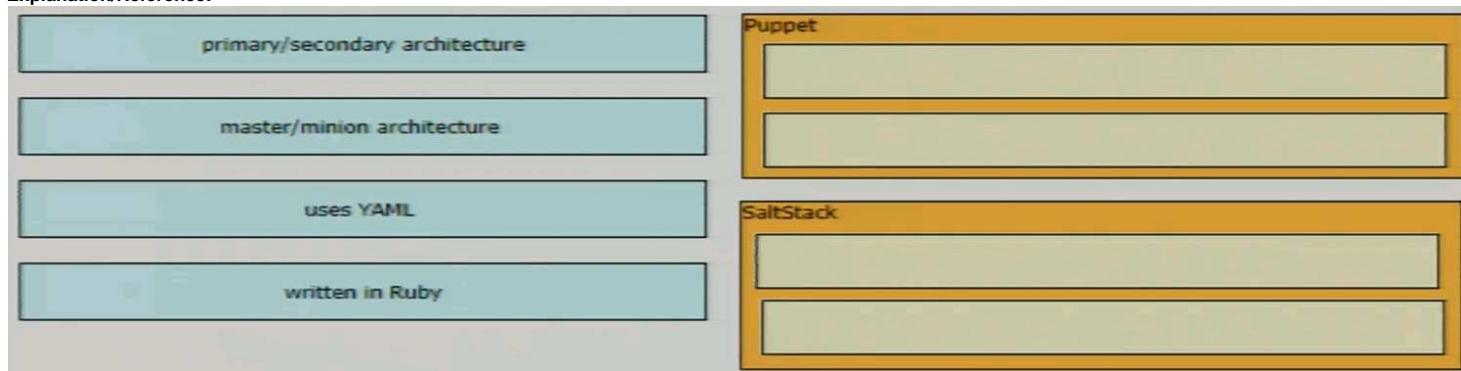
**QUESTION 854**

Drag and drop the characteristics from the left onto the corresponding configuration management tools on the right. Not all options are used. Which are the characteristics of Puppet? (Choose two.)

- A. primary/secondary architecture
- B. master/minion architecture
- C. uses YAML
- D. written in Ruby

**Correct Answer:** AD  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**



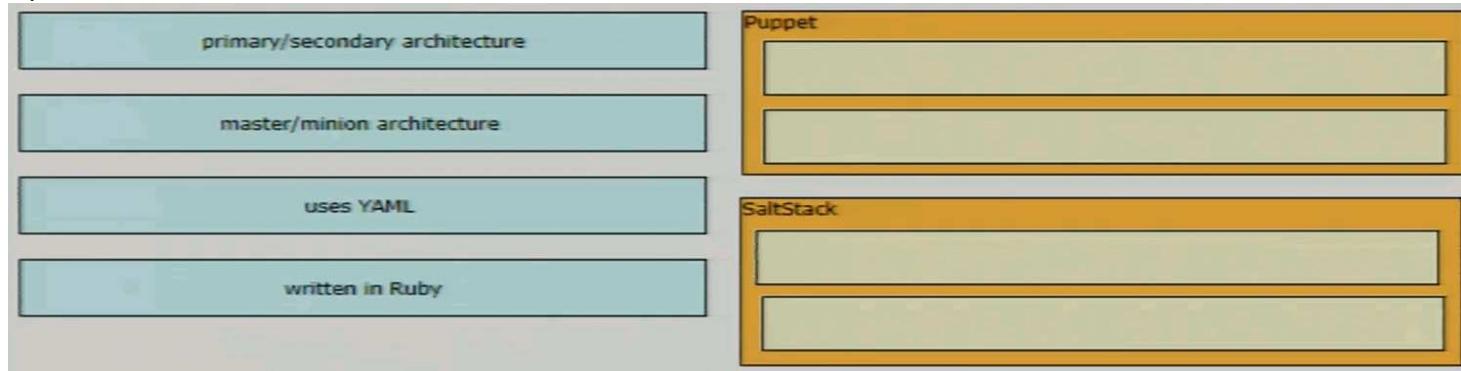
**QUESTION 855**

Drag and drop the characteristics from the left onto the corresponding configuration management tools on the right. Not all options are used. Which are the characteristics of SaltStack? (Choose two.)

- A. primary/secondary architecture
- B. master/minion architecture
- C. uses YAML
- D. written in Ruby

**Correct Answer:** BC  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**



**QUESTION 856**

How do OSPF and EIGRP compare?

- A. EIGRP shows successor and feasible successor routes, and OSPF shows all known routes.
- B. EIGRP shows all known routes, and OSPF shows successor and feasible successor routes.
- C. OSPF and EIGRP use the same administrative distance.
- D. Both OSPF and EIGRP use the concept of areas.

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 857**

```
router#debug ip packet detail 100
IP packet debugging is on (detailed) for access list 100
router#

12:11:05: IP: s=1.1.1.1 (Serial1/0), d=10.1.1.1 (Serial3/0),
g=10.1.1.1, len 100, forward
12:11:05:     ICMP type=0, code=0
12:11:05: IP: s=1.1.1.1 (Serial1/0), d=10.1.1.1 (Serial3/0),
g=10.1.1.1, len 100, forward
12:11:05:     ICMP type=0, code=0
12:11:05: IP: s=1.1.1.1 (Serial1/0), d=10.1.1.1 (Serial3/0),
g=10.1.1.1, len 100, forward
12:11:05:     ICMP type=0, code=0
```

A network engineer issues the debug command while troubleshooting a network issue. What does the output confirm?

- A. ACL100 is tracking all traffic from 10.1.1.1 destined for 1.1.1.1.
- B. ACL100 is tracking ICMP traffic from Serial1/0 destined for Serial3/0.
- C. ACL100 is tracking ICMP traffic from 10.1.1.1 destined for 1.1.1.1.
- D. ACL100 is tracking ICMP traffic from 1.1.1.1 destined for 10.1.1.1.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 858**

An engineer must construct an access list for a Cisco Catalyst 9800 Series WLC that will redirect wireless guest users to a splash page that is posted 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 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
- B. 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
- C. 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
- D. 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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 859**

Which JSON script is properly formatted?

- A. ["plants": {  
 "type": annual,  
 "color": "yellow",  
 "season": "summer"  
 }]  
]
- B. [  
 "subject": {  
 [  
 "title": "Language"

```

        "ID": "723816",
        "location": "Main Campus"
    }
]
C. "Stores": [
    {
        "type": "retail",
        "location": "B27",
        "contact": "375-121-9061"
    }
]
D. {
    "activity": [
        {
            "type": "golf",
            "level": "beginning",
            "session": "2125"
        }
    ]
}

```

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

A JSON string must start with "{" and end with "}".

**QUESTION 860**

The screenshot shows a network configuration interface with two main tabs: "Layer2" (selected) and "AAA". Under "Layer2", there are sections for "Layer 2 Security" (with a dropdown menu showing "None", "WPA + WPA2", "WPA2 + WPA3", and "Static WEP", where "None" is selected), "MAC Filtering", and "Transition Mode WLAN ID". Under "AAA", there is an "Authorization List\*" section with a dropdown menu showing "default".

A client requests a new SSID that will use web-based authentication and external RADIUS servers. Which Layer 2 security mode must be selected?

- A. None
- B. WPA2 + WPA3
- C. WPA + WPA2
- D. Static WEP

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Under the Layer 2 menu, choose None for Layer 2 Security.

Under the Layer 3 menu, choose None for Layer 3 Security. Check the Web Policy checkbox, and choose Authentication.

**QUESTION 861**

Which resource must a hypervisor make available to the virtual machines?

- A. memory
- B. bandwidth
- C. IP address
- D. secure access

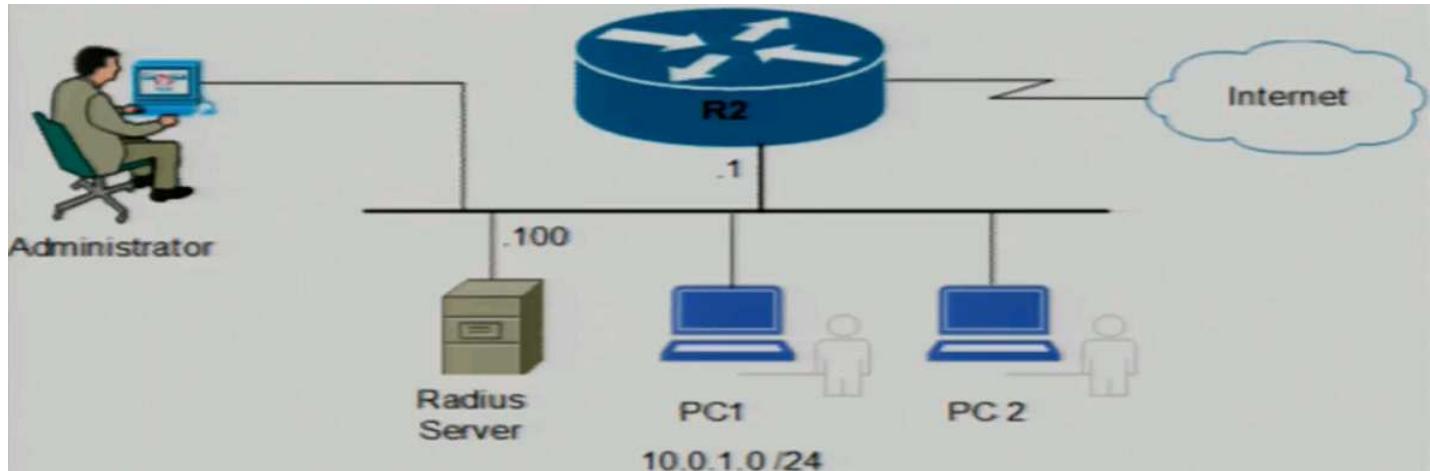
**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 862**



Which command set enables router R2 to be configured via NETCONF?

- A. R1(config)# netconf  
R1(config)# ip http secure-server
- B. R1(config)# username Netconf privilege 15 password example\_password  
R1(config)# netconf-yang  
R1(config)# netconf-yang feature candidate-datastore
- C. R1(config)# snmp-server manager  
R1(config)# snmp-server community ENCOR rw
- D. R1(config)# snmp-server manager  
R1(config)# snmp-server community ENCOR ro

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

NETCONF can be enabled with “netconf-yang” command. Note that NETCONF connections should be authenticated using AAA credentials. RADIUS, TACACS+ or local users defined with privilege level 15 access.

**Reference:**

The Candidate Config Support feature enables support for candidate capability by implementing RFC 6241 with a simple commit option.

Candidate datastore provides a temporary work space in which a copy of the device’s running configuration is stored. You can create and modify the running configuration before committing the running configuration to the device.

**QUESTION 863**

Which method ensures the confidentiality of data exchanged over a REST API?

- A. Use TLS to secure the underlying HTTP session.
- B. Deploy digest-based authentication to protect the access to the API.
- C. Use the POST method instead of URL-encoded GET to pass parameters.
- D. Encode sensitive data using Base64 encoding.

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 864**

Which element is unique to a Type 2 hypervisor?

- A. VM OS
- B. host hardware
- C. host OS
- D. memory

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 865**

Drag and drop the tools from the left onto the agent types on the right.

Which are the tools of Agent-Based type? (Choose two.)

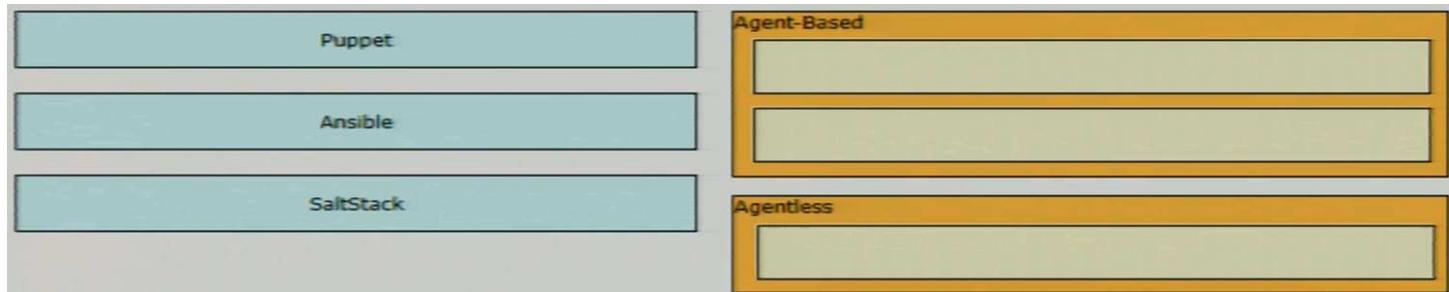
- A. Puppet
- B. Ansible
- C. SaltStack

**Correct Answer:** AC

**Section:** Selected

**Explanation**

**Explanation/Reference:**



**QUESTION 866**

Drag and drop the tools from the left onto the agent types on the right.  
Which is the tool of Agentless type?

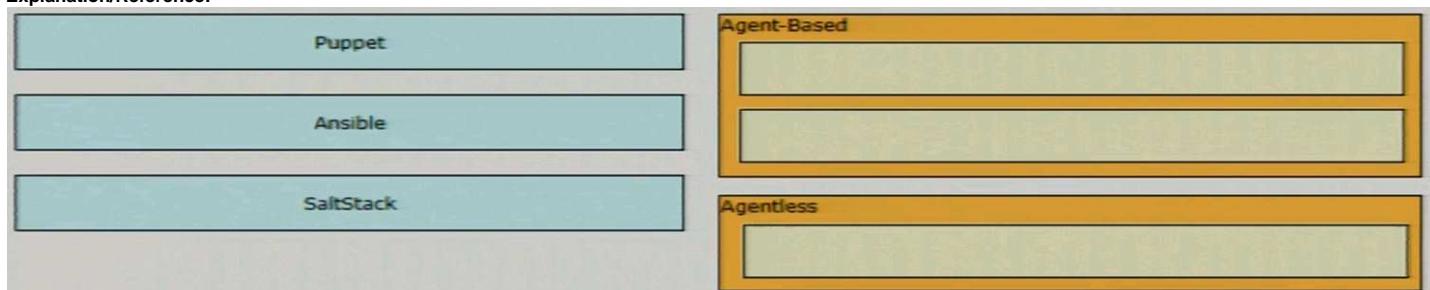
- A. Puppet
- B. Ansible
- C. SaltStack

**Correct Answer: B**

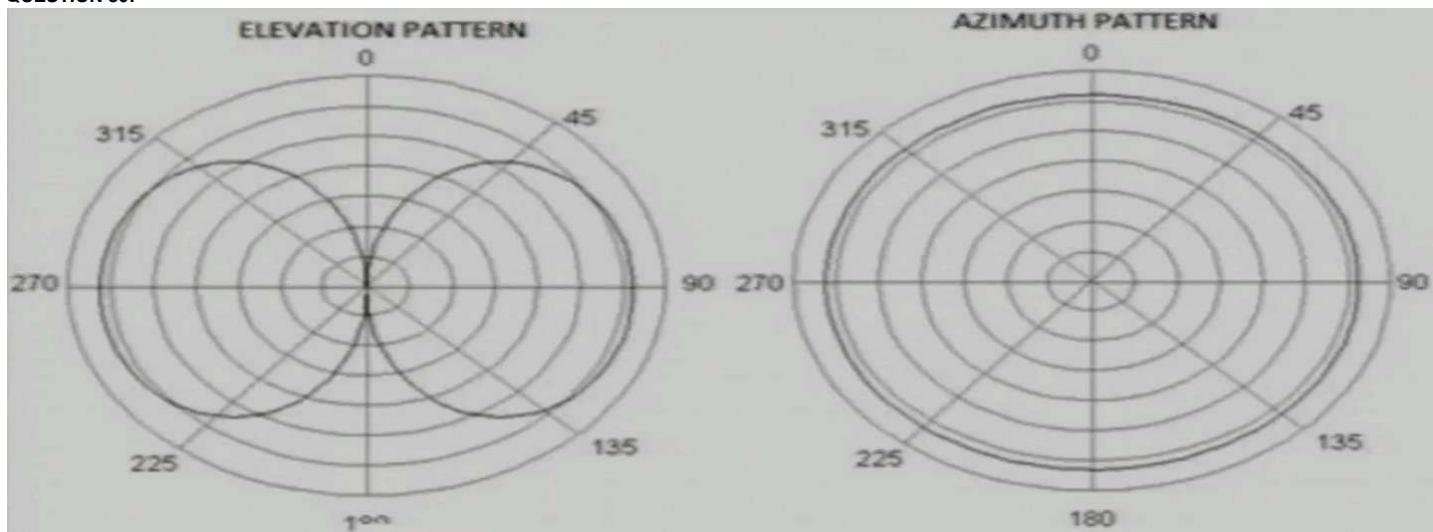
**Section: Selected**

**Explanation**

**Explanation/Reference:**



**QUESTION 867**



Which antenna emits this radiation pattern?

- A. dish
- B. omnidirectional
- C. Yagi
- D. RP-TNC

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 868**

How is OAuth framework used in REST API?

- A. by providing the external application a token that authorizes access to the account
- B. as a framework to hash the security information in the REST URL
- C. as a framework to hide the security information in the REST URL
- D. by providing the user credentials to the external application

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 869**

An engineer must configure a new WLAN that supports 802.11r and requires users to enter a passphrase. What must be configured to support this requirement?

- A. 802.1X and Fast Transition
- B. FT PSK and SUITEB-1X
- C. FT PSK and Fast Transition
- D. 802.1X and SUITEB-1X

Correct Answer: C

Section: Selected

Explanation

Explanation/Reference:

Step 1 Choose WLANs to open the WLANs window.

Step 2 Click a WLAN ID to open the WLANs > Edit window.

Step 3 Choose Security > Layer 2 tab.

Step 4 From the Layer 2 Security drop-down list, choose WPA+WPA2.

The Authentication Key Management parameters for Fast Transition are displayed.

Step 5 From the Fast Transition drop-down list, choose Fast Transition on the WLAN.

Step 6 Check or uncheck the Over the DS check box to enable or disable Fast Transition over a distributed system.

This option is available only if you enable Fast Transition or if Fast Transition is adaptive.

To use 802.11r Fast Transition over-the-air and over-the-ds must be disabled.

Step 7 In the Reassociation Timeout field, enter the number of seconds after which the reassociation attempt of a client to an AP should time out. The valid range is 1 to 100 seconds.

Note : This option is available only if you enable Fast Transition.

Step 8 Under Authentication Key Management, choose FT 802.1X or FT PSK. Check or uncheck the corresponding check boxes to enable or disable the keys. If you check the FT PSK check box, from the PSK Format drop-down list, choose ASCII or Hex and enter the key value.

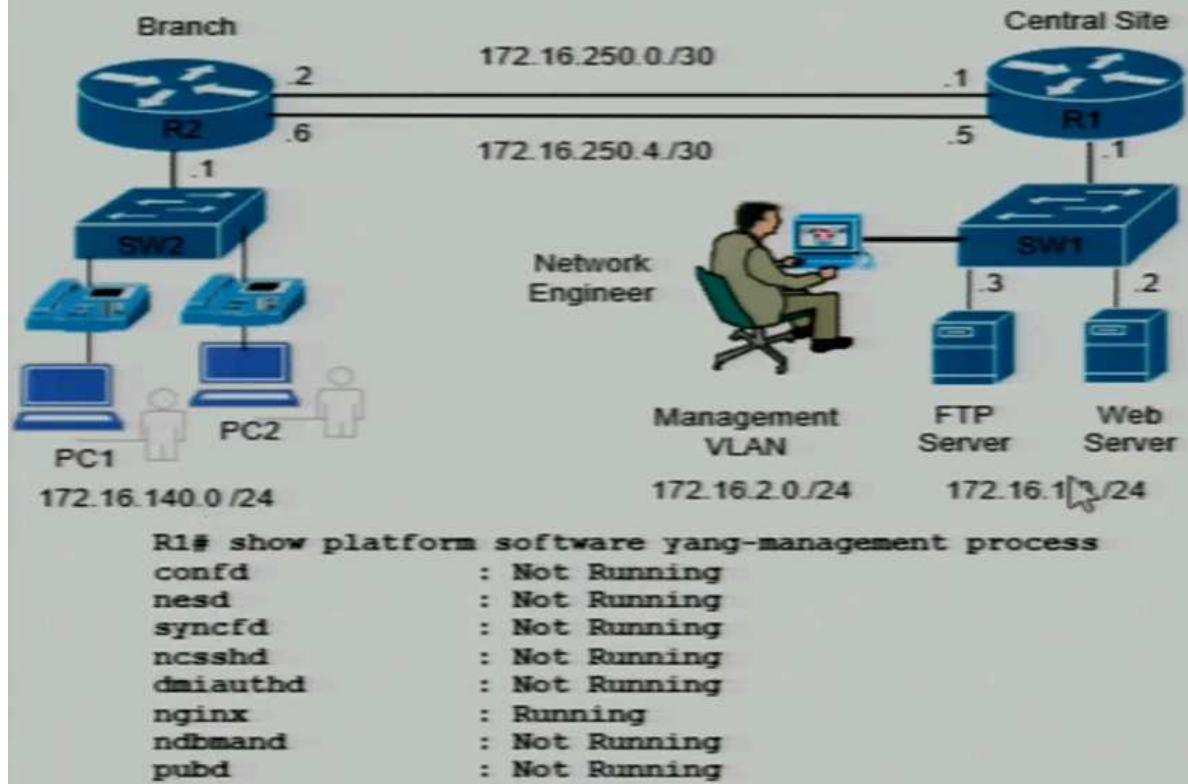
Note : When Fast Transition adaptive is enabled, you can use only 802.1X and PSK AKM..

Step 9 From the WPA gtk-randomize State drop-down list, choose Enable or Disable to configure the Wi-Fi Protected Access (WPA) group temporal key (GTK) randomize state.

Step 10 Click Apply to save your settings.

Since the question requires users to enter a passphrase, therefore PreShared Key (i.e. PSK) should be used instead of 802.1x.

**QUESTION 870**



Which command is required on router R1 to start receiving RESTCONF requests?

- A. R1(config)# ip http access-class 12
- B. R1(config)# ip http server

- C. R1(config)# ip http accounting commands 12 default
- D. R1(config)# restconf

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 871**

Which version of NetFlow does Cisco Threat Defense utilize to obtain visibility into the network?

- A. NBAR2
- B. IPFIX
- C. 8
- D. flexible

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The Cisco Cyber Threat Defense solution takes advantage of the customization capability of the Flexible NetFlow Feature in Cisco IOS.

**QUESTION 872**

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. CAPWAP-CISCO-CONTROLLER
- C. CISCO-CAPWAP-CONTROLLER
- D. CISCO-CONTROLLER-CAPWAP

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 873**

How is CAPWAP data traffic encapsulated when running an Over the Top WLAN in a Cisco SD-Access wireless environment?

- A. LISP
- B. VXLAN
- C. GRE
- D. IPsec

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 874**

```
1  def main():
2      vlans = {'vlan10':'192.168.1.0',
3                'vlan20':'192.168.2.0',
4                'vlan30':'192.168.3.0' }
5      vlans_key(vlans)
6
7  def vlans_key(vlans):
8      for key in vlans.keys():
9          print(str(key) +' '+ str(vlans[key]))
10
11 if __name__ == '__main__':
12     main()
```

What is printed to the console when this script is run?

- A. an error
- B. a key-value pair in list type
- C. a key-value pair in string type
- D. a key-value pair in tuple type

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 875**

What is a characteristic of an AP operating in FlexConnect mode?

- A. All traffic traverses the WLC to ensure policy enforcement on client traffic
- B. Forwarding for locally switched traffic continues when the AP loses connectivity to the WLC
- C. APs connect in a mesh topology and elect a root AP
- D. FlexConnect enables an AP to connect to multiple WLCs

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 876**

What are two benefits of implementing a traditional WAN instead of an SD-WAN solution? (Choose two.)

- A. faster fault detection
- B. lower control plane abstraction
- C. simplified troubleshooting
- D. lower data plane overhead
- E. comprehensive configuration standardization

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 877**

Drag and drop the components of the Cisco SD-Access fabric architecture from the left onto the correct descriptions on the right. Not all options are used.

**Select and Place:**

fabric mode AP	map system that manages endpoint ID to location relationships
CP node	fabric device (for example, Core) that connects external Layer 3 networks to the SD-Access fabric
border node	Fabric device (for example, Access) that connects wired endpoints to the SD-Access fabric
edge node	
fabric wireless controller	

**Correct Answer:**

fabric mode AP	CP node
	border node
	edge node
fabric wireless controller	

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Control-Plane Nodes : Map System that manages Endpoint to Device relationships

Fabric Border Nodes : A Fabric device (e.g. Core) that connects External L3 network(s) to the SDA Fabric

Fabric Edge Nodes : A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric

Fabric Wireless Controller : A Fabric device (WLC) that connects APs and Wireless Endpoints to the SDA Fabric

**QUESTION 878**

```

PYTHON CODE:
import requests
import json

url='http://switch.foo.com/ins'
switchuser='username'
switchpassword='password'

myheaders={'content-type':'application/json'}
payload={
    "ins_api": {
        "version": "1.0",
        "type": "cli_conf",
        "chunk": "0",
        "sid": "1",
        "input": "configure terminal ;interface e1/32 ;shutdown",
        "output_format": "json"
    }
}
response = requests.post(url,data=json.dumps(payload), headers=myheaders,auth=(switchuser,switchpassword)).json()

```

What does the Python code accomplish?

- A. It configures interface e1/32 to be in an admin down state
- B. It generates a status code of 403 because the type is incorrect
- C. It configures interface e1/32 to be in an err-disable state
- D. It returns data in JSON-RPC format

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 879

What is the purpose of an integration API in Cisco DNA Center?

- A. Allow the platform into approval chains in ITSM.
- B. Obtain information about clients, sites, and topology from Cisco DNA Center.
- C. Enable external systems to take actions in response to an event.
- D. Enable discovery and control of the network by using HTTPS verbs.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Integration API (Westbound)

Integration capabilities are part of Westbound interfaces. To meet the need to scale and accelerate operations in modern data centers, IT operators require intelligent, end-to-end work flows built with open APIs. The Cisco DNA Center platform provides mechanisms for integrating Cisco DNA Assurance workflows and data with third-party IT Service Management (ITSM) solutions.

#### QUESTION 880

Which DNS record type is required to allow APs to discover a WLC by using DNS on IPv4?

- A. NS
- B. MX
- C. SOA
- D. A

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 881

What are two NTP poll-based association modes? (Choose two.)

- A. symmetric active
- B. broadcast
- C. client
- D. multicast
- E. asymmetric active

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

A networking device can obtain time information on a network in two ways—by polling host servers and by listening to NTP broadcasts. The following are the two most commonly used poll-based association modes:

- Client mode
- Symmetric active mode

**QUESTION 882**

Which JSON script is properly formatted?

- A. {
 

```
  "class": [
    {
      "title": "Cooking 202",
      "type": "elective",
      "session": "fall"
    }
  ]
}
```
- B. "student": [
 

```
  {
    "grade": "8",
    "ID": "5190345918",
    "type": "on-line",
  }
]
```
- C. [
 

```
  "class": {
    [
      "title": "History",
      "grade": "7",
      "location": "Site 4"
    ]
  }
]
```
- D. {
 

```
  "plants": [
    {
      "name": "Fern",
      "color": "green",
      "type": "indoor",
    }
  ]
}
```

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

A JSON String must start with "{" and end with "}".

An array enclosed by "[ ]" can store different types of values or objects as items. But the item cannot be a key-value pairs e.g. {"name": "Fern"} unless they can be part of an object i.e. the key-value pairs are enclosed by "{ }".

**QUESTION 883**

What is one role of the VTEP in a VXLAN environment?

- A. to maintain VLAN configuration consistency
- B. to provide EID-to-RLOC mapping
- C. to forward packets to non-LISP sites
- D. to encapsulate the tunnel

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The VXLAN tunnel endpoint (VTEP) is the device that's responsible for encapsulating and de-encapsulating layer 2 traffic. This device is the connection between the overlay and the underlay network.

**QUESTION 884**



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 source configuration to enable the ERSPAN tunnel?

- A. (config-mon-erspan-src-dst)# no shut
  - B. (config-mon-erspan-src-dst)# traffic bidirectional
  - C. (config-mon-erspan-src-dst)# monitor session 1 activate
  - D. (config-mon-erspan-src-dst)# ip address 10.10.10.10

**Correct Answer:** D

**Section: (none)**

## Explanation

### **Explanation/Reference:**

**QUESTION 885**

<b>General</b>	<b>Security</b>	<b>QoS</b>	<b>Policy-Mapping</b>	<b>Advanced</b>																																																																	
<table border="0"> <tr> <td>Allow AAA Override</td> <td><input type="checkbox"/> Enabled</td> <td colspan="3"></td> </tr> <tr> <td>Coverage Hole Detection</td> <td><input checked="" type="checkbox"/> Enabled</td> <td colspan="3"></td> </tr> <tr> <td>Enable Session Timeout</td> <td><input checked="" type="checkbox"/></td> <td>1800</td> <td>Session Timeout (secs)</td> <td></td> </tr> <tr> <td>Aironet IE</td> <td><input type="checkbox"/> Enabled</td> <td colspan="3"></td> </tr> <tr> <td>Diagnostic Channel</td> <td><input type="checkbox"/> Enabled</td> <td colspan="3"></td> </tr> <tr> <td>Override Interface ACL</td> <td>IPv4 <input type="button" value="None"/></td> <td>IPv6 <input type="button" value="None"/></td> <td colspan="2"></td> </tr> <tr> <td>Layer2 Adl</td> <td><input type="button" value="None"/></td> <td colspan="3"></td> </tr> <tr> <td>URL ACL</td> <td><input type="button" value="None"/></td> <td colspan="3"></td> </tr> <tr> <td>P2P Blocking Action</td> <td colspan="4">Disabled</td> </tr> <tr> <td>Client Exclusion</td> <td><input checked="" type="checkbox"/> Enabled</td> <td>180</td> <td>Timeout Value (secs)</td> <td></td> </tr> <tr> <td>Maximum Allowed Clients</td> <td><input type="button" value="0"/></td> <td colspan="3"></td> </tr> <tr> <td>Static IP Tunneling</td> <td><input type="checkbox"/> Enabled</td> <td colspan="3"></td> </tr> <tr> <td>Wi-Fi Direct Clients Policy</td> <td colspan="4">Disabled</td> </tr> </table>					Allow AAA Override	<input type="checkbox"/> Enabled				Coverage Hole Detection	<input checked="" type="checkbox"/> Enabled				Enable Session Timeout	<input checked="" type="checkbox"/>	1800	Session Timeout (secs)		Aironet IE	<input type="checkbox"/> Enabled				Diagnostic Channel	<input type="checkbox"/> Enabled				Override Interface ACL	IPv4 <input type="button" value="None"/>	IPv6 <input type="button" value="None"/>			Layer2 Adl	<input type="button" value="None"/>				URL ACL	<input type="button" value="None"/>				P2P Blocking Action	Disabled				Client Exclusion	<input checked="" type="checkbox"/> Enabled	180	Timeout Value (secs)		Maximum Allowed Clients	<input type="button" value="0"/>				Static IP Tunneling	<input type="checkbox"/> Enabled				Wi-Fi Direct Clients Policy	Disabled			
Allow AAA Override	<input type="checkbox"/> Enabled																																																																				
Coverage Hole Detection	<input checked="" type="checkbox"/> Enabled																																																																				
Enable Session Timeout	<input checked="" type="checkbox"/>	1800	Session Timeout (secs)																																																																		
Aironet IE	<input type="checkbox"/> Enabled																																																																				
Diagnostic Channel	<input type="checkbox"/> Enabled																																																																				
Override Interface ACL	IPv4 <input type="button" value="None"/>	IPv6 <input type="button" value="None"/>																																																																			
Layer2 Adl	<input type="button" value="None"/>																																																																				
URL ACL	<input type="button" value="None"/>																																																																				
P2P Blocking Action	Disabled																																																																				
Client Exclusion	<input checked="" type="checkbox"/> Enabled	180	Timeout Value (secs)																																																																		
Maximum Allowed Clients	<input type="button" value="0"/>																																																																				
Static IP Tunneling	<input type="checkbox"/> Enabled																																																																				
Wi-Fi Direct Clients Policy	Disabled																																																																				
<table border="0"> <tr> <td colspan="5"><b>DHCP</b></td> </tr> <tr> <td>DHCP Server</td> <td><input type="checkbox"/> Override</td> <td colspan="3"></td> </tr> <tr> <td>DHCP Addr. Assignment</td> <td><input type="checkbox"/> Required</td> <td colspan="3"></td> </tr> <tr> <td colspan="5"><b>DEAP</b></td> </tr> <tr> <td>Split Tunnel</td> <td><input type="checkbox"/> Enabled</td> <td colspan="3"></td> </tr> <tr> <td colspan="5"><b>Management Frame Protection (MFP)</b></td> </tr> <tr> <td>MFP Client Protection</td> <td><input type="checkbox"/> Optional</td> <td colspan="3"></td> </tr> <tr> <td colspan="5"><b>DTIM Period (in beacon intervals)</b></td> </tr> <tr> <td>802.11a/n (1 - 255)</td> <td><input type="button" value="1"/></td> <td colspan="3"></td> </tr> <tr> <td>802.11b/g/n (1 - 255)</td> <td><input type="button" value="1"/></td> <td colspan="3"></td> </tr> <tr> <td colspan="5"><b>NAC</b></td> </tr> <tr> <td>NAC State</td> <td><input type="button" value="None"/></td> <td colspan="3"></td> </tr> </table>					<b>DHCP</b>					DHCP Server	<input type="checkbox"/> Override				DHCP Addr. Assignment	<input type="checkbox"/> Required				<b>DEAP</b>					Split Tunnel	<input type="checkbox"/> Enabled				<b>Management Frame Protection (MFP)</b>					MFP Client Protection	<input type="checkbox"/> Optional				<b>DTIM Period (in beacon intervals)</b>					802.11a/n (1 - 255)	<input type="button" value="1"/>				802.11b/g/n (1 - 255)	<input type="button" value="1"/>				<b>NAC</b>					NAC State	<input type="button" value="None"/>								
<b>DHCP</b>																																																																					
DHCP Server	<input type="checkbox"/> Override																																																																				
DHCP Addr. Assignment	<input type="checkbox"/> Required																																																																				
<b>DEAP</b>																																																																					
Split Tunnel	<input type="checkbox"/> Enabled																																																																				
<b>Management Frame Protection (MFP)</b>																																																																					
MFP Client Protection	<input type="checkbox"/> Optional																																																																				
<b>DTIM Period (in beacon intervals)</b>																																																																					
802.11a/n (1 - 255)	<input type="button" value="1"/>																																																																				
802.11b/g/n (1 - 255)	<input type="button" value="1"/>																																																																				
<b>NAC</b>																																																																					
NAC State	<input type="button" value="None"/>																																																																				

An engineer is troubleshooting an mDNS issue in an environment where Cisco ISE is used to dynamically assign mDNS roles to users. The engineer has confirmed that ISE is sending the correct values, but name resolution is not functioning as expected. Which WLC configuration change resolves the issue?

- A. Set MFP client protection to Required.
  - B. Change NAC state to ISE NAC.
  - C. Enable AAA Override.
  - D. Enable Aironet IE.

**Correct Answer:** C

**Correct Answer:**  
**Section: (none)**

## Explanation

**Explanation/Reference:****QUESTION 886**

Which feature is provided by Cisco Mobility Services Engine in a Cisco Wireless Unified Network architecture?

- A. It adds client packet capturing
- B. It enables NetFlow data collection
- C. It adds client tracking and location API
- D. It identifies authentication problems

**Correct Answer: C**

Section: (none)

Explanation

**Explanation/Reference:**

The Cisco MSE (Mobility Service Engine) provides two primary services

Context Aware Services (CAS) :

Ability to track the physical location of Network Devices, both wired and wireless, using wireless LAN controllers (WLCs) and Cisco Aironet Lightweight Access Points (LAPs). This solution allows a customer to track any Wi-Fi device, including clients, active RFID tags, and rogue clients and access points (APs).

Adaptive Wireless Intrusion Prevention System (wIPS) :

wIPS software provides visibility and comprehensive threat prevention for the mobility network through monitoring, alerts, classifying, and remediation of wireless and wired network vulnerabilities

**QUESTION 887**

What is a characteristic of Cisco DNA southbound APIs?

- A. utilizes REST API
- B. simplifies management of network devices
- C. enables orchestration and automation of network devices based on intent
- D. implements monitoring by using the SOAP protocol

**Correct Answer: B**

Section: Selected

Explanation

**Explanation/Reference:****QUESTION 888**

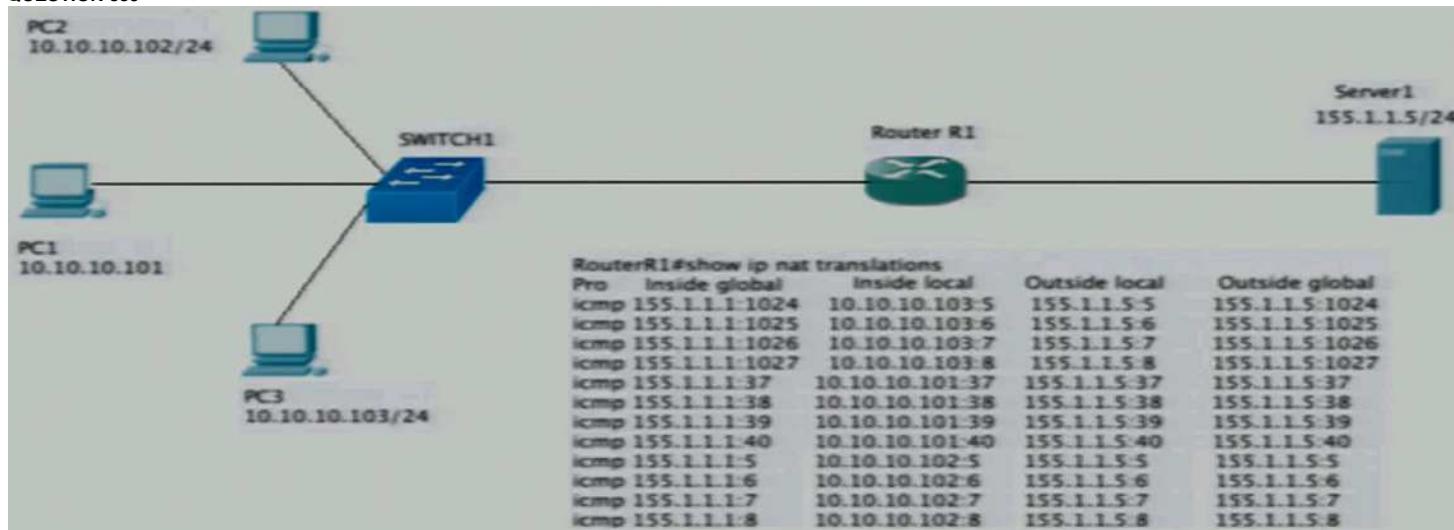
In a campus network design, what are two benefits of using BFD for failure detection? (Choose two.)

- A. BFD speeds up routing convergence time.
- B. BFD is an efficient way to reduce memory and CPU usage.
- C. BFD enables network peers to continue forwarding packets in the event of a restart.
- D. BFD provides fault tolerance by enabling multiple routers to appear as a single virtual router.
- E. BFD provides path failure detection in less than a second.

**Correct Answer: AE**

Section: Selected

Explanation

**Explanation/Reference:****QUESTION 889**

Hosts PC1, PC2, and PC3 must access resources on Server1. An engineer configures NAT on Router R1 to enable the communication and enters the show command to verify operation. Which IP address is used by the hosts when they communicate globally to Server1?

- A. 155.1.1.1
- B. 155.1.1.5
- C. their own address in the 10.10.10.0/24 range
- D. random addresses in the 155.1.1.0/24 range

Correct Answer: A

Section: (none)

Explanation

**Explanation/Reference:**

From the column "Inside global", it shows that all hosts are translated to 155.1.1.1 and therefore they use this address as source in global for accessing Server1.

**QUESTION 890**

High bandwidth utilization is occurring on interface Gig0/1 of a router. An engineer must identify the flows that are consuming the most bandwidth. Cisco DNA Center is used as a flow exporter and is configured with the IP address 192.168.23.1 and UDP port 23000. Which configuration must be applied to set NetFlow data export and capture on the router?

- A. R1(config)# ip flow-export version 9  
R1(config)# ip flow-export destination 192.168.23.1 23000  
R1(config)# interface Gig0/1  
R1(config-if)# ip flow ingress  
R1(config-if)# ip flow egress
- B. R1(config)# ip flow-export  
R1(config)# ip flow-export destination 192.168.23.1 23000  
R1(config)# interface Gig0/1  
R1(config-if)# ip flow monitor
- C. R1(config)# ip flow-export  
R1(config)# ip flow-export destination 192.168.23.1  
R1(config)# interface Gig0/1  
R1(config-if)# collect counter bytes  
R1(config-if)# collect counter packets
- D. R1(config)# ip flow-export version 9  
R1(config)# ip flow-export destination 192.168.23.1 23000  
R1(config)# interface Gig0/1  
R1(config-if)# ip flow-top-talkers

Correct Answer: A

Section: (none)

Explanation

**Explanation/Reference:**

In order to use flexible netflow, the command should be "ip flow monitor <monitor name>" and you need to define the monitor name first.

**QUESTION 891**

Drag and drop the code snippets from the bottom onto the blanks in the code to construct a request that configures policy-based routing.

Select and Place:

```
{
  "route-map": {
    "name": "auto",
    "ios-route-map:route-map-without-order-seq": {
      "ios-route-map:seq_no": "100",
      "ios-route-map:operation": "[ ]",
      "ios-route-map:[ ]": {
        "ios-route-map:ip": {
          "ios-route-map:[ ]": {"ios-route-map:address": "\\" + isp2iprmt + "\"}
        },
        "ios-route-map:match": {
          "ios-route-map:ip": {
            "ios-route-map:[ ]": {"ios-route-map:access-list": "auto"}
          }
        }
      }
    }
  }
}
```

address

permit

next-hop

set

Correct Answer:

```
{
  "route-map": {
    "name": "auto",
    "ios-route-map:route-map-without-order-seq": {
      "ios-route-map:seq_no": "100",
      "ios-route-map:operation": "[ permit ]",
      "ios-route-map:[ set ]": {
        "ios-route-map:ip": {
          "ios-route-map:[ next-hop ]": {"ios-route-map:address": "\\" + isp2iprmt + "\"}
        },
        "ios-route-map:match": {
          "ios-route-map:ip": {
            "ios-route-map:[ address ]": {"ios-route-map:access-list": "auto"}
          }
        }
      }
    }
  }
}
```

[ ]

[ ]

[ ]

[ ]

**Section: (none)****Explanation****Explanation/Reference:****QUESTION 892**

```
*Apr 6 13:35:07.826: AAA/BIND(00000055): Bind i/f
*Apr 6 13:35:07.826: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*Apr 6 13:35:07.826: TPLUS: Queuing AAA Authentication request 85 for processing
*Apr 6 13:35:07.826: TPLUS(00000055) login timer started 1020 sec timeout
*Apr 6 13:35:07.826: TPLUS: processing authentication start request id 85
*Apr 6 13:35:07.826: TPLUS: Authentication start packet created for 85()
*Apr 6 13:35:07.826: TPLUS: Using server 10.106.60.182
*Apr 6 13:35:07.826: TPLUS(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*Apr 6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: socket event 2
*Apr 6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*Apr 6 13:35:07.830: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.830: TPLUS(00000055)/0/READ: Would block while reading
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 18 bytes response
*Apr 6 13:35:07.886: TPLUS(00000055)/0/225FE2DC: Processing the reply packet
*Apr 6 13:35:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*Apr 6 13:35:07.886: TPLUS: Invalid AUTHEN packet (check keys).
```

An engineer configured TACACS+ to authenticate remote users, but the configuration is not working as expected. Which configuration must be applied to enable access?

- A. R1(config)# ip tacacs source-interface Gig 0/0
- B. R1(config)# aaa authorization exec default group tacacs+ local
- C. R1(config)# tacacs server prod  
R1(config-server-tacacs)# key cisco123
- D. R1(config)# tacacs server prod  
R1(config-server-tacacs)# port 1020

**Correct Answer: C****Section: (none)****Explanation****Explanation/Reference:**

The message "received bad AUTHEN packet" appears when the configured shared secret is incorrect.

**QUESTION 893**

What is a difference between Chef and other automation tools?

- A. Chef uses Domain Specific Language, and Puppet uses Ruby.
- B. Chef is an agentless tool that uses a primary/minion architecture, and SaltStack is an agent-based tool that uses a primary/secondary architecture.
- C. Chef is an agent-based tool that uses cookbooks, and Ansible is an agentless tool that uses playbooks.
- D. Chef is an agentless tool that uses playbooks, and Ansible is an agent-based tool that uses cookbooks.

**Correct Answer: C****Section: (none)****Explanation****Explanation/Reference:****QUESTION 894**

```
R1#  
OSPF-1 HELLO Gi0/0: Rcv hello from 10.2.2.2 area 0 10.0.0.2  
OSPF-1 HELLO Gi0/0: No more immediate hello for nbr 10.2.2.2, which has been sent on this intf 2 times  
OSPF-1 HELLO Gi0/0: Send hello to 224.0.0.5 area 0 from 10.0.0.1  
OSPF-1 HELLO Gi0/0: Rcv hello from 10.2.2.2 area 0 10.0.0.2  
OSPF-1 HELLO Gi0/0: No more immediate hello for nbr 10.2.2.2, which has been sent on this intf 2 times  
OSPF-1 HELLO Gi0/0: Send hello to 224.0.0.5 area 0 from 10.0.0.1  
OSPF-1 ADJ Gi0/0: Rcv DBD from 10.2.2.2 seq 0xE09 opt 0x52 flag 0x7 len 32 mtu 1400 state INIT  
OSPF-1 ADJ Gi0/0: 2 Way Communication to 10.2.2.2, state 2WAY  
OSPF-1 ADJ Gi0/0: Neighbor change event  
OSPF-1 ADJ Gi0/0: Nbr 10.2.2.2: Prepare dbase exchange  
OSPF-1 ADJ Gi0/0: Send DBD to 10.2.2.2 seq 0x1C01 opt 0x52 flag 0x7 len 32  
OSPF-1 ADJ Gi0/0: NBR Negotiation Done. We are the SLAVE  
OSPF-1 ADJ Gi0/0: Nbr 10.2.2.2: Summary list built, size 5  
OSPF-1 ADJ Gi0/0: Send DBD to 10.2.2.2 seq 0xE09 opt 0x52 flag 0x2 len 132  
OSPF-1 HELLO Gi0/0: Rcv hello from 10.2.2.2 area 0 10.0.0.2  
OSPF-1 ADJ Gi0/0: Rcv DBD from 10.2.2.2 seq 0xE09 opt 0x52 flag 0x7 len 32 mtu 1400 state EXCHANGE  
OSPF-1 ADJ Gi0/0: Nbr 10.2.2.2 has smaller interface MTU  
OSPF-1 ADJ Gi0/0: Send DBD to 10.2.2.2 seq 0xE09 opt 0x52 flag 0x2 len 132  
OSPF-1 HELLO Gi0/0: Rcv hello from 10.2.2.2 area 0 10.0.0.2  
OSPF-1 HELLO Gi0/0: Send hello to 224.0.0.5 area 0 from 10.0.0.1
```

Two indirectly connected routers fail to form an OSPF neighborship. What is the cause of the issue?

- A. DR/BDR selection dispute
- B. MTU mismatch
- C. OSPF network type mismatch
- D. failing hello packets between the two routers

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 895

Which technology is used as the basis for the Cisco SD-Access data plane?

- A. VXLAN
- B. 802.1Q
- C. LISP
- D. IPsec

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Control Plane – LISP  
Data Plane – VXLAN

#### QUESTION 896

```
CPE# show iox-service  
IOx service (CAF) : Not Running  
IOx service (HA) : Not Supported  
IOx service (IOxman) : Not Running  
Libvirttd : Running  
  
CPE# show platform software yang-management process  
confd : Running  
nesd : Running  
syncfd : Running  
ncsshd : Not Running  
dmiauthd : Running  
nginx : Not Running  
ndbmand : Running  
pubd : Running
```

Which action must be performed to allow RESTCONF access to the device?

- A. Enable the HTTPS service
- B. Enable the SSH service
- C. Enable the NETCONF service
- D. Enable the IOX service

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In the output, the process "nginx" providing the web service is not running.

**QUESTION 897**

Drag and drop the code snippets from the bottom onto the blanks in the PHP script to convert a PHP array into JSON format. Not all options are used.

Select and Place:

```
<?php  
    ( [ ]  
        "Listed devices" => array ( [ ]  
            "Site" => "Backbone",  
            "data" => array ("IP" => "192.168.1.2",  
                "Hostname" => "SW - Core01",  
                "Status" => "Active")  
        ) ;  
  
    $encodedJSON = [ ] ( [ ] , JSON_PRETTY_PRINT);  
  
    print( [ ] );  
?>
```

\$encodedJSON

\$inputArray = array

json\_decode

\$inputArray

json\_encode

Correct Answer:

```
<?php  
    $inputArray = array ( [ ]  
        "Listed devices" => array ( [ ]  
            "Site" => "Backbone",  
            "data" => array ("IP" => "192.168.1.2",  
                "Hostname" => "SW - Core01",  
                "Status" => "Active")  
        ) ;  
  
    $encodedJSON = [ ] json_encode ( [ ] $inputArray , JSON_PRETTY_PRINT);  
  
    print( [ ] $encodedJSON );  
?>
```

json\_decode

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 898**

What is a benefit of using a Type 2 hypervisor instead of a Type 1 hypervisor?

- A. better application performance
- B. improved security because the underlying OS is eliminated
- C. improved density and scalability
- D. ability to operate on hardware that is running other OSs

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 899**

General		Security		QoS		Policy-Mapping		Advanced	
Allow AAA Override	<input checked="" type="checkbox"/> Enabled	Coverage Hole Detection	<input checked="" type="checkbox"/> Enabled	Enable Session Timeout	<input checked="" type="checkbox"/> 1800	Session Timeout (secs)			
Aironet IE	<input checked="" type="checkbox"/> Enabled	Diagnostic Channel	<input type="checkbox"/> Enabled	Override Interface ACL	IPv4 Guest_Permit	IPv6 None			
Layer2 Ad	None	URL ACL	None	P2P Blocking Action	Disabled				
Client Exclusion	<input type="checkbox"/> Enabled	180	Timeout Value (secs)	Maximum Allowed Clients	0				
Static IP Tunneling	<input type="checkbox"/> Enabled			Wi-Fi Direct Clients Policy	Disabled				

An engineer configures a new WLAN that will be used for secure communications; however, wireless clients report that they are able to communicate with each other. Which action resolves this issue?

- A. Enable Client Exclusions
- B. Enable P2P Blocking
- C. Disable Aironet IE
- D. Enable Wi-Fi Direct Client Policy

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

To block traffic between wireless clients, you can enable P2P Blocking Action by setting it to "Drop".

Edit Web Auth Parameter	
General Advanced	
Parameter-map name	global
Banner Title	
Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text <input type="radio"/> File Name
Maximum HTTP connections	100
Init-State Timeout(secs)	120
Type	webauth
Virtual IPv4 Address	192.0.2.100
Trustpoint	3rdPartyCert
Virtual IPv4 Hostname	
Virtual IPv6 Address	xxxxxx
Web Auth Intercept HTTPS	<input type="checkbox"/>
Watch List Enable	<input type="checkbox"/>
Watch List Expiry Timeout(secs)	0

An engineer is configuring WebAuth on a Cisco Catalyst 9800 Series WLC. The engineer has purchased a third-party certificate using the FQDN of the WLC as the CN and intends to use it on the WebAuth splash page. What must be configured so that the clients do not receive a certificate error?

- A. Virtual IPv4 Hostname must match the CN of the certificate.
- B. Trustpoint must be set to the management certificate of the WLC.
- C. Virtual IPv4 Address must be set to a routable address.
- D. Web Auth Intercept HTTPS must be enabled.

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 901**

```

Router# show running-config
! lines omitted for brevity
enable secret 5 $dfefw525ffd$@$R@D2d2d2f
username cisco password 0 cisco
aaa new-model
radius-server host 10.11.11.11 auth-port 1812 acct-port 1646
radius-server host 10.11.11.12 auth-port 1645 acct-port 1646
radius-server key cisco123

```

A network engineer must permit administrators to automatically authenticate if there is no response from either of the AAA servers. Which configuration achieves these results?

- A. aaa authentication login default group radius none
- B. aaa authentication login default group tacacs+ line
- C. aaa authentication enable default group radius local
- D. aaa authentication login default group radius

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Radius must be configured as the first method and there should be a second method configured. Since the question mentioned "automatically authenticate", typing any username/password should not be needed. Hence, the second method should be "none".

#### QUESTION 902

In Cisco DNA Center, what is used to publish events and notifications to a third-party product such as IPAM?

- A. intent API
- B. southbound SDK
- C. integration API
- D. RESTful API

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

There are two ways to provide events / notifications to another application:

- webhooks; and
- integration APIs.

Although both of the above ways can be REST-based, it uses push model (i.e. server sends data to clients when there is something new). It is different from RESTFUL APIs since RESTFUL APIs uses pull model (i.e. client requests data from server).

The followings are extracted from a Cisco web site,  
Eastbound—Events and Notifications APIs

Eastbound APIs publish event notifications that enable third party applications to act on system level, operational or Cisco DNA Assurance notifications. For instance, when some of the devices in the network are out of compliance, an eastbound API can enable an application to execute a software upgrade when it receives a notification. To configure events and notifications webhooks, Cisco DNA Center has to have a call back URL where it will send the notification out.

Westbound—Integration APIs

Cisco DNA Center platform can power end-to-end IT processes across the value chain by integrating various domains such as ITSM, IPAM, and reporting. By leveraging the REST-based Integration Adapter APIs, bi-directional interfaces can be built to allow the exchange of contextual information between Cisco DNA Center and the external, third-party IT systems. The westbound APIs provide the capability to publish the network data, events and notifications to the external systems and consume information in Cisco DNA Center from the connected systems.

#### QUESTION 903

```

ip access-list extended 101
 10 deny ip any any
!
event manager applet Block_Users
  action 1.0 cli command "enable"
  action 2.0 cli command "configure terminal"
  action 3.0 cli command "interface GigabitEthernet1"
  action 4.0 cli command "ip access-group 101 in"
  action 5.0 cli command "ip access-group 101 out"

```

An engineer builds an EEM script to apply an access list. Which statement must be added to complete the script?

- A. action 3.1 cli command "ip access-list extended 101"
- B. event none
- C. action 2.1 cli command "ip access-list extended 101"
- D. action 6.0 cli command "ip access-list extended 101"

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Since the access-list 101 has already been configured, you do not need it in the action of the EEM applet "Block\_Users". Instead, you need an event to specify when the action should be taken. Even if you want to run it manually with "event manager run Block\_Users", you must include "event none" in the applet.

#### QUESTION 904

Drag the characteristics from the left onto the routing protocols they describe on the right  
Which are the characteristics of EIGRP? (Choose two.)

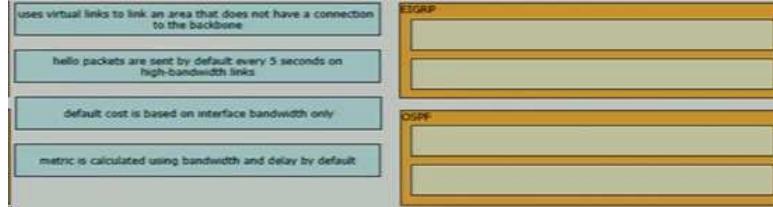
- A. uses virtual links to link an area that does not have a connection to the backbone
- B. hello packets are sent by default every 5 seconds on high-bandwidth links
- C. default cost is based on interface bandwidth only
- D. metric is calculated using bandwidth and delay by default

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 905

Drag the characteristics from the left onto the routing protocols they describe on the right  
Which are the characteristics of OSPF? (Choose two.)

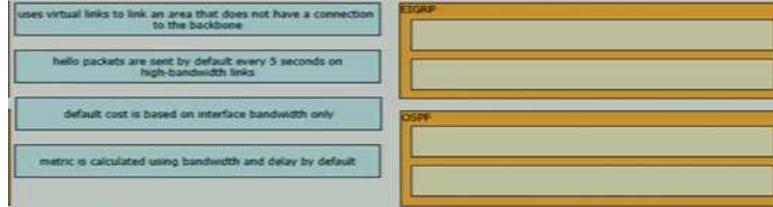
- A. uses virtual links to link an area that does not have a connection to the backbone
- B. hello packets are sent by default every 5 seconds on high-bandwidth links
- C. default cost is based on interface bandwidth only
- D. metric is calculated using bandwidth and delay by default

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 906

What is a difference between OSPF and EIGRP?

- A. OSPF uses a default hello timer of 5 seconds. EIGRP uses a default hello timer of 10 seconds
- B. OSPF uses an administrative distance of 115. EIGRP uses an administrative distance of 160
- C. OSPF uses multicast addresses 224.0.0.5 and 224.0.0.6. EIGRP uses multicast address 224.0.0.10
- D. OSPF uses IP protocol number 88. EIGRP uses IP protocol number 89

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 907

Which mechanism can be used to enforce network access authentication against an AAA server if the endpoint does not support the 802.1X supplicant functionality?

- A. WebAuth
- B. private VLANs
- C. port security
- D. MACsec

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 908

```
args_dict = {'1st_item': '645298791871446',
            '2nd_item_that_must_display': 'jlugyydt'}

for key,value in args_dict.items():
    txt='{:<15} : {:<10}'.format(key,str(value))
    print(txt)
```

What is the output of this code?

- A. 1st\_item##### : 8791871446  
at\_must\_display : jlugyydt
- B. 645298791871446  
##jlugyydt

- C. 1st\_item##### : 645298791871446  
2nd\_item\_that\_must\_display : jlugyydt##
- D. 1st\_item##### : 6452987918  
2nd\_item\_that\_m : jlugyydt##

**Correct Answer:** C  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

When using with "format()":

"{:#<15} means the appending the character "#" if needed so that the first argument (i.e. key) will have at least 15 characters.

"{:#<10}" means appending the character "#" if needed so that the second argument (i.e. str(value)) will have at least 10 characters.

**First line:**

```
1st_item##### : 645298791871446  
123456789012345 (no append is needed)
```

**Second line:**

```
2nd_item_that_must_display : jlugyydt##  
(no append is needed) 1234567890
```

**QUESTION 909**

Which type of antenna is designed to provide a 360-degree radiation pattern?

- A. patch
- B. directional
- C. omnidirectional
- D. Yagi

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 910**

What does the Cisco WLC Layer 3 roaming feature allow clients to do?

- A. roam seamlessly between controllers even when the controller management VLANs are different
- B. maintain their connection between APs even when the AP management VLANs are different
- C. maintain their IP address when roaming to an AP or controller with a different client VLAN assignment
- D. maintain their connection even if the client IP address changes when roaming

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 911**

```
hostname router  
ip domain-name cisco.com  
  
line vty 0 15  
session-timeout 30  
exec-timeout 120 0  
login local
```

Which configuration must be added to enable remote access only using SSHv1 or SSHv2 to this router?

- A. R1(config)# ip ssh version 2  
R1(config)# line vty 0 15  
R1(config-line)# transport input ssh  
R1(config-line)# transport output ssh
- B. R1(config)# line vty 0 15  
R1(config-line)# transport input ssh  
R1(config-line)# transport output ssh
- C. R1(config)# crypto key generate rsa modulus 2048  
R1(config)# ip ssh version 2  
R1(config)# line vty 0 15  
R1(config-line)# transport input all
- D. R1(config)# crypto key generate rsa modulus 2048  
R1(config)# line vty 0 15  
R1(config-line)# transport input ssh

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 912**

Which two actions are recommended as security best practices to protect REST API? (Choose two.)

- A. Use a password hash
- B. Use TACACS+ authentication
- C. Use SSL for encryption
- D. Enable dual authentication of the session
- E. Enable out-of-band authentication

**Correct Answer:** AC

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 913**

What is the VXLAN network Identifier used to identify?

- A. virtual tunnel endpoint
- B. network tunnel interface
- C. IP subnet
- D. broadcast domain

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 914**

Where are operations related to software images located in the Cisco DNA Center GUI?

- A. Services
- B. Assurance
- C. Design
- D. Provisioning

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

"Image Repository" is under the "Design" menu.

Family	Image Name	Device(s)	Version	Advisory	Golden Image	Device Role	Action
Cisco Catalyst IE-3200-8P2S Rugged	1c3200-universalk9.17.06.01.SPA.bin verified	0	17.06.01 Add On (N/A)	0 Critical High <span style="color: yellow;">!</span> Add On (N/A)	ALL <span style="color: yellow;">!</span>		<span style="color: blue;">Import</span> <span style="color: green;">Update Devices</span> <span style="color: orange;">Show Tasks</span> <span style="color: purple;">Take a Tour</span> <span style="color: red;">Physical</span> <span style="color: cyan;">Virtual</span>
	Install Mode (17.06.01.0.144)	1	17.5.1 Add On (N/A)	0 Critical High <span style="color: yellow;">!</span> Add On (N/A)	<span style="color: blue;">Import</span> <span style="color: green;">Update Devices</span> <span style="color: orange;">Show Tasks</span> <span style="color: purple;">Take a Tour</span> <span style="color: red;">Physical</span> <span style="color: cyan;">Virtual</span>		
	ie3200-universalk9.17.02.01.SPA.bin	0	17.2.1 Add On (N/A)	0 Critical High <span style="color: yellow;">!</span> Add On (N/A)	<span style="color: blue;">Import</span> <span style="color: green;">Update Devices</span> <span style="color: orange;">Show Tasks</span> <span style="color: purple;">Take a Tour</span> <span style="color: red;">Physical</span> <span style="color: cyan;">Virtual</span>		

**QUESTION 915**

```
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 15  
no exec-timeout
- B. line vty 0 15  
exec-timeout 10 0
- C. line vty 0 15  
absolute-timeout 600
- D. line vty 0 4  
exec-timeout 600

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

```
R1(config-line)#exec-timeout ?
<0-35791> Timeout in minutes
R1(config-line)#exec-timeout 10 ?
<0-2147483> Timeout in seconds
<cr>
```

**QUESTION 916**

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 917**

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 authentication exec default radius
- B. aaa authorization exec default radius
- C. aaa authentication exec default radius local
- D. aaa authorization exec default radius local

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

"aaa authentication exec ..." does not exist.

A better answer should be "aaa authentication login default group radius local".

**QUESTION 918**

Drag and drop the code snippets from the bottom onto the blanks in the script to convert a Python object into a compact JSON object by removing space characters. Not all options are used.

**Select and Place:**

```

import json

data = {
    "measurement": "cpmCPUTotalInMinRev",
    "collectionInterval": "default",
    "tagCount": "0",
    "policy": None,
    "devices": [{"model": "Cisco 3500 Series WLC", "ipv4": "10.10.20.52"}]
}

obj = json._____([{"key": "loads", "value": "dumps"}])

print(obj)

separators=(',', ':')

data
"loads"
"dumps"

```

**Correct Answer:**

```

import json

data = {
    "measurement": "cpmCPUTotalInMinRev",
    "collectionInterval": "default",
    "tagCount": "0",
    "policy": None,
    "devices": [{"model": "Cisco 3500 Series WLC", "ipv4": "10.10.20.52"}]
}

obj = json._____("dumps")([{"key": "loads", "value": "data"}], separators=(',', ':'))

print(obj)

"loads"

```

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 919

802.11a > RRM > Dynamic Channel Assignment (DCA)

##### Dynamic Channel Assignment Algorithm

Channel Assignment Method	<input checked="" type="radio"/> Automatic	Interval: 10 minutes	AnchorTime: 0
	<input type="radio"/> Freeze	Invoke Channel Update Once	
	<input type="radio"/> OFF		
Avoid Foreign AP interference	<input checked="" type="checkbox"/> Enabled		
Avoid Cisco AP load	<input type="checkbox"/> Enabled		
Avoid non-802.11a noise	<input checked="" type="checkbox"/> Enabled		
Avoid Persistent Non-WiFi Interference	<input type="checkbox"/> Enabled		
Channel Assignment Leader			
Last Auto Channel Assignment	85 secs ago		
DCA Channel Sensitivity	Medium	(15 dB)	
Channel Width	<input type="radio"/> 20 MHz	<input checked="" type="radio"/> 40 MHz	<input type="radio"/> 80 MHz
Avoid check for non-DFS channel	<input type="checkbox"/> Enabled		
<b>DCA Channel List</b>			
DCA Channels	36, 40, 44, 48, 52, 56, 60, 64		
Select	Channel		
<input checked="" type="checkbox"/>	36		
<input checked="" type="checkbox"/>	40		
<input checked="" type="checkbox"/>	44		
<input type="checkbox"/>	--		
Extended UNII-2 channels <input type="checkbox"/> Enabled			
<b>Event Driven RRM</b>			
EDRAM	<input type="checkbox"/> Enabled		

An engineer is troubleshooting an issue with non-Wi-Fi interference on the 5-GHz band. The engineer has enabled Cisco CleanAir and set the appropriate traps, but the AP does not change the channel when it detects significant interference. Which action will resolve the issue?

- A. Change the DCA Sensitivity option to High
- B. Disable the Avoid Foreign AP Interference option
- C. Enable the Avoid Persistent Non-WiFi Interference option
- D. Enable the Event Driven Radio Resource Management option

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

EDRRM is a feature that allows an access point that is in distress to bypass normal RRM intervals and immediately change channels.

**QUESTION 920**

Which Cisco FlexConnect state allows wireless users that are connected to the network to continue working after the connection to the WLC has been lost?

- A. Authentication-Central/Switch-Local
- B. Authentication Down/Switching Down
- C. Authentication-Central/Switch-Central
- D. Authentication-Down/Switch-Local

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 921**

```
pt1= [
<get-config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <filter>
    <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
      <ip>
        <access-list>
          <extended xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-acl">
            <name>TEST-ACL</name>
            <extended>
              <access-list>
                <ip>
                  <native>
                    <filter>
                      <get-config>

```

with manager connect(host=10.1.1.1, port=830, username=cisco, password=cisco, timeout=90, hostkey\_verify=False) as m:  
for rpc in pt1:  
 r1= m.dispatch(et.fromstring(rpc))  
 d1= xmldict.parse(r1.xml)[('rpc-reply')[('data')[('native')[('ip')[('access-list')[('extended')[('access-list-seq-rule')]]]]]]]

What is achieved by the XML code?

- A. It reads the access list sequence numbers from the output of the show ip access-list extended fip command into a dictionary list
- B. It displays the access list sequence numbers from the output of the show ip access-list extended fip command on the terminal screen
- C. It displays the output of the show ip access-list extended fip command on the terminal screen
- D. It reads the output of the show ip access-list extended fip command into a dictionary list

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since there is no print(), no output will be displayed.

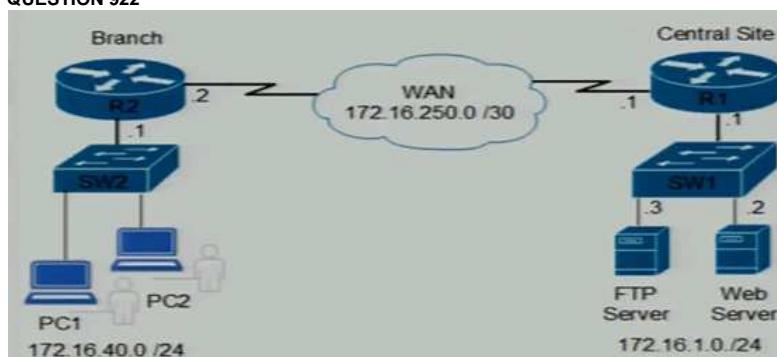
The program code just converts specific XML data obtained to a dictionary. The specific data is the sequence numbers in the access list fip i.e. the information under the tag "<access-list-seq-rule>". Note that the details of each rule are also included.

The following shows the part of the XML data obtained for a sample access list "TEST-ACL":

```
<extended xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-acl">
  <name>TEST-ACL</name>
  <access-list-seq-rule>
    <sequence>10</sequence>
    <ace-rule>
      <action>permit</action>
      <protocol>esp</protocol>
      <any/>
      <dst-any/>
    </ace-rule>
    <sequence>20</sequence>
    <ace-rule>
      <action>permit</action>
      <protocol>ah</protocol>
      <any/>
      <dst-any/>
    </ace-rule>
  </access-list-seq-rule>
</extended>
```

The dictionary returned for the above XML data using the xmldict() in the question will be :

```
{'sequence': ['10', '20'], 'ace-rule': [{'action': 'permit', 'protocol': 'esp', 'any': None, 'dst-any': None}, {'action': 'permit', 'protocol': 'ah', 'any': None, 'dst-any': None}]}
```

**QUESTION 922**

Which command is required to validate that an IP SLA configuration matches the traffic between the branch office and the central site?

- A. R1# show ip sla statistics
- B. R1# show ip sla configuration
- C. R1# show ip sla group schedule
- D. R1# show ip route

**Correct Answer: B**

Section: (none)

Explanation

Explanation/Reference:

#### QUESTION 923

The screenshot shows the 'Edit WLAN' configuration interface. Key settings include:

- Layer 2 Security Mode: WPA + WPA2
- Protected Management Frame: PMF (Disabled)
- WPA Parameters: WPA2 Policy (checked)
- WPA2 Encryption: AES(CCMP128) (selected)
- Auth Key Mgmt: 802.1x (checked)

Which action must be taken to configure a WLAN for WPA2-AES with PSK and allow only 802.11r-capable clients to connect?

- A. Enable Fast Transition and FT + PSK
- B. Change Fast Transition to Adaptive Enabled and enable FT + PSK
- C. Enable PSK and FT + PSK
- D. Enable Fast Transition and PSK

**Correct Answer: A**

Section: Selected

Explanation

Explanation/Reference:

The two settings are :

- Select "Enable" in the following setting near the top right corner

The screenshot shows the 'Edit WLAN' configuration interface. The 'Fast Transition' dropdown is set to 'Enabled'.

- Check the following box near the bottom.

The screenshot shows the 'Edit WLAN' configuration interface. In the 'Auth Key Mgmt' section, the 'FT + PSK' checkbox is checked.

#### QUESTION 924

An engineer must configure a Cisco WLC with WPA2 Enterprise mode and avoid global server lists. Which action is required?

- A. Select a RADIUS authentication server
- B. Apply CISCO ISE default settings
- C. Disable the RADIUS server accounting interim update
- D. Enable EAP parameters

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

If a RADIUS server is selected for a WLAN, then that WLAN will use the selected RADIUS server for authentication instead of using those RADIUS servers configured in the global list.

**QUESTION 925**

How are control traffic, client authentication and data traffic handled in a mobility express environment?

- A. Control traffic and client authentication is handled centrally by the controller. Data traffic is switched centrally by the controller
- B. Control traffic and client authentication is handled centrally by the controller. Data traffic is switched locally by the access points
- C. Control traffic and client authentication is handled locally by each access point. Data traffic is switched locally by the access points
- D. Control traffic and client authentication is handled locally by each access point. Data traffic is switched centrally by the controller

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Mobility Express is based on the Flex architecture and supports central authentication and local switching of data traffic.

**QUESTION 926**

What is the purpose of Cisco Express Forwarding adjacency tables?

- A. To attach Layer 2 addressing information
- B. To allow Cisco Express Forwarding for switching decisions based on IP destinations
- C. To attach Layer 3 addressing information
- D. To allow Cisco Express Forwarding for switching decisions based on IP source addresses

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The FIB contains information about the best next hop for each destination network, while the Adjacency Table contains information about the Layer 2 headers and interfaces for each next hop.

During forwarding:

- The router extracts the destination IP address from the packet header when a packet reaches the router interface, then searches the FIB for the excellent matched path and its next-hop address (i.e. for making switching decisions)
- The router then consults the Adjacency Table to find the corresponding Layer 2 header and interface for the next hop. The router adds the Layer 2 header to the packet and forwards it to the appropriate interface.

**QUESTION 927**

Drag and drop the characteristics from the left onto the corresponding switching architectures on the right.

What are the suitable characteristics for RIB? (Choose two)

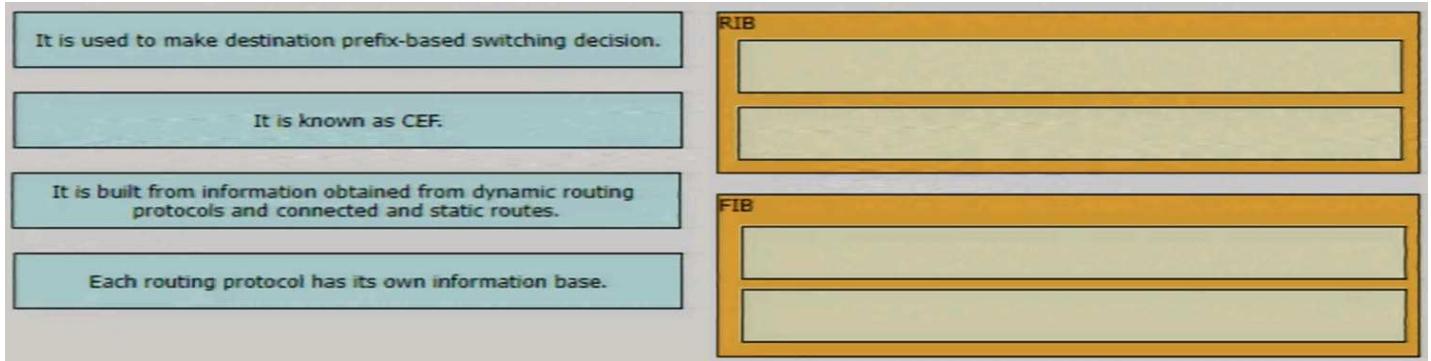
- A. It is used to make destination prefix-based switching decision
- B. It is known as CEF
- C. It is built from information obtained from dynamic routing protocols and connected and static routes
- D. Each routing protocol has its own information base

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 928**

Drag and drop the characteristics from the left onto the corresponding switching architectures on the right.  
What are the suitable characteristics for FIB? (Choose two)

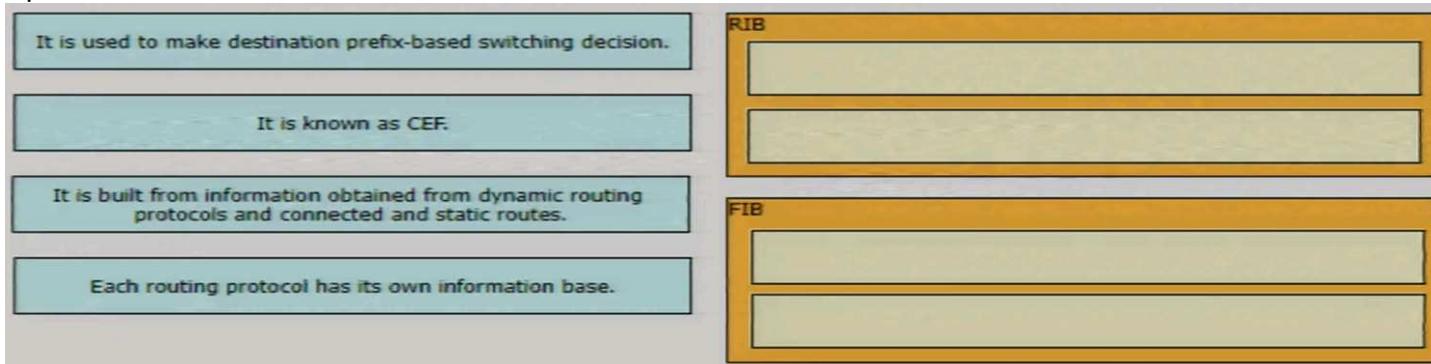
- A. It is used to make destination prefix-based switching decision
- B. It is known as CEF
- C. It is built from information obtained from dynamic routing protocols and connected and static routes
- D. Each routing protocol has its own information base

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 929**

Drag and drop the code snippets from the bottom onto the blanks in the Python script to print the device model to the screen and write JSON data to file. Not all options are used.

**Select and Place:**

```
import json

data = {
    "measurement": "ifHCInOctets",
    "maxDataPoints": 30,
    "policy": "default",
    "params": None,
    "devices": [
        {"model": "Cisco Nexus 3550", "ipv4": '172.16.16.249'}
    ]
}
[ ] (data["devices"][0]["model"])
with [ ] ("data.json", " [ ] ") as file:
    json. [ ] (data, file, indent=4)
```

[ ] dumps [ ] print [ ] dump [ ] open [ ] r [ ] w

**Correct Answer:**

```

import json

data = {
    "measurement": "ifHCInOctets",
    "maxDataPoints": 30,
    "policy": "default",
    "params": None,
    "devices": [
        {"model": "Cisco Nexus 3550", "ipv4": '172.16.16.249'}
    ]
}
print(data["devices"][0]["model"])
with open("data.json", "w") as file:
    json.dump(data, file, indent=4)

```

dumps

open

w

r

**Section: Selected Explanation**

**Explanation/Reference:**

For outputting JSON to a file, the following is required:

- The file must be opened in write mode (i.e. "w")
- The function "dump" should be used if you want the JSON to be written a target file.

Remarks :

The other function "dumps()" writes the JSON output to a string.

**QUESTION 930**

Which Cisco DNA Center Assurance feature verifies host reachability?

- A. network time travel
- B. detail information
- C. path trace
- D. application experience

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

When you initiate a path trace, the Cisco DNA Center controller reviews and collects network topology and routing data from the discovered devices. It then uses this data to calculate a path between the two hosts or Layer 3 interfaces, and displays the path in a path trace topology. The topology includes the path direction and the devices along the path, including their IP addresses.

**QUESTION 931**

Which character formatting is required for DHCP Option 43 to function with current AP models?

- A. ASCII
- B. MD5
- C. Hex
- D. Base64

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 932**

Which collection contains the resources to obtain a list of fabric nodes through the vManage API?

- A. device inventory
- B. administration
- C. device management
- D. monitoring

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 933**

```

<interface>
    <Loopback>
        <name>100</name>
        <enabled>true</enabled>
    </Loopback>
</interface>

```

What is achieved by this code?

- A. It deletes the loopback interface
  - B. It displays the loopback interface
  - C. It renames the loopback interface
  - D. It unshuts the loopback interface

**Correct Answer: D**

## Section: (none)

## Explanation

### **Explanation/Reference:**

## QUESTION 934

Which policy feature is used with TrustSec to provide endpoint entitlement in an enterprise network?

- A. access control lists
  - B. virtual local area network
  - C. security group tags
  - D. virtual routing and forwarding

**Correct Answer:** C

**Section: (none)**

### **Explanation**

#### **Explanation/Reference:**

## QUESTION 935

The Radio Resource Management software that is embedded in the Cisco WLC acts as a manager to constantly monitor over-the-air metrics. Which other factor does the Radio Resource Management software detect?

- A. presence of rogue APs or malicious SSIDs
  - B. unauthorized wireless network access
  - C. repeated attempts to authenticate to a wireless network
  - D. end-node vulnerabilities

**Correct Answer:** A

**Section: (none)**

### **Explanation**

#### **Explanation/Reference:**

The Radio Resource Management (RRM) software embedded in the Cisco Wireless LAN Controller acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. RRM enables Cisco WLCs to continually monitor their associated lightweight access points for the following information:

- Traffic load: The total bandwidth used for transmitting and receiving traffic. It enables wireless LAN managers to track and plan network growth ahead of client demand.

Interference: The amount of traffic coming from other 802.11 sources.

Noise: The amount of non-802.11 traffic that is interfering with the currently assigned channel.

Coverage: The received signal strength (RSSI) and signal-to-noise ratio (SNR) for all connected clients.

Other: The number of nearby access points.

## QUESTION 936



```
hostname Switch-1
!
interface GigabitEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan10
 ip address 192.168.1.254 255.255.255.0
!
router ospf 1
 router-id 10.1.1.1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
!

hostname Switch-2
!
interface GigabitEthernet0/0
 ip address 10.1.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan20
 ip address 192.168.2.254 255.255.255.0
!
router ospf 1
 router-id 10.1.1.2
 log-adjacency-changes
 network 10.1.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 1
```

An engineer must prevent VLAN 20 routes from appearing in the routing table of Switch-1. Which command set must be applied?

- A. On Switch-2:  
router ospf 1

- ```

distribute-list 1 in
access-list 1 deny 192.168.2.0 0.0.0.255
B. On Switch-1:
router ospf 1
distribute-list 1 out
access-list 1 deny 192.168.2.0 0.0.0.255
C. On Switch-1:
router ospf 1
distribute-list 1 in
access-list 1 deny 192.168.2.0 0.0.0.255
D. On Switch-2:
router ospf 1
distribute-list 1 out
access-list 1 permit 192.168.2.0 0.0.0.255

```

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

You cannot use "distribute-list ... out ..." in Switch-2 since the Switch-2 is not an ASBR and the route "192.168.2.0" is not an external route redistributed into OSPF in that router.

In this question, since there is only one OSPF route learnt by Switch-1, the suggested answer can do what the question required. However, if Switch-1 needs to add other OSPF routes into the routing table, "access-list 1 permit any" has to be appended at the end of the access-list 1.

**QUESTION 937**

An engineer modifies the existing ISE guest portal URL to use a static FQDN. Users immediately report that they receive certificate errors when they are redirected to the new page. Which two additional configuration steps are needed to implement the change? (Choose two.)

- A. Add a new DNS record to resolve the FQDN to the PSN IP address
- B. Create and sign a new CSR that contains the static FQDN entry
- C. Manually configure the hosts file on each user device
- D. Disable HTTPS on the WLC under the Management menu
- E. Add the FQDN entry under the WLC virtual interface.

**Correct Answer:** AB

**Section:** (none)

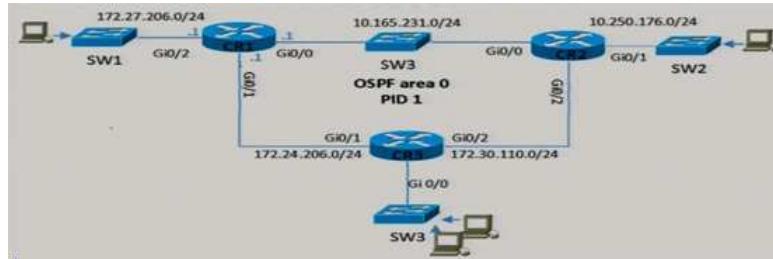
**Explanation**

**Explanation/Reference:**

You need to specify the FQDN in WLC if you want WLC to provide the portal for login. Since ISE's guest portal is used in the question, the FQDN should be configured in ISE. The URL containing the FQDN for redirection to the guest portal will be provided through a cisco-av-pair in RADIUS Access-Accept. Therefore the FQDN is not configured in WLC.

In this question, the FQDN should already been configured in the ISE since it says "An engineer modifies the existing ISE guest portal URL to use a static FQDN". Therefore the question is asking what other actions should be performed.

**QUESTION 938**



CR2 and CR3 are configured with OSPF. Which configuration, when applied to CR1, allows CR1 to exchange OSPF formation with CR2 and CR3 but not with other network devices or on new interfaces that are added to CR1?

- A. router ospf 1
 

```
network 10.0.0.0 255.255.255.255 area 0
      passive-interface GigabitEthernet0/2
```
- B. 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
```
- C. 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
      passive-interface GigabitEthernet0/2
```
- D. interface G1/0/2
 

```
ip ospf 1 area 0
      router ospf 1
      passive-interface GigabitEthernet0/2
```

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The command "network 172.27.206.0 0.0.0.255 area 0" is needed in order to let CR1 advertises this network to CR2 and CR3. The command "passive-interface GigabitEthernet0/2" will then prevent CR1 from forming any neighbor with device in this network to learn route.

**QUESTION 939**

Drag and drop the code snippets from the bottom onto blanks in the Python script so that the program changes the IP address and saves it as a new JSON file on the disk. Not all options are used.

Select and Place:

### Answer Area

```
import json

with open("json ios xe.json", "r") as json_file:
    json_file_content = json_file. read()

decoded_json = json. loads()(json_file_content)

decoded_json['Cisco-IOS-XE-native:interface']['GigabitEthernet'][0]['ip']
    ['address']['primary']['address'] = \ "192.168.1.2"

encoded_json_compact = json. dumps()(decoded_json)
encoded_jsonIndented = json.dumps(decoded_json, indent = 4)

with open("json ios xe compact.json", "w") as json_file:
    json_file. write()(encoded_json_compact)

with open("json ios xe indented.json", "w") as json_file:
    json_file.write(encoded_jsonIndented)
```

write() loads() dumps() open() read()

Correct Answer:

### Answer Area

```
import json

with open("json ios xe.json", "r") as json_file:
    json_file_content = json_file. read()

decoded_json = json. loads()(json_file_content)

decoded_json['Cisco-IOS-XE-native:interface']['GigabitEthernet'][0]['ip']
    ['address']['primary']['address'] = \ "192.168.1.2"

encoded_json_compact = json. dumps()(decoded_json)
encoded_jsonIndented = json.dumps(decoded_json, indent = 4)

with open("json ios xe compact.json", "w") as json_file:
    json_file. write()(encoded_json_compact)

with open("json ios xe indented.json", "w") as json_file:
    json_file.write(encoded_jsonIndented)
```

open() \_\_\_\_\_

Section: Selected  
Explanation

**Explanation/Reference:**

`loads()` Convert a string in JSON format to a Python object

`load()` Read JSON in a file and convert it to a Python object. Therefore, this performs both `read()` for file and then `loads()`.

`dumps()` Convert a Python object to a string in JSON format

`dump()` Convert a Python object to JSON for writing to a file. Therefore, this performs both `dumps()` and then `write()` to file.

In this question, instead of the simpler “`load()`” and “`dump()`”, it handles the files and performs conversion separately in two steps for each operation. Therefore, four commands are needed instead of two.

**QUESTION 940**

```

1 def main():
2     vlans_list = [10, 20, 30]
3     add_vlans(vlans_list)
4     print(vlans_list)
5 def add_vlans(vlans):
6     for i in range(len(vlans)):
7         vlans[i] += 100
8
9 if __name__ == '__main__':
10    main()

```

What is the result of running this code?

- A. A list of new VLANs is created
- B. A list of lists is created
- C. A dictionary is created
- D. An error is displayed

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In the original list "vlans\_list", the items are 10, 20 and 30. When "add\_vlans()" is called, 100 is added to each of the items. Therefore, the printout will be as follows:  
[110, 120, 130]

#### QUESTION 941

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.

Select and Place:

#### Answer Area

```

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

data

decode

.encode

JSONDecoder

**Correct Answer:**

#### Answer Area

```

import json

data = {
    "measurement": "cefcFRUPowerOperStatus",
    "maxDataPoints": 45,
    "alert": "True",
    "errorDescription": None,
    "devices": [{"model": "Cisco 4331 ISR"}, {"model": "Cisco 3500 S"}]
}

obj = json. JSONEncoder(). [ ] .encode( [ ] data [ ] )

print(obj)

```

[ ]

decode

[ ]

JSONDecoder

**Section: Selected**  
**Explanation**

**Explanation/Reference:**

Other than using answer in this question, the same JSON string can be stored in the variable "obj" with:  
`obj = json.dumps(data)`

Usually, instead of using the class "JSONEncoder" directly, it is used for creating subclasses in which you can customize how the conversion to JSON should be performed when "encode()" is called.

**QUESTION 942**

How does a WLC achieve stateful switchover for APs and clients?

- A. The active and standby WLCs establish separate CAPWAP tunnels to the AP
- B. The active WLC establishes a CAPWAP tunnel to the AP, and the standby WLC establishes a LWAPP tunnel to the AP
- C. The active WLC establishes a CAPWAP tunnel with the AP and standby WLC to share the AP database information
- D. The active WLC establishes a CAPWAP tunnel with the AP, and the standby WLC copies the AP database and the client database from the active WLC

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The new High Availability (HA) feature (that is, AP SSO) set within the Cisco Unified Wireless Network software release version 8.0 and above allows the access point (AP) to establish a CAPWAP tunnel with the Active WLC and share a mirror copy of the AP database with the Standby WLC.

Since a mirror copy of the database is shared, the standby WLC is not sharing the same actual database used by the active WLC. The database used by standby WLC is therefore copied from the actual database.

**QUESTION 943**

Which way are EIGRP and OSPF similar?

- A. They both support MD5 authentication for routing updates
- B. They have similar CPU usage, scalability, and network convergence times
- C. They both support autosummarization
- D. They both support unequal-cost load balancing

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

OSPF does not support automatic summarization

OSPF does not support unequal-cost load balancing

**QUESTION 944**

```
Python 3.10.2 (tags/v3.10.2:a58ebcc, Jan 17 2022, 14:12:15) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>>
>>> customer1 = {
...     "inventory": {
...         "device": [
...             {
...                 "hostname": "asr9k-01",
...                 "ver": "16.09",
...                 "vendor": "cisco",
...                 "uptime": "39 days",
...                 "serial": "XX123456",
...             }
...         ]
...     }
... }
>>>
```

Which class type is returned for the command prompt "type(customer1)"?

- A. dict
- B. str
- C. list
- D. tuple

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

The Python object stored in the variable "customer1" is a "dict" i.e. a dictionary

```
customer1 = { ←
    "inventory": { ←
        "device": [ ←
            {
                "hostname": "asr9k-01",
                "ver": "16.09",
                "vendor": "cisco",
                "uptime": "39 days",
                "serial": "XX123456",
            }
        ]
    } ←
}
```

For Python objects:

```
dict    is an object enclosed by { }
```

```
list    is an object enclosed by [ ]
```

```
tuple   is an object enclosed by ( )
```

**QUESTION 945**

What is a characteristic of vManage?

- A. It leverages the overlay management protocol to interface with WAN Edge devices
- B. It supports protocols such as OSPF to integrate with legacy network devices
- C. It requires a public IP address to allow WAN Edge devices to discover fabric components
- D. It uses NETCONF to configure vSmart devices to build the overlay network data plane

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The primary components for the Cisco Catalyst SD-WAN solution consist of the SD-WAN Manager network management system (management plane), the SD-WAN Controller (control plane), the SD-WAN Validator (orchestration plane), and the WAN Edge router (data plane).

SD-WAN Manager (former known as vManager) - This centralized network management system is software-based and provides a GUI interface to easily monitor, configure, and maintain all Cisco Catalyst SD-WAN devices and their connected links in the underlay and overlay network. (vManager use NETCONF to configure other components in the SD-WAN).

SD-WAN Controller (formerly known as vSmart) - This software-based component is responsible for the centralized control plane of the SD-WAN network. It maintains a secure connection to each WAN Edge router and distributes routes and policy information via the Overlay Management Protocol (OMP), acting as a route reflector. It also orchestrates the secure data plane connectivity between the WAN Edge routers by reflecting crypto key information originating from WAN Edge routers, allowing for a very scalable, IKE-less architecture.

SD-WAN Validator (former known as vBond) - This software-based component performs the initial authentication of WAN Edge devices and orchestrates SD-WAN Controller, Manager, and WAN Edge connectivity. It also has an important role in enabling the communication between devices that sit behind Network Address Translation (NAT).

WAN Edge router - This device, available as either a hardware appliance or software-based router, sits at a physical site or in the cloud and provides secure data plane connectivity among the sites over one or more WAN transports. It is responsible for traffic forwarding, security, encryption, quality of service (QoS), routing protocols such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF), and more.

**QUESTION 946**

What is one characteristic of Cisco DNA Center and vManage northbound APIs?

- A. They implement the NETCONF protocol
- B. They exchange XML-formatted content.
- C. They push configuration changes down to devices
- D. They implement the RESTCONF protocol

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 947**

What does the statement print(format(0.8, '.0%')) display?

- A. .08%
- B. 8.8%
- C. 8%
- D. 80%

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

For the 2nd argument supplied when calling the function "format()":

"0" means converting into percentage format"

".0%" means the converted result should be rounded so that there is "0" number of digit after the decimal point.

```
print(format(0.801234, '.0%')) # this prints '80%
```

```
print(format(0.801234, '.3%')) # this prints '80.123'
```

**QUESTION 948**

What is one fact about Cisco SD-Access wireless network deployments?

- A. The WLC is part of the fabric underlay
- B. The wireless client is part of the fabric overlay
- C. The access point is part of the fabric underlay
- D. The access point is part of the fabric overlay

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 949**

Which characteristic applies to a traditional WAN solution but not to a Cisco SD-WAN solution?

- A. centralized reachability, security, and application policies
- B. low complexity and increased overall solution scale
- C. time consuming configuration and maintenance
- D. operates over DTLS/TLS authenticated and secured tunnels

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 950**

What is a characteristic of a Type 2 hypervisor?

- A. its main task is to manage hardware resources between different operating
- B. Problems in the base operating system can affect the entire system
- C. It is completely independent of the operating system
- D. It eliminates the need for an underlying operating system

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 951**

>>> (3 \* 5) % 2

What is the result of this Python code?

- A. 1
- B. 0
- C. 7
- D. 7.5

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

(3 \* 5) is evaluated first and the result is 15.

Then 15 % 2 means the finding of the remainder after 15 is divided by 2.

The diagram illustrates the division of 15 by 2. The divisor is 2, the dividend is 15, the quotient is 7, and the remainder is 1. The calculation is shown as 2 goes into 15 seven times (labeled 7) with a remainder of 1 (labeled 1).

The remainder is therefore 1.

**QUESTION 952**

A wireless network engineer must configure a WPA2+WPA3 policy with the Personal security type. Which action meets this requirement?

- A. Configure the CCMP256 encryption cipher.
- B. Configure the CCMP128 encryption cipher.
- C. Configure the GCMP256 encryption cipher.
- D. Configure the GCMP128 encryption cipher.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The following is extracted from a Cisco web page:

## Configuring SAE Mixed Mode (WPA2+WPA3) (GUI)

### Procedure

- Step 1 Choose **WLANS** to open the WLANS page.
- Step 2 Click the ID number of the desired WLAN to open the **WLANS > Edit** page.
- Step 3 Choose the **Security > Layer 2** tabs.
- Step 4 Choose **WPA2+WPA3** from the **Layer 2 Security** drop-down list.
- Step 5 From the **Security Type** drop-down list, choose from the following options:
  - Personal
  - Enterprise
- Step 6 In the **WPA2+WPA3 Parameters** section, choose **WPA2** and **WPA3** as the **Policy**.
- Step 7 Choose the **Encryption Cipher** from the following options:
  - **CCMP128(AES)**
  - **CCMP256** (not available for Personal security type)
  - **GCMP128** (not available for Personal security type)
  - **GCMP256** (not available for Personal security type)

### QUESTION 953

```
aaa new-model
aaa authentication login default group tacacs+ local
!
tacacs server prod
address ipv4 10.10.10.23
key cisco123
!
ip tacacs source-interface Gig 0/0
```

Which configuration must be applied for the TACACS+ server to grant access-level rights to remote users?

- A. R1(config)# aaa accounting commands 15 default start-stop group tacacs+
- B. R1(config)# aaa authorization exec default local if-authenticated
- C. R1(config)# aaa authorization exec default group tacacs+
- D. R1(config)# aaa authentication login enable

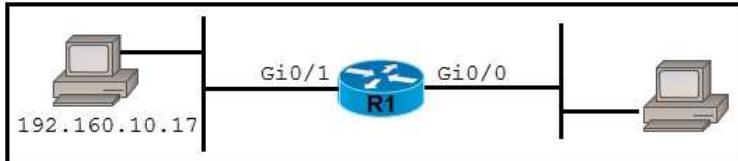
**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 954



An engineer applies this configuration to R1: ip nat inside source static 192.168.10.17 192.168.27.42

Which command set should be added to complete the configuration?

- A. R1(config)# interface GigabitEthernet 0/0
 R1(config-if)# ip nat outside
 R1(config)# interface GigabitEthernet 0/1
 R1(config-if)# ip nat inside
- B. R1(config)# interface GigabitEthernet 0/0
 R1(config-if)# ip pat outside
 R1(config)# interface GigabitEthernet 0/1
 R1(config-if)# ip pat inside
- C. R1(config)# interface GigabitEthernet 0/0
 R1(config-if)# ip pat inside
 R1(config)# interface GigabitEthernet 0/1
 R1(config-if)# ip pat outside
- D. R1(config)# interface GigabitEthernet 0/0
 R1(config-if)# ip nat inside
 R1(config)# interface GigabitEthernet 0/1
 R1(config-if)# ip nat outside

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since 192.168.10.17 is the inside local IP address, the interface connecting to this host (i.e. g0/1) should be configured as the inside interface.

#### QUESTION 955

What is a characteristic of VXLAN?

- A. It extends Layer 2 and Layer 3 overlay networks over a Layer 2 underlay
- B. It uses VTEPs to encapsulate and de-encapsulate frames
- C. It uses TCP for transport
- D. It has a 12-bit network identifier

**Correct Answer:** B

**Section:** (none)

**Explanation**

#### Explanation/Reference:

VXLAN is a technology that allows overlaying a Layer 2 (L2) network over a Layer 3 (L3) underlay with use of any IP routing protocol. It uses MAC-in-UDP Encapsulation.

VNID (Vxlan Network Identifier) is a 24-bit segment ID that defines the broadcast domain. Interchangeable with "VXLAN Segment ID". **VTEP (Virtual Tunnel Endpoint)** is the device that does the encapsulation and de-encapsulation.

#### QUESTION 956

What is a characteristic of an omnidirectional antenna?

- A. It is well suited for point-to-multipoint environments
- B. It provides the most focused and narrow beamwidth
- C. It includes dish antennas
- D. It has high gain

**Correct Answer:** A

**Section:** (none)

**Explanation**

#### Explanation/Reference:

**Table 2.** Cisco Aironet 2.4 GHz Bridge Antenna Features

|                    |  |  |
|--------------------|--|--|
|                    | <b>AIR-ANT2506</b>   | <b>AIR-ANT24120</b>  |
| <b>Description</b> | Omnidirectional mast mount   | High-gain omnidirectional mast mount   |
| <b>Application</b> | Outdoor short-range point-to-multipoint applications                               | Outdoor midrange point-to-multipoint applications                                  |
| <b>Gain</b>        | 5.2 dBi  | 12 dBi   |

#### QUESTION 957

```
1  Status Code: 200
2  Body:
3  {
4      "response": [
5          {
6              "memorySize": "3735302144",
7              "family": "Wireless Controller",
8              "role": "ACCESS",
9              "description": "Cisco Controller Wireless Version:8.5.140.0",
10             "roleSource": "AUTO",
11             "lastUpdated": "2022-08-10 13:48:02",
12             "deviceContextLevel": "Supported",
13             "softwareType": "Cisco Controller",
14             "softwareVersion": "8.5.140.0",
15             "macAddress": "ac:4a:56:6c:7c:00",
16             "collectionInterval": "Global Default",
17             "inventoryStatusDetail": "<status><general code=\"SUCCESS\"/></status>",
18             "serialNumber": "FOL25040021",
19             "lastUpdateTime": 1631281662276,
20             "hostname": "fc3504.abc.inc",
21             "tagCount": "0",
22
23             ***Output omitted***
24             "lineCardId": "",
25             "managedAtLeastOnce": true,
26             "location": null,
27             "type": "Cisco 3504 Wireless LAN Controller",
28             "managementState": "Managed",
29             "instanceUuid": "4b741b27-f7e7-4470-befc-d5168cc59502",
30             "instanceTenantId": "5e48964d4add00ca2b6487",
31             "id": "4b741b27-f7e7-4470-befc-d5168cc59502"
32         },
33     ],
34     "version": "1.0"
35 }
```

Which HTTP request produced the REST API response that was returned by Cisco DNA Center?

- A. fetch /network-device?macAddress=ac:4a:56:6c:7c:00
- B. PUT /network-device?macAddress=ac:4a:56:6c:7c:00
- C. POST /network-device?macAddress=ac:4a:56:6c:7c:00

D. GET /network-device?macAddress=ac:4a:56:6c:7c:00

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since the response include the details of a device, the corresponding request should be a GET request.

**QUESTION 958**

Which protocol is implemented to establish secure control plane adjacencies between Cisco SD-WAN nodes?

- A. IKE
- B. TLS
- C. IPsec
- D. ESP

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Control plane is secured by DTLS or TLS. Data plane is secured by IPsec.

**QUESTION 959**

Which enhancement was introduced in NTP version 4?

- A. support for asymmetric key authentication
- B. reduced time state refresh interval
- C. support for IPv6
- D. support for symmetric mode

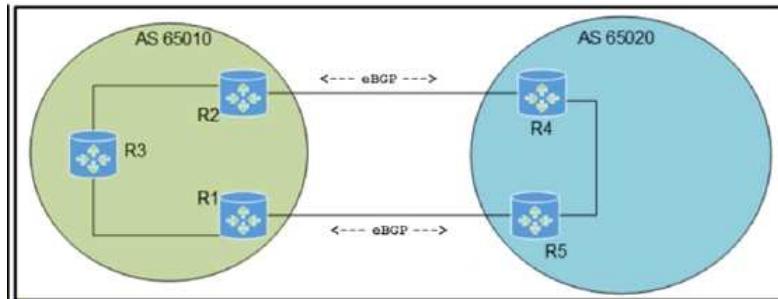
**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 960**



Which configuration must be applied to ensure that the preferred path for traffic from AS 65010 toward AS 65020 uses the R2 to R4 path?

- A. R4(config)# router bgp 65020  
R4(config-router)# bgp default local-preference 300  
R5(config)# router bgp 65020  
R5(config-router)# bgp default local-preference 200
- B. R2(config)# router bgp 65010  
R2(config-router)# bgp default local-preference 300  
R1(config)# router bgp 65010  
R1(config-router)# bgp default local-preference 200
- C. R2(config)# router bgp 65010  
R2(config-router)# bgp default local-preference 200  
R1(config)# router bgp 65010  
R1(config-router)# bgp default local-preference 300
- D. R4(config)# router bgp 65020  
R4(config-router)# bgp default local-preference 200  
R5(config)# router bgp 65020  
R5(config-router)# bgp default local-preference 300

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 961**

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 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
C. 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
D. ip access-list standard nms
  permit 10.15.2.19 0.0.0.0
  snmp-server view ro iso included
  snmp-server view ro ifEntry included
  snmp-server group nms v3 priv read ro access nms
    snmp-server user user1 nms v3 auth sha Password1 pri aes 256 Password123

```

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

```
R1(config)#snmp-server user user1 nms v3 auth sha Password1 priv ?
```

```
  3des  Use 168 bit 3DES algorithm for encryption
  aes   Use AES algorithm for encryption
  des   Use 56 bit DES algorithm for encryption
```

```
R1(config)#snmp-server user user1 nms v3 auth sha Password1 priv aes ?
```

```
  128  Use 128 bit AES algorithm for encryption
  192  Use 192 bit AES algorithm for encryption
  256  Use 256 bit AES algorithm for encryption
```

Among the configurable values, "aes" and "256" is the most secure algorithm.

Moreover, setting up "read" view should be enough for monitoring.

**QUESTION 962**

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

**Select and Place:**

```

import [REDACTED]

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 = [REDACTED] (data)

print([REDACTED])

```

|             |
|-------------|
| model       |
| json.loads  |
| json        |
| json_string |
| json.dumps  |

**Correct Answer:**

```

import json

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 = json.dumps (data)

print( json_string )

```

|            |
|------------|
| model      |
| json.loads |
|            |
|            |
|            |

**Section: Selected Explanation**

**Explanation/Reference:**

**QUESTION 963**

Which encoding is used to protect a username and login with RESTful API basic authentication?

- A. MD5
- B. SHA-1
- C. Type-7
- D. Base64

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Basic Authentication simply sends a username and password along with every request in the Authorization header. The header value begins with the word "Basic" followed by a space and then the credentials. The credentials are the username and password concatenated together with a colon (:) character in between and then Base64 encoded.

**QUESTION 964**

Which configuration creates a CoPP policy that provides unlimited SSH access from client 10.0.0.5 and denies access from all other SSH clients?

- A. !

```

access-list 100 permit tcp host 10.0.0.5 any eq 22
access-list 100 deny tcp any any eq 22
!
class-map match-all telnet_copp
match access-group 100
!
policy-map CoPP
class telnet_copp
police 8000
!
control-plane
service-policy input CoPP
!
```
- B. !

```

access-list 100 permit tcp host 10.0.0.5 any eq 22
access-list 100 deny tcp any any eq 22
!
class-map match-all telnet_copp
match access-group 100
!
policy-map CoPP
class telnet_copp
drop
!
control-plane
service-policy input CoPP
!
```
- C. !

```

access-list 100 deny tcp host 10.0.0.5 any eq 22
access-list 100 permit tcp any any eq 22
!
class-map match-all telnet_copp
match access-group 100
!
```

```

policy-map CoPP
class telnet_copp
drop
!
control-plane
service-policy input CoPP
!
D. access-list 100 permit tcp any any eq 22
access-list 100 deny tcp host 10.0.0.5 any eq 22
!
class-map match-all telnet_copp
match access-group 100
!
policy-map CoPP
class telnet_copp
police 8000
!
control-plane
service-policy input CoPP
!

```

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In order to provide unlimited SSH access from client 10.0.0.5, you should not limit its traffic with "police". Moreover, you also need to drop SSH access from other devices. Hence the correct answer is to configure an access-list that matches SSH traffic from all other clients (i.e. except 10.0.0.5) and then configure a policy in CoPP to drop traffic matching this access-list.

**QUESTION 965**

Drag and drop the automation characteristics from the left onto the corresponding tools on the right. Not all options are used  
What are the suitable characteristics for Puppet? (Choose two)

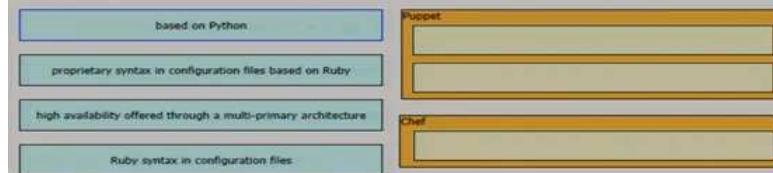
- A. based on python
- B. proprietary syntax in configuration files based on Ruby
- C. high availability offered through a multi-primary architecture
- D. Ruby syntax in configuration files

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



Puppet is a software configuration management tool written in Ruby. It has its own declarative language to describe system configuration.

**QUESTION 966**

Drag and drop the automation characteristics from the left onto the corresponding tools on the right. Not all options are used  
What is the suitable characteristic for Chef?

- A. based on python
- B. proprietary syntax in configuration files based on Ruby
- C. high availability offered through a multi-primary architecture
- D. Ruby syntax in configuration files

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**



Chef uses a pure-Ruby domain-specific language (DSL) for writing system configuration "recipes".

**QUESTION 967**

Which two new security capabilities are introduced by using a next-generation firewall at the Internet edge? (Choose two.)

- A. stateful packet inspection
- B. integrated intrusion prevention
- C. NAT
- D. VPN
- E. application-level inspection

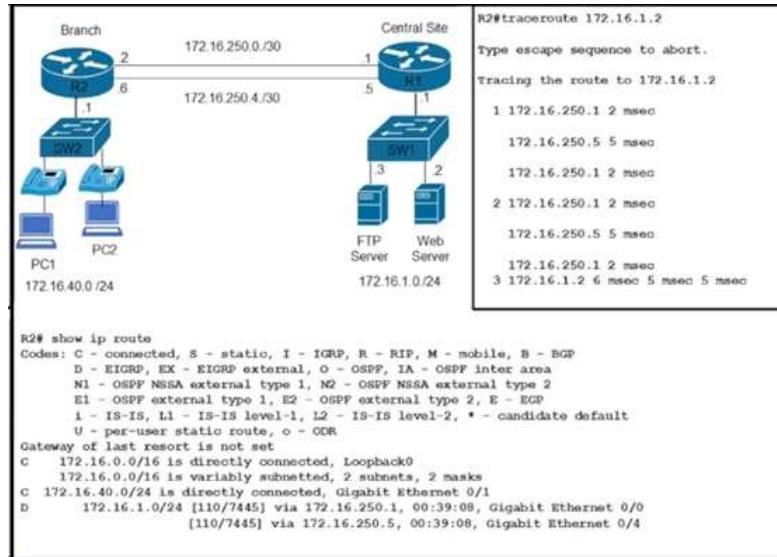
**Correct Answer:** BE

**Section:** Selected

## Explanation

Explanation/Reference:

### QUESTION 968



Clients are reporting an issue with the voice traffic from the branch site to the central site. What is the cause of this issue?

- A. There is a routing loop on the network
- B. There is a high delay on the WAN links
- C. Traffic is load-balancing over both links, causing packets to arrive out of order
- D. The voice traffic is using the link with less available bandwidth

Correct Answer: C

Section: (none)

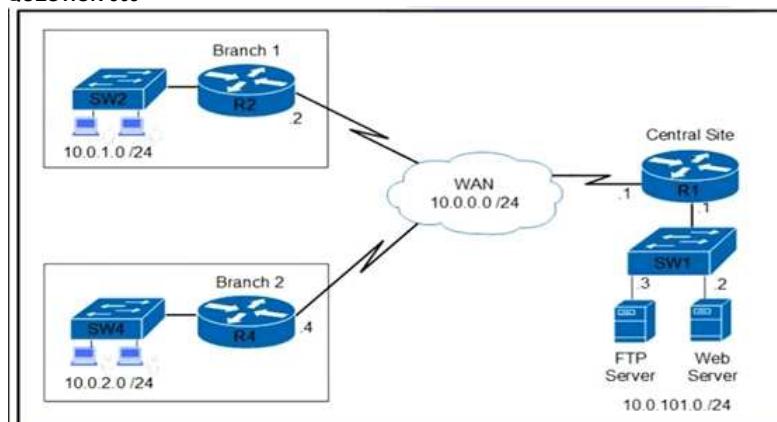
Explanation

Explanation/Reference:

Since hop 1 shows more than 1 IP address, packets are traveling different paths to reach the destination.

Although hop 1 and hop 2 are showing the same IP addresses, since the packets can finally reach the destination 172.16.1.2 in hop 3, there should be no routing loop.

### QUESTION 969



Which two commands are required on router R1 to block FTP and allow all other traffic from the Branch 2 network? (Choose two.)

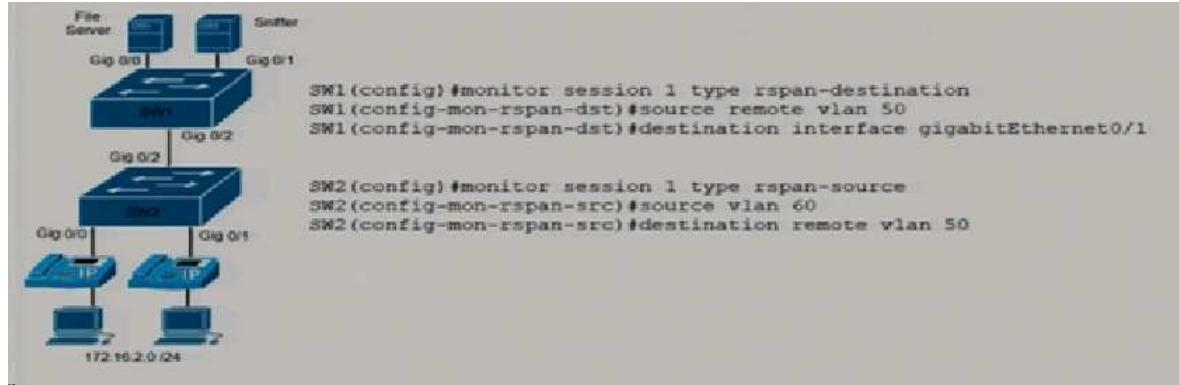
- A. access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp  
access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp-data  
access-list 101 permit ip any any
- B. access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp-data  
access-list 101 permit ip any any
- C. interface GigabitEthernet0/0  
ip address 10.0.0.1 255.255.255.0  
ip access-group 101 out
- D. access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp  
access-list 101 permit ip any any
- E. interface GigabitEthernet0/0  
ip address 10.0.0.1 255.255.255.0  
ip access-group 101 in

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 970**

An engineer must send the 172.16.2.0 /24 user traffic to a packet capture tool to troubleshoot an issue. Which action completes the configuration?

- A. Define the remote span VLAN on SW1 and SW2
- B. Encrypt the traffic between the users and the monitoring servers
- C. Enable the Cisco Discovery Protocol on the server interfaces
- D. Disable the spanning tree protocol on the monitoring server VLAN

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The remote VLAN i.e. VLAN 50 must be created in both switches.

**QUESTION 971**

Drag and drop the Cisco DNA Center northbound API characteristics from the left to the right. Not all options are used. Select suitable characteristics for DNA Center northbound API. (Choose three)

- A. referred to as Intent API
- B. multivendor focus
- C. uses JSON exclusively
- D. RESTful API based on HTTP methods
- E. supports NETCONF, SSH, SNMP, and others

**Correct Answer:** ACD

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**Answer Area**

|   |                           |
|---|---------------------------|
| referred to as Intent API               | DNA Center northbound API |
| multivendor focus                       |                           |
| uses JSON exclusively                   |                           |
| RESTful API based on HTTP methods       |                           |
| supports NETCONF, SSH, SNMP, and others |                           |

**QUESTION 972**



```
R1# debug vrrp error

00:15:30: %IP-5-DUPADDR: Duplicate address 10.18.0.2 on Ethernet1/0, sourced
by 0000.5e00.0101

June 12 8:41:54.447: VRRP: Grp 1 Advertisement Primary address 10.18.0.2
different from ours 10.18.0.1

June 12 8:41:57.443: VRRP: Grp 1 Advertisement Primary address 10.18.0.2
different from ours 10.18.0.1

June 12 8:42:00.443: VRRP: Grp 1 Advertisement Primary address 10.18.0.2
different from ours 10.18.0.1
```

R1 and R2 are on the same VLAN. VRRP is configured between the two routers. What is the cause of the VRRP error?

- A. R1 is configured with VIP 10.18.0.2 on VRRP group 1 and R2 is configured with VIP 10.18.0.1 on VRRP group 1.
- B. R1 is configured with VIP 10.18.0.2 on VRRP group 1 and R2 is configured with VIP 10.18.0.2 on VRRP group 1.
- C. R1 is configured with VIP 10.18.0.1 on VRRP group 1 and R2 is configured with VIP 10.18.0.2 on VRRP group 0.
- D. R1 is configured with VIP 10.18.0.1 on VRRP group 1 and R2 is configured with VIP 10.18.0.2 on VRRP group 1.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

From R1's debug output, it is receiving an advertisement for VRRP group 1 with VIP address 10.18.0.2. However, the debug show that VRRP group 1 in R1 is configured with the VIP address 10.18.0.1.

**QUESTION 973**

An engineer must configure HSRP on two switches. The HSRP virtual MAC address must be the burned-in address of the interface. If the primary router fails, it must regain active status 10 seconds after returning to operational status. Which two configurations must be applied? (Choose two)

- A. Configure standby use-bia on the interface level
- B. Configure standby follow hw-address in the global configuration
- C. Configure standby 1 preempt delay minimum 10 on the interface level
- D. Configure standby 1 preempt delay reload 10 on the interface level
- E. Configure standby 1 preempt delay sync 10 in the global configuration

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

```
R1(config-if)#standby ?
...
follow      Name of HSRP group to follow
use-bia    HSRP uses interface's burned in address
...
R1(config-if)#
For delay:
minimum means the delay after each time an interface goes down and up again.
reload means the delay after an interface goes up when there is a reload.
```

Since the question says about "router fails", it seems that `reload` should be a better answer.

**QUESTION 974**

Which capability does a distributed virtual switch have?

- A. to use advanced IPsec encryption algorithms
- B. to provide centralized management for virtual switches
- C. to run dynamic routing protocols
- D. to use floating static routes

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

A distributed virtual switch allows you to easily manage the virtual switches and also provide a consistency configuration for the switches among different hypervisors.

**QUESTION 975**

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

For "marking", it set the IP Precedence bits so that other routers can prioritize the traffic.

For "classification", a router can read the IP Precedence bits in the packets so that it can differentiate the traffic and handle the traffic with different prioritization.

Both A and D can be the answers. However, since the word "uses" is mentioned in the question, "classification" seems to be better.

**QUESTION 976**

Which function is performed by vSmart in the Cisco SD-WAN architecture?

- A. execution of localized policies
- B. facilitation of NAT detection and traversal
- C. redistribution between OMP and other routing protocols
- D. distribution of centralized policies

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Remarks:**

However, there are two types of centralized policies:

- Centralized control policy applies to the network-wide routing of traffic by affecting the information that is stored in the Cisco vSmart Controller's route table and that is advertised to the Cisco vEdge devices. The centralized control policy configuration itself remains on the Cisco vSmart Controller and is never pushed to local devices.
- Centralized data policy applies to the flow of data traffic throughout the VPNs in the overlay network. These policies are pushed to the selected Cisco vEdge devices.

**QUESTION 977**

A client requests a wireless solution for remote branch offices to eliminate the need for a local controller at each branch. The branch users require local termination in a specific VLAN for local internet breakout. Which solution must be deployed?

- A. central switched
- B. FlexConnect local switching
- C. auto-anchor mobility
- D. asymmetric tunneling

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 978**

```
>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>
```

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. There is a loop in the path to the server.
- C. The gateway cannot translate the server domain name.
- D. The server is out of service.

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 979**

Which component does Cisco Threat Defense use to measure bandwidth, application performance, and utilization?

- A. TrustSec
- B. Advanced Malware Protection for Endpoints
- C. NetFlow
- D. Cisco Umbrella

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 980**

Which two prerequisites must be met before Cisco DNA Center can provision device? (Choose two.)

- A. Cisco DNA Center must have the software image for the provisioned device in its image repository.
- B. The provisioned device must be put into bootloader mode.
- C. The provisioned device must be configured with CLI and SNMP credentials that are known to Cisco DNA Center.
- D. Cisco DNA Center must have IP connectivity to the provisioned device.
- E. The provisioned device must recognize Cisco DNA Center as its LLDP neighbor.

**Correct Answer:** CD  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 981**

Drag and drop the NTP elements from the left onto the correct descriptions on the right.

**Select and Place:**

**Answer Area**

NTP associations	network device listening for NTP broadcast packets
broadcast client command	NTP servers propagating NTP broadcast packets
NTP access groups	uses MD5 Message Digest Algorithm
NTP authentication	used to permit or deny access privileges to a subnet or host

**Correct Answer:**

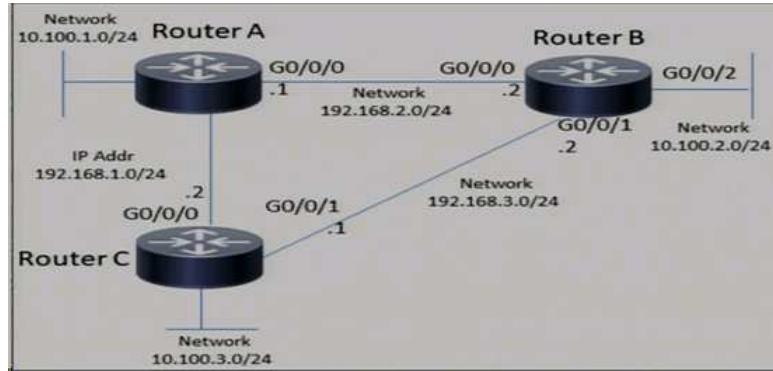
**Answer Area**

	broadcast client command
	NTP associations
	NTP authentication
	NTP access groups

**Section:** (none)  
**Explanation**

**Explanation/Reference:**

You can check whether a server is sending NTP broadcast and can be received by a client through the output of the command "sh ntp associations".

**QUESTION 982**

A network engineer must block Telnet traffic from hosts in the range of 10.100.2.248 to 10.100.2.255 to the network 10.100.3.0 and permit everything else. Which configuration must the engineer apply?

- A. RouterB(config)# access-list 101 deny icmp 10.100.2.0 0.0.0.248 10.100.2.0 0.0.0.248  
RouterB(config)# access-list 101 permit any any  
RouterB(config)# int g0/0/2  
RouterB(config-if)# ip access-group 101 in
- B. RouterB(config)# access-list 101 deny tcp 10.100.2.0 0.0.0.248 10.100.3.0 0.0.0.255 eq 23  
RouterB(config)# access-list 101 permit any any  
RouterB(config)# int g0/0/2  
RouterB(config-if)# ip access-group 101 in
- C. RouterB(config)# access-list 101 deny tcp 10.100.2.0 0.0.0.248 10.100.3.0 0.0.0.255 eq 22  
RouterB(config)# access-list 101 permit any any  
RouterB(config)# int g0/0/2  
RouterB(config-if)# ip access-group 101 in
- D. RouterB(config)# access-list 101 permit tcp 10.100.2.0 0.0.0.252 10.100.3.0 0.0.0.255  
RouterB(config)# int g0/0/2  
RouterB(config-if)# ip access-group 101 in

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Only one choice denies the traffic for TCP port 23 which is the port used by telnet.

Remarks :

There is something wrong with the choices since in order to block 10.100.2.248 to 10.100.2.255, the correct source address and its wildcard mask should be 10.100.2.248 0.0.0.7

**QUESTION 983**

When does Cisco DNA Center make changes to a device?

- A. when the device credentials are added
- B. when the network device is assigned to the site and device controllability is turned on
- C. when the network device is discovered and device controllability is turned on
- D. when a NETCONF port has been configured

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Other than the choice "when the network device is assigned to the site ...", the choice "when network device is discovered ..." can also be the answer.

Remarks:

Device controllability is a system-level process on Cisco DNA Center that enforces state synchronization for some device-layer features. Its purpose is to aid in the deployment of network settings that Cisco DNA Center needs to manage devices. Changes are made on network devices when running discovery, when adding a device to inventory, or when assigning a device to a site.

**QUESTION 984**

```
Router#show running-config | section line vty
line vty 0 4
login local
line vty 5 15
login local
!
Router#show running-config | include username
username cisco secret 5 $1$cM67$v7NQK0g2BGit77x88U1/00
```

Which action automatically enables privilege exec mode when logging in via SSH?

- A. Configure a password under the line configuration.
- B. Configure the enable secret to be the same as the secret for user "Cisco".
- C. Configure privilege level 15 under the line configuration.
- D. Configure user "cisco" with privilege level 15.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Although setting up privilege level 15 for the user "cisco" also allows the user to obtain privilege exec mode after login, the question does not specify that privilege level 15 should be granted only to the user "cisco". Therefore, configuring the setting in line configuration seems to be a better answer.

**QUESTION 985**

Which Cisco SD-WAN component authenticates the routers and the vSmart controllers?

- A. vEdge
- B. vManage NMS
- C. vAnalytics
- D. vBond orchestrator

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Cisco SD-WAN Validator (formerly known as vBond) is a software module that authenticates the Cisco SD-WAN Controllers (formerly known as vSmart) and the vEdge routers in the overlay network and coordinates connectivity between them.

**QUESTION 986**

Drag and drop the snippets onto the blanks within the code to construct a script that brings up the failover Ethernet port if the primary port goes down and also shuts down the failover port when the primary returns to service. Not all options are used.

**Select and Place:**

**Answer Area**

```
event manager applet SRV-1-Up
  event syslog pattern "Line protocol on Interface GigabitEthernet4/0/9, changed state to 
    action 1.0 cli command "enable"
    action 2.0 cli command "configure terminal"
    action 3.0 cli command "Interface GigabitEthernet3/0/10"
    action 4.0 cli command "no shutdown"
    action 5.0 cli command "end"

event manager applet SRV-1-Down
  event syslog pattern "Line protocol on Interface  , changed state to up"
    action 1.0 cli command "enable"
    action 2.0 cli command "configure terminal"
    action 3.0 cli command "Interface GigabitEthernet3/0/10"
    action 4.0 cli command " "
    action 5.0 cli command "end"
```

**Correct Answer:**

**Answer Area**

```
event manager applet SRV-1-Up
  event syslog pattern "Line protocol on Interface GigabitEthernet4/0/9, changed state to  Down"
    action 1.0 cli command "enable"
    action 2.0 cli command "configure terminal"
    action 3.0 cli command "Interface GigabitEthernet3/0/10"
    action 4.0 cli command "no shutdown"
    action 5.0 cli command "end"

event manager applet SRV-1-Down
  event syslog pattern "Line protocol on Interface  GigabitEthernet4/0/9 , changed state to up"
    action 1.0 cli command "enable"
    action 2.0 cli command "configure terminal"
    action 3.0 cli command "Interface GigabitEthernet3/0/10"
    action 4.0 cli command " Shutdown"
    action 5.0 cli command "end"
```

**Section: Selected**

**Explanation**

**Explanation/Reference:**

**QUESTION 987**

```

class-map match-any dscp-1
match ip dscp 1

policy-map set-dscp-63
class dscp-1
set dscp 63

interface GigabitEthernet0/0/0
  mls qos trust dscp
  service-policy input set-dscp-63

```

What is the outcome of applying the service policy "set-dscp-63" to switch port Gig0/0/0?

- A. DSCP 1 marked traffic will be re-marked to 63 and all other DSCP values will be honored
- B. None. The service-policy configuration must be applied in the outbound direction
- C. DSCP 1 marked traffic will be re-marked to 63 and all other DSCP values will be ignored
- D. DSCP 1 marked traffic will be ignored and DSCP 63 marked traffic will be honored

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 988

What is the architectural difference between the MAC address table and TCAM?

- A. TCAM entries consist of VLAN, port ID and source MAC Address, and MAC address table entries consist of source MAC address and port ID
- B. TCAM entries are populated using the ARP table, and the MAC address table is populated dynamically from outgoing framesTCAM entries are stored for 600 seconds, and MAC address table entries are kept for 200 seconds
- C. TCAM entries are stored for 600 seconds, and MAC address table entries are kept for 200 seconds
- D. TCAM entries are composed of value, mask, and result, and MAC address table entries are composed of value and results

**Correct Answer:** D

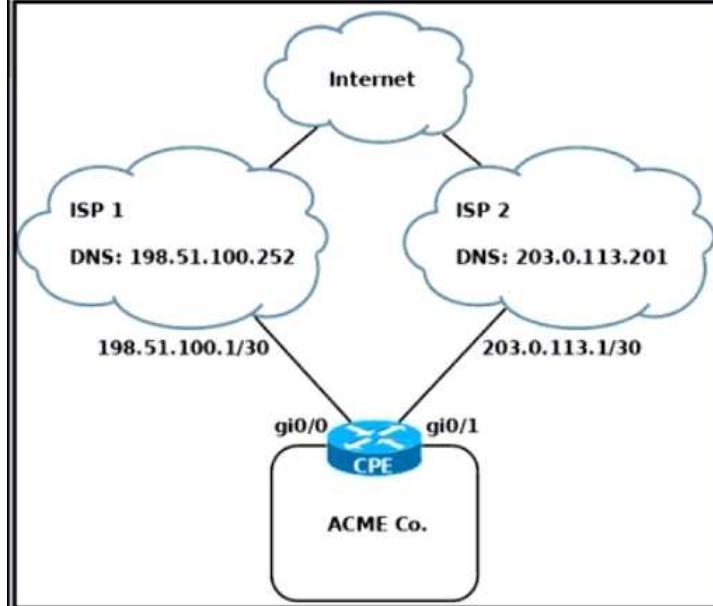
**Section:** (none)

**Explanation**

**Explanation/Reference:**

TCAM is used for storing routing table since TCAM provides three results: 0, 1, and "don't care." The term VMR (Value, Mask and Result) refers to the format of entries in TCAM. The "value" in VMR refers to the pattern that is to be matched; examples include IP addresses, protocol ports, DSCP values, and so on.

#### QUESTION 989



An engineer must verify the operational status of ISP 1 by testing the IP reachability of the ISP1 DNS server every 10 seconds. If the DNS server is not reachable from the CPE through the Gi0/0 interface, then the test should fail. Which two configuration sets must be used to accomplish this task? (Choose two.)

- A. ip route 0.0.0.0 0.0.0.0 198.51.100.1  
ip route 0.0.0.0 0.0.0.0 203.0.113.1
- B. ip route 0.0.0.0 255.255.255.255 198.51.100.1  
ip route 0.0.0.0 255.255.255.255 203.0.113.1
- C. ip route 198.51.100.252 255.255.255.255 198.51.100.1
- D. ip sla 1  
icmp-echo 198.51.100.252  
frequency 10  
ip sla schedule 1 life forever start-time now
- E. ip sla 1  
dns www.cisco.com name-server 198.51.100.252  
frequency 10  
ip sla schedule 1 life forever start-time now

**Correct Answer:** CD

**Section:** (none)

## Explanation

### Explanation/Reference:

For this the question, you need:

- a route that will send traffic to 198.51.100.252 through ISP 1 i.e. 198.51.100.1 only.
- a IP SLA that test reachability to 198.51.100.252. Since it is not testing the DNS service, icmp-echo should be used.

## QUESTION 990

An engineer is implementing a new SSID on a Cisco Catalyst 9800 Series WLC that must be broadcast on 6 GHz radios. Users will be required to use EAP-TLS to authenticate. Which wireless Layer 2 security method is required?

- A. WPA2 Enterprise
- B. WPA2 Personal
- C. WPA3 Enterprise
- D. WPA3 Personal

**Correct Answer:** C

**Section:** (none)

**Explanation**

### Explanation/Reference:

In 6GHz (Wi-Fi 6E) you can only configure following security methods

- WPA3 (Personal or Enterprise)

- Enhanced Open or OWE

Moreover, EAP-TLS is for Enterprise only.

## QUESTION 991

```
import requests

### The authentication part is omitted for brevity purposes

URL = "https://dnac/dna/intent/api/v1/topology/vlan/vlan-names"
VlanNames = requests.get(URL, headers=Header).json()
print(VlanNames)

[{"response": ["Vlan1", "Vlan3002", "Vlan3003", "Vlan1023", "Vlan2046", "Vlan3009", "Vlan3999"], "version": "1.0"}]
```

How should the programmer access the list of VLANs that were received via the API call?

- A. VlanNames['response']
- B. VlanNames[0]
- C. VlanNames['Vlan1']
- D. list(VlanNames)

**Correct Answer:** A

**Section:** Selected

**Explanation**

### Explanation/Reference:

## QUESTION 992

```
count = 8
while count > 4 :
    print(count)
    count -= 1
```

What is output by this code?

- A. 8 7 6 5
- B. 4 5 6 7
- C. -4 -5 -6 -7
- D. -1 -2 -3 -4

**Correct Answer:** A

**Section:** (none)

**Explanation**

### Explanation/Reference:

## QUESTION 993

What is a difference between OSPF and EIGRP?

- A. OSPF uses the DUAL algorithm. EIGRP uses the SPF algorithm
- B. OSPF is an advanced distance vector protocol. EIGRP is a link-state protocol
- C. OSPF uses an administrative distance of 110. EIGRP uses an administrative distance of 170
- D. OSPF is a hybrid routing protocol. EIGRP is a link-state routing protocol

**Correct Answer:** C

**Section:** (none)

**Explanation**

### Explanation/Reference:

Remarks:

Although the AD of a normal EIGRP route is 90, an external EIGRP route has an AD of 170.

## QUESTION 994

When voice services are deployed over a wireless environment, which service must be disabled to ensure the quality of calls?

- A. priority queuing
- B. dynamic transmit power control
- C. aggressive load balancing
- D. Fastlane

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Enabling aggressive load balancing on the controller allows lightweight access points to load balance wireless clients across access points. You can enable aggressive load balancing using the controller. You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients (such as time-sensitive voice clients).

**QUESTION 995**

What are two characteristics of a directional antenna? (Choose two.)

- A. commonly used to cover large areas
- B. low gain
- C. provides the most focused and narrow beam-width
- D. receive signals equally from all directions
- E. high gain

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 996**

Using the EIRP formula, what parameter is subtracted to determine the EIRP value?

- A. transmitter power
- B. antenna cable loss
- C. antenna gain
- D. signal-to-noise ratio

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The formula for EIRP (Effective Isotropic Radiated Power) is:  
EIRP = TxPower (dBm) - Cable Loss (dB) + Antenna Gain (dBi)

**QUESTION 997**

What is a characteristic of a Type 1 hypervisor?

- A. It is referred to as a hosted hypervisor
- B. It is completely independent of the operating system
- C. Problems in the base operating system can affect the entire system
- D. It is installed on an operating system and supports other operating systems above it.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 998**

```
#!/usr/bin/python3

import requests

requests.urllib3.disable_warnings()

AuthURL="https://dna-center/dna/system/api/v1/auth/token"
USER="admin"
PASSWORD="SomePassword"

Response = requests.post(AuthURL, auth=(USER, PASSWORD), verify=False)
if Response.status_code < 200 or Response.status_code > 299:
    print(f"Aborting: received status code {Response.status_code}")
    exit()

<...removed...>

admin@linux:~/fetch.py
Aborting: received status code 401
```

An administrator writes a script to fetch the list of devices that are registered with Cisco DNA Center. Why does the execution abort?

- A. The TLS certificate of DNA Center is invalid
- B. The username or the password is incorrect
- C. The "dna-center" hostname cannot be resolved to an IP address
- D. The authentication URL is incorrect

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

HTTP status code 401 means Unauthorized

**QUESTION 999**

```
switch > enable
switch # configure terminal
switch(config)# interface GigabitEthernet 1/10
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 10,20,30
switch(config-if)# exit
switch (config)# monitor session 1 type erspan-source
switch(config-mon-erspan-src)# description source1
switch(config-mon-erspan-src)# source vlan 10
switch(config-mon-erspan-src)# source vlan 20
switch(config-mon-erspan-src)# filter vlan 30
switch(config-mon-erspan-src)# destination
switch(config-mon-erspan-src-dst)# erspan-id 100
switch(config-mon-erspan-src-dst)# origin ip address 10.1.0.1
switch(config-mon-erspan-src-dst)# ip prec 5
switch(config-mon-erspan-src-dst)# ip ttl 32
switch(config-mon-erspan-src-dst)# mtu 1500
switch(config-mon-erspan-src-dst)# ip address 10.10.0.1
switch(config-mon-erspan-src-dst)# vrf 1
switch(config-mon-erspan-src-dst)# no shutdown
switch(config-mon-erspan-src-dst)# end
```

An engineer configures the trunk and proceeds to configure an ESPAN session to monitor VLANs 10, 20, and 30. Which command must be added to complete this configuration?

- A. Device(config-mon-erspan-src-dst)# no vrf 1
- B. Device(config-mon-erspan-src)# no filter vlan 30
- C. Device(config-mon-erspan-src-dst)# mtu 1460
- D. Device(config-mon-erspan-src-dst)# erspan-id 6

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since VLAN 30 has to be monitored, it should not be filtered.

Moreover, you cannot include source VLANs and filter VLANs in the same session.

**QUESTION 1000**

What is contained in the VXLAN header?

- A. VXLAN network identifier
- B. source and destination RLOC ID
- C. endpoint ID
- D. original Layer 2 VLAN ID

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1001**

What is a characteristic of a type 2 hypervisor?

- A. Referred to as bare-metal
- B. Quick deployment
- C. Complicated deployment
- D. Ideal for data center

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1002**

Which two mechanisms are used with OAuth 2.0 for enhanced validation? (choose two)

- A. Request management
- B. Custom headers
- C. Accounting
- D. Authorization
- E. Authentication

**Correct Answer:** DE

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1003**

```
for x in range(5):  
    print(x)
```

What is output by this code?

- A. 0 5
- B. 0 1 2 3 4 5
- C. 0 1 2 3 4
- D. (0,5)

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

The number 5 in “range( )” is the ending number. Without specifying a starting number, the default 0 will be used. Note that the ending number is exclusive i.e. the range will start at 0 and ends after 4.

**QUESTION 1004**

Which two methods are used to assign security group tags to the user in a Cisco TrustSec. architecture? (Choose two.)

- A. web authentication
- B. IEEE 802.1x
- C. DHCP
- D. modular QoS
- E. policy routing

**Correct Answer:** AB

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1005**

Which action is a LISP ITR responsible for?

- A. Forwarding user data traffic
- B. Responding to map-request messages
- C. Finding EID-to-RLOC mappings
- D. Accepting registration requests from ETRs

**Correct Answer:** C

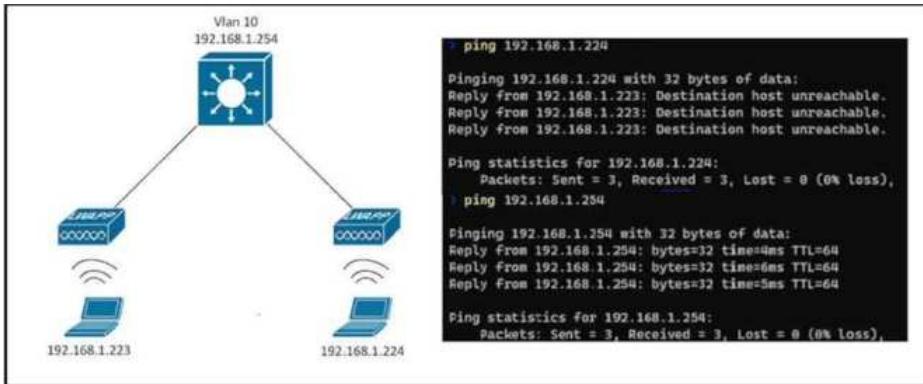
**Section:** (none)

**Explanation**

**Explanation/Reference:**

Ingress Tunnel Router (ITR) is the router which encapsulates IP packet through the tunnel and create LISP packet. ITR is responsible to find EID to RLOC mappings.

**QUESTION 1006**



An SSID is configured and both clients can reach their gateways on the Layer 3 switch, but they cannot communicate with each other. Which action resolves this issue?

- A. Set the WMM Policy to Allowed
- B. Set the P2P Blocking Action to Disabled
- C. Set the WMM Policy to Required
- D. Set the P2P Blocking Action to Forward-UpStream

**Correct Answer: B**

Section: (none)

Explanation

Explanation/Reference:

#### QUESTION 1007

Which virtualization component creates VMs and performs hardware abstraction that allows multiple VMs to run at the same time?

- A. Docker
- B. Hypervisor
- C. rkt
- D. container

**Correct Answer: B**

Section: (none)

Explanation

Explanation/Reference:

#### QUESTION 1008

Drag and drop the characteristics from the left onto the routing protocols they describe on the right.  
What are the suitable characteristics for EIGRP? (choose three)

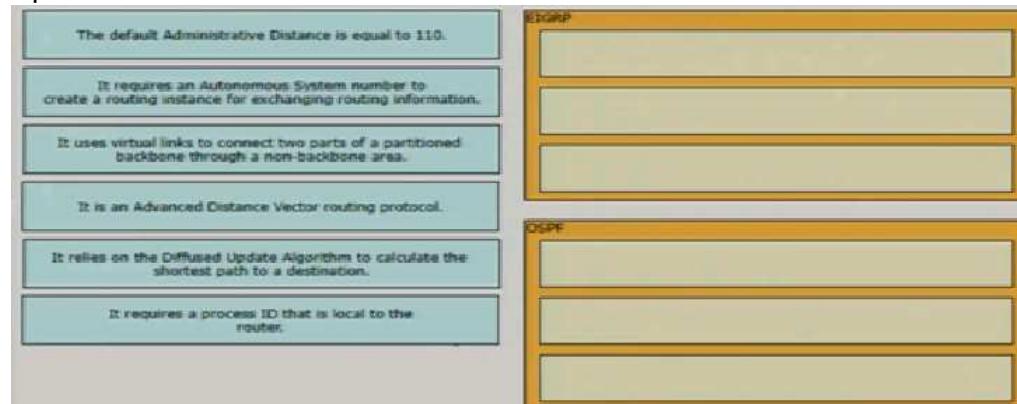
- A. The default Administrative Distance is equal to 110
- B. It requires an Autonomous System number to create a routing instance for exchanging routing information
- C. It uses virtual links to connect two parts of a partitioned backbone through a non-backbone area
- D. It is an Advanced Distance Vector routing protocol
- E. It relies on the Diffused Update Algorithm to calculate the shortest path to a destination
- F. It requires a process ID that is local to the router

**Correct Answer: BDE**

Section: (none)

Explanation

Explanation/Reference:



#### QUESTION 1009

Drag and drop the characteristics from the left onto the routing protocols they describe on the right.  
What are the suitable characteristics for OSPF? (choose three)

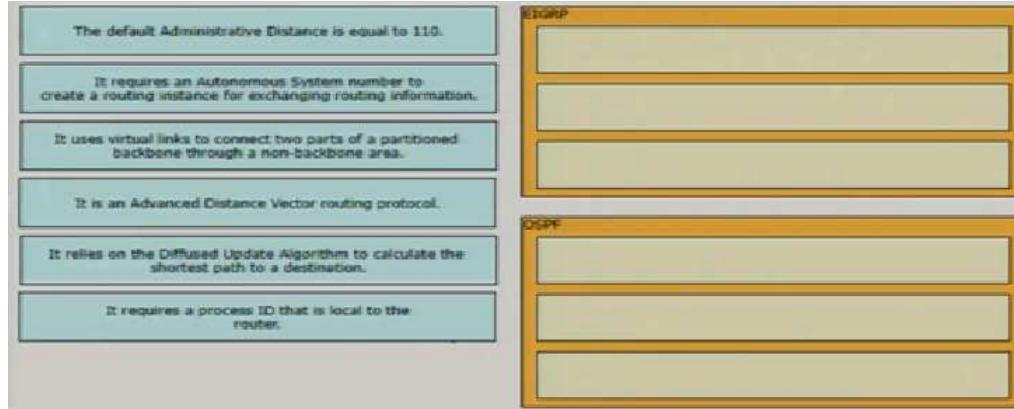
- A. The default Administrative Distance is equal to 110
- B. It requires an Autonomous System number to create a routing instance for exchanging routing information
- C. It uses virtual links to connect two parts of a partitioned backbone through a non-backbone area
- D. It is an Advanced Distance Vector routing protocol
- E. It relies on the Diffused Update Algorithm to calculate the shortest path to a destination
- F. It requires a process ID that is local to the router

**Correct Answer:** ACF

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 1010

Which resource must a hypervisor make available to the virtual machines?

- A. Bandwidth
- B. IP address
- C. Processor
- D. Secure access

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 1011

Which two security mechanisms are used by Cisco Threat Defense to gain visibility into the most dangerous cyber threats? (Choose two)

- A. VLAN segmentation
- B. Traffic Telemetry
- C. Dynamic enforce policy
- D. Virtual private networks
- E. File reputation

**Correct Answer:** BE

**Section:** Selected

**Explanation**

**Explanation/Reference:**

#### QUESTION 1012

Customer requires their wireless data traffic to egress at the switch port of the access point. Which access point mode supports this?

- A. Monitor
- B. Sniffer
- C. FlexConnect
- D. Bridge

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

#### QUESTION 1013

Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.  
What are the suitable characteristics for Ansible? (Choose two)

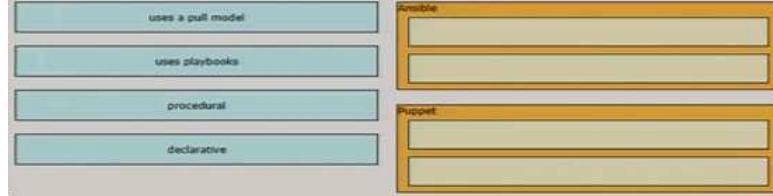
- A. uses a pull model
- B. uses playbooks
- C. procedural
- D. declarative

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 1014**

Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.  
What are the suitable characteristics for Puppet? (Choose two)

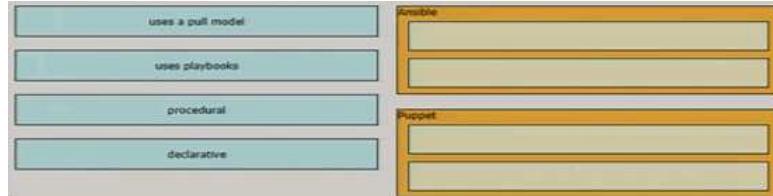
- A. uses a pull model
- B. uses playbooks
- C. procedural
- D. declarative

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 1015**

Drag and drop the automation characteristics from the left onto the corresponding tools on the right.  
What are the suitable characteristics for Ansible? (Choose three)

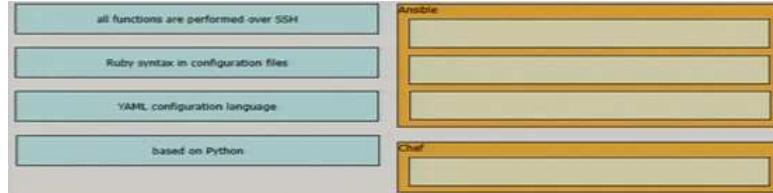
- A. All functions are performed over SSH
- B. Ruby syntax in configuration files
- C. YAML configuration language
- D. based on Python

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 1016**

Drag and drop the automation characteristics from the left onto the corresponding tools on the right.  
What is the suitable characteristic for Chef? (Choose one)

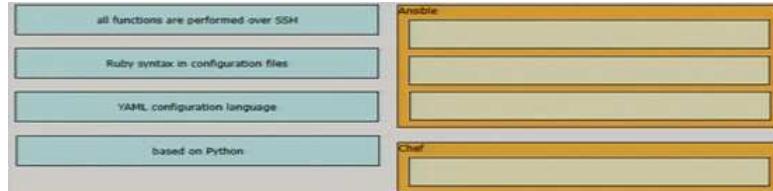
- A. All functions are performed over SSH
- B. Ruby syntax in configuration files
- C. YAML configuration language
- D. based on Python

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 1017**

```

flow record v4Talkers
match ipv4 source address
match ipv4 destination address
collect counter bytes long
!
flow record v6Talkers
match ipv6 source address
match ipv6 destination address
collect counter bytes long
!
flow monitor v4Talkers
record v4Talkers
!
flow monitor v6Talkers
record v6Talkers

```

An administrator must collect basic statistics about the approximate amount of IPv4 and IPv6 flows entering Gi0/0 using NetFlow. However the administrator is concerned that NetFlow processing during periods of high utilization on Gi0/0 will overwhelm the router CPU. Which configuration minimizes CPU impact and keeps the data flows across Gi0/0 intact?

- A. interface Gi0/0
 

```

no ip route-cache
ip flow monitor v4Talkers
ipv6 flow monitor v6Talkers
      
```
- B. interface Gi0/0
 

```

load-interval 600
ip flow monitor v4Talkers
ipv6 flow monitor v6Talkers
      
```
- C. sampler R-1-1024
 

```

mode random 1 out-of 1024
!
interface Gi0/0
ip flow monitor v4Talkers sampler R-1-1024 input
ipv6 flow monitor v6Talkers sampler R-1-1024 input
      
```
- D. policy-map Talkers
 

```

class class-default
police cir percent 50
conform-action transmit
exceed-action drop
!
interface Gi0/0
service-policy input Talkers
ip flow monitor v4Talkers
ipv6 flow monitor v6Talkers
      
```

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Flow samplers are created as separate components in a router's configuration. Flow samplers are used to reduce the load on the device that is running Flexible NetFlow by limiting the number of packets that are selected for analysis.

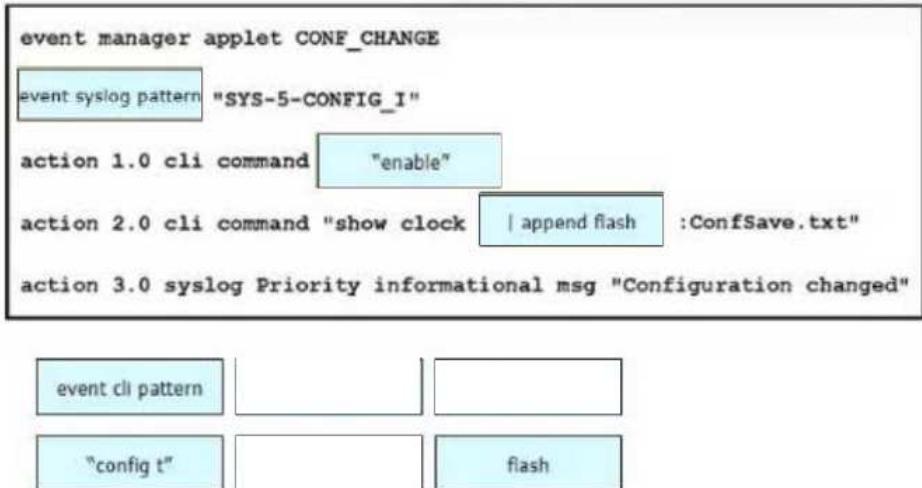
**QUESTION 1018**

Drag and drop the snippets onto the blanks within the code that creates an EEM script that adds an entry to a locally stored text file with a timestamp when a configuration change is made. Not all options are used.

**Select and Place:**

<pre> event manager applet CONF_CHANGE [ ] "SYS-5-CONFIG_I" action 1.0 cli command [ ] action 2.0 cli command "show clock" [ ] :ConfSave.txt" action 3.0 syslog Priority informational msg "Configuration changed" </pre>		
event cli pattern	append flash	"enable"
"config t"	event syslog pattern	flash

**Correct Answer:**



**Section:** (none)  
**Explanation**

**Explanation/Reference:**

#### QUESTION 1019

A network engineer wants to configure console access to a router without using AAA so that the privileged exec mode is entered directly after a user provides the correct login credentials. Which action achieves this goal?

- A. Configure a RADIUS or TACACS+ server and use it to send the privilege level.
- B. Configure login authentication privileged on line con 0.
- C. Configure privilege level 15 on line con 0.
- D. Configure a local username with privilege level 15

**Correct Answer:** D

**Section:** (none)  
**Explanation**

**Explanation/Reference:**

"Configure privilege level 15 on line con 0" also allows the user to enter privileged exec mode directly. However, if no password or "login local" is configured under con 0, any one can enter privileged exec mode directly without entering any login credentials.

#### QUESTION 1020

R2#show ip ospf neighbor	R3#show ip ospf neighbor
R2#show ip ospf interface fastEthernet 1/1	R3#show ip ospf interface fastEthernet 1/1
FastEthernet1/1 is up, line protocol is up	FastEthernet1/1 is up, line protocol is up
Internet Address 192.168.0.5/30, Area 0	Internet Address 192.168.0.6/29, Area 0
Process ID 1, Router ID 10.0.0.5, Network Type BROADCAST, Cost 1	Process ID 1, Router ID 10.0.0.3, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State DR, Priority 1	Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 10.0.0.5, Interface address 192.168.0.5	Designated Router (ID) 10.0.0.3, Interface address 192.168.0.6
No backup designated router on this network	No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5	Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
dead-peer-sync timeout 40	dead-peer-sync timeout 40
Hello due in 00:00:00	Hello due in 00:00:06
Supports Link-local Signaling (LLS)	Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled	Cisco NSF helper support enabled
IETF NSF helper support enabled	IETF NSF helper support enabled
Index 2/2, flood queue length 0	Index 2/2, flood queue length 0
Next 0x0(0x0)(0x0)	Next 0x0(0x0)(0x0)
Last flood scan length is 0, maximum is 0	Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec	Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0	Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)	Suppress hello for 0 neighbor(s)
R2#ping 192.168.0.6 df-bit size 1500	R3#ping 192.168.0.5 df-bit size 1500
Type escape sequence to abort.	Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 192.168.0.6, timeout is 2 seconds.	Sending 5, 1500-byte ICMP Echos to 192.168.0.5, timeout is 2 seconds.
Packet sent with the DF bit set	Packet sent with the DF bit set
!!!!	!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/16 ms	Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/20 ms

Why does the OSPF neighborship fail between the two interfaces?

- A. The MTU is not the same.
- B. The OSPF timers are different.
- C. There is a mismatch in the OSPF interface network type.
- D. The IP subnet mask is not the same.

**Correct Answer:** D

**Section:** (none)  
**Explanation**

**Explanation/Reference:**

In R2, the configured subnet prefix length is /30. In R3, the configured subnet prefix length is /29.

#### QUESTION 1021

When using a Cisco Catalyst 9800 Series WLC, which tag/profile can be applied to APs to change the mode to FlexConnect in a specific location?

- A. AP join profile
- B. Flex profile
- C. Policy tag
- D. Site tag

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

The Site Tag is the element that allows you to specify which AP join and/or Flex Profile is assigned to the APs.

**QUESTION 1022**

What is a characteristic of VXLAN?

- A. It uses TCP for transport
- B. It extends Layer 2 and Layer 3 overlay networks over a Layer 2 underlay
- C. It has a 12-byte packet header
- D. It is a multi-tenant solution

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1023**

Which function does a virtual switch provide?

- A. Emulation of power for virtual machines
- B. Communication between virtual machines and hosts outside the hypervisor
- C. CPU context switching for multitasking between virtual machines
- D. RAID storage for virtual machines

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1024**

What is a benefit of YANG?

- A. It enforces the use of a specific encoding format for NETCONF.
- B. It collects statistical constraint analysis information.
- C. It enables multiple leaf statements to exist within a leaf list.
- D. It enforces configuration constraints.

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1025**

```
Device(config)# ntp authenticate  
Device(config)# ntp trusted-key 1 - 3
```

What are two results of the NTP configuration? (Choose two)

- A. The device is configured to synchronize with a system that authenticates with clear text key
- B. The device is configured to synchronize with a system that uses authentication keys 1,2, or 3 in their NTP packets.
- C. The device is configured with the authentication key character string "1 - 3"
- D. The device is configured to synchronize with a system that authenticates with an MD5 key
- E. The device is configured to synchronize with a system that authenticates with an SHA key

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Remarks:

The authentication keys for the 3 keys (i.e. 1, 2 and 3) are configured with the "ntp authentication-key ..." commands.

When configuring authentication key, most IOS versions support MD5 key only. However, some versions (e.g. IOS-XE) support the use of SHA. MD5 key is chosen as suggested answer since it is supported in all IOS versions.

**QUESTION 1026**

Which wireless deployment mode uses a Flex architecture and allows Layer 2 roaming between APs without a physical wireless controller?

- A. Cisco Mobility Express
- B. Unified
- C. Autonomous mode

D. Fabric

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Cisco Mobility Express is a virtual wireless LAN controller integrated within an Access Point.

**QUESTION 1027**

A company requires a wireless solution to support its main office and multiple branch locations. All sites have local Internet connections and a link to the main office for corporate connectivity. The branch offices are managed centrally. Which solution should the company choose?

- A. Cisco DNA Spaces
- B. Cisco Unified Wireless Network
- C. Cisco Mobility Express
- D. Cisco Catalyst switch with embedded controller

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Remarks:**

Cisco DNA Spaces (also known as Cisco Spaces) is a cloud-based location services platform.

**QUESTION 1028**

What is the purpose of data modeling languages?

- A. to describe a data schema convertible into any data encoding format
- B. to provide a framework to describe data flow patterns in networks
- C. to specify algorithms necessary to decode binary-encoded protocol data units
- D. to translate encoded data for interoperability between different CPU architectures

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1029**

```
event manager applet Config
  event cli pattern "configure terminal" [REDACTED]
    action 1.0 cli command "enable"
```

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**sync**

Indicates whether the policy should be executed synchronously before the CLI command executes.

- If the yes keyword is specified, the policy will run synchronously with the CLI command.
- If the no keyword is specified, the policy will run asynchronously with the CLI command.

**skip**

Indicates whether the CLI command should be executed. This keyword is required if the sync keyword is followed by the no keyword. **If the sync keyword is followed by the yes keyword, the skip keyword should not be specified.**

- If the yes keyword is specified, the CLI command will not be executed.
- If the no keyword is specified, the CLI command will be executed. This is the default.

Therefore, in order to prevent "configure terminal" from being executed, sync must be configured with "no" and skip must be configured with "yes".

**QUESTION 1030**

Drag and drop the descriptions from the left onto the routing protocols they describe on the right.

What are the suitable descriptions for OSPF? (Choose two)

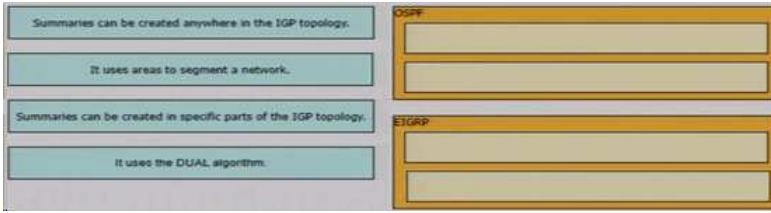
- A. Summaries can be created anywhere in the IGP topology
- B. It uses areas to segment a network
- C. Summaries can be created in specific parts of the IGP topology
- D. It uses the DUAL algorithm

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



### QUESTION 1031

Drag and drop the descriptions from the left onto the routing protocols they describe on the right.  
What are the suitable descriptions for EIGRP? (Choose two)

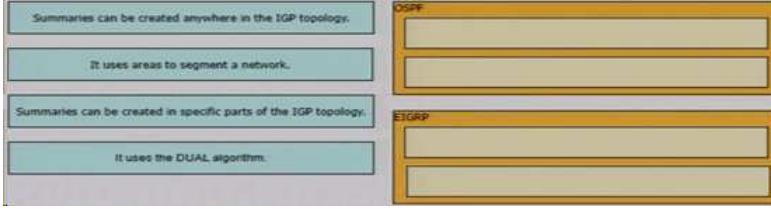
- A. Summaries can be created anywhere in the IGP topology
- B. It uses areas to segment a network
- C. Summaries can be created in specific parts of the IGP topology
- D. It uses the DUAL algorithm

**Correct Answer:** AD

**Section:** (none)

**Explanation**

#### Explanation/Reference:



### QUESTION 1032

How does Cisco DNA center perform a network discovery?

- A. Using ICMP
- B. Using SNMP
- C. Through a DHCP server
- D. Using CDP with a seed IP address

**Correct Answer:** D

**Section:** Selected

**Explanation**

#### Explanation/Reference:

The Discovery feature scans the devices in your network and sends the list of discovered devices to inventory. There are three ways for you to discover devices:

- Use Cisco Discovery Protocol (CDP) and provide a seed IP address.
- Specify a range of IP addresses. (A maximum range of 4096 devices is supported.)
- Use Link Layer Discovery Protocol (LLDP) and provide a seed IP address.

### QUESTION 1033

Which characteristic applies to Cisco SD-Access?

- A. It uses dynamic routing to discover and provision access switches
- B. It uses VXLAN for the data plane
- C. It uses dynamic routing to discover and provision border switches
- D. It uses VXLAN for the control plane

**Correct Answer:** B

**Section:** Selected

**Explanation**

#### Explanation/Reference:

SD-Access Operational Planes:

Control Plane – LISP

Data Plane – VXLAN

Policy Plane – Cisco TrustSec

Management Plane – Cisco DNA Center

### QUESTION 1034

R1#show ntp associations						
address	ref clock	st	when	poll	reach	delay offset disp
*~127.127.1.1	LOCL.	0	4	15	374	0.000 0.000 0.252
* sys.peer, # selected, + candidate, - outlier, x falseticker, ~ configured						

What can be determined from the NTP association information from R1?

- A. R1 is an NTP client and peers with an NTP master of 127.127.1.1
- B. R1 is an NTP master set to Stratum 0.
- C. R1 is an NTP master and is using its internal clock as a time source
- D. R1 is an NTP client and peers with an NTP master set to Stratum 0

**Correct Answer:** C

**Section: (none)****Explanation****Explanation/Reference:**

The word ".LOCL." means that the local clock is being used as a time source so that the router can act as a NTP server. This is configured by the command "ntp master <stratum number 1 - 15>". Note that the stratum information is not shown in the above output. It is shown in the output of "sh ntp associations detail"

**QUESTION 1035**

What is a characteristic of a Type 1 hypervisor?

- A. It is preferred for supporting nonproduction workloads
- B. It has greater latency than a Type 2 hypervisor
- C. It runs on top of the host operating system
- D. It runs on top of bare metal servers

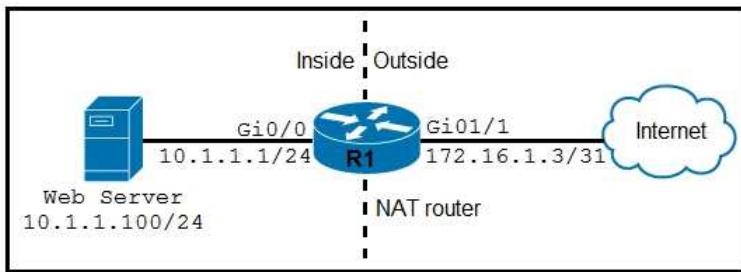
**Correct Answer: D**

**Section: Selected****Explanation****Explanation/Reference:****QUESTION 1036**

Which protocol does Cisco SD-WAN use to protect control plane communication?

- A. STUN
- B. DTLS
- C. OMP
- D. IPsec

**Correct Answer: B**

**Section: Selected****Explanation****Explanation/Reference:****QUESTION 1037**

The web server is configured to listen only to TCP port 8080 for all HTTP requests. Which command is required to allow Internet users to access the web server on HTTP port 80?

- A. ip nat outside source static tcp 10.1.1.100 8080 10.1.1.100 80
- B. ip nat inside source static tcp 10.1.1.100 80 10.1.1.100 8080
- C. ip nat inside source static tcp 10.1.1.100 8080 10.1.1.100 80
- D. ip nat outside source static tcp 10.1.1.100 80 10.1.1.100 8080

**Correct Answer: C**

**Section: (none)****Explanation****Explanation/Reference:**

Normally, the inside network is using private IP address and the NAT setup should be as follows (i.e. assume 10.1.1.0/24 is private and 172.16.1.3/31 is public):  
 ip nat inside source static tcp 10.1.1.100 8080 172.16.1.3 80

With the above setup, Internet user can access the web server with "http://172.16.1.3:80"

However, if both networks have public IP addresses and NAT can also be setup as follows (i.e. assume 10.1.1.0/24 and 172.16.1.3/31 are public):

ip nat inside source static tcp 10.1.1.100 8080 10.1.1.100 80

With the above setup, Internet user can access the web server with "http://10.1.1.100:80" (since 10.1.1.100 is assumed to be accessible from Internet).

**Remarks:**

For some IOS versions, "no-alias" has to be appended at the end i.e.

ip nat inside source static tcp 10.1.1.100 8080 10.1.1.100 80 **no-alias**

Otherwise, error messages about duplicate address will appear e.g.:

%IP-4-DUPADDR: Duplicate address 10.1.1.100 on GigabitEthernet0/0

**QUESTION 1038**

Which mechanism does OAuth use to strengthen REST API security when compared to BasicAuth?

- A. Token
- B. SSL
- C. Authentication
- D. TLS

**Correct Answer: A**

**Section: Selected**

## Explanation

### Explanation/Reference:

OAuth tokens offer more granular authorization control than API keys. They can also be set to expire, which helps to protect against unauthorized access.

### QUESTION 1039

```
v = json.loads(requests.get("http://10.66.77.88:3000/version").text)[0]['ver']
c= json.loads(requests.get("http://10.66.77.88:3000/version").text)[1]['cnt']
bp= []
for i in range (int(c)):
    bp.append(json.loads(requests.get("http://10.66.77.88:3000/badip").text)[i]['ip'])
```

What is achieved by this Python script?

- A. It loads JSON data into an HTTP request.
- B. It converts JSON data to an HTML document.
- C. It counts JSON data from a website.
- D. It reads JSON data into a formatted list.

**Correct Answer: D**

Section: (none)

Explanation

### Explanation/Reference:

The above get JSON data from a web server. The JSON data is converted into Python dictionary. Finally, the data is extracted from the Python dictionary to form a Python list “bp”.

### QUESTION 1040

Which mechanism can be used to enforce network access authentication against an AAA server if the endpoint does not support the 802.1X supplicant functionality?

- A. MAC Authentication Bypass
- B. MACsec
- C. private VLANs
- D. port security

**Correct Answer: A**

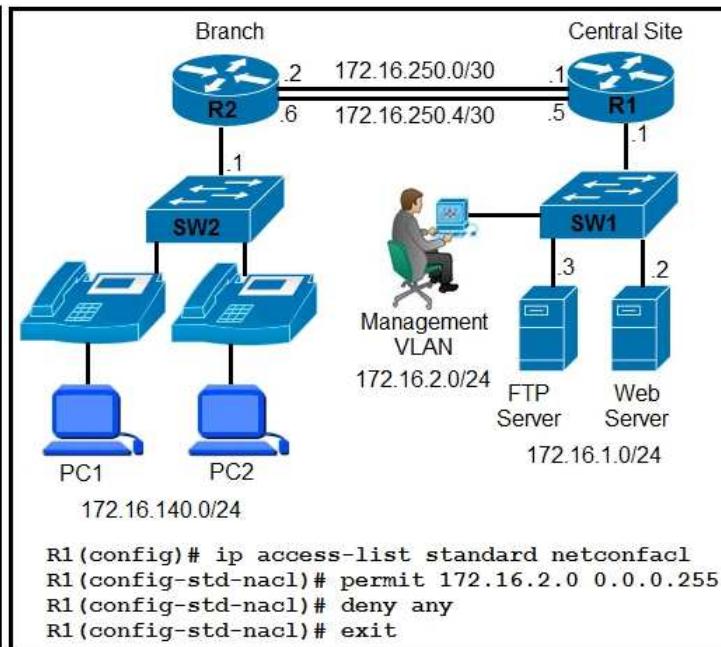
Section: (none)

Explanation

### Explanation/Reference:

Both MAB (MAC authentication bypass) and/or WebAuth can be configured as fallback mechanisms for IEEE 802.1X. In the event that a port is configured for IEEE 802.1X, MAB, and fallback WebAuth, the port first attempts to authenticate the user through IEEE 802.1X. If IEEE 802.1X authentication times out, the switch attempts MAB. If MAB fails, the switch attempts to authenticate with WebAuth.

### QUESTION 1041



An engineer must configure router R1 to allow only NETCONF connections from the management VLAN. Which command completes this configuration?

- A. R1(config-if)# ip access-group netconfacl in
- B. R1(config)# netconf-yang ssh ipv4 access-list name netconfacl
- C. R1(config)#ip http secure-server
 R1(config)# ip http accounting commands 12 default
- D. R1(config-if)#ip access-group netconfacl out

**Correct Answer: B**

Section: (none)

Explanation

### Explanation/Reference:

```
netconf-yang ssh {[ipv4 | ipv6]} access-list name access-list-name} | port port-
```

number]

**Example:**

```
Device(config)# netconf-yang ssh ipv4 access-list name acl1_permit
```

Configures an ACL  
for the NETCONF-  
YANG session.

#### QUESTION 1042

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1
Router(config-if)# ip address 10.0.0.3 255.255.255.0
Router(config-if)# standby 512 ip 10.0.0.1
```

An engineer attempts to configure standby group 512 on interface GigabitEthernet0/1, but the configuration is not accepted. Which command resolves this problem?

- A. standby redirects
- B. standby 512 priority 100
- C. standby 512 preempt
- D. standby version 2

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In HSRP version 1, group numbers are restricted to the range from 0 to 255. HSRP version 2 expands the group number range from 0 to 4095.

#### QUESTION 1043

```
hostname CPE
!
ip dhcp excluded-address 192.168.10.0 192.168.10.10
!
ip dhcp pool LAN
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 192.0.2.254
!
interface Loopback0
ip address 192.168.255.1 255.255.255.255
!
interface GigabitEthernet0/1
description => LAN <=
ip address 192.168.10.1 255.255.255.0
!
--
CPE# debug ip dhcp server packet
DHCP server packet debugging is on.
CPE#
*Sep 11 11:00:12.520: DHCPD: inconsistent relay information.
*Sep 11 11:00:12.520: DHCPD: relay information option exists, but giaddr is zero.
CPE#
```

The CPE router acts as a DHCP server for the locally attached LAN. After DHCP snooping is enabled on the switch where the DHCP clients are connected, clients are unable to obtain their configuration from the DHCP server. What is the cause of this issue?

- A. The IP address of the DHCP server is in the excluded DHCP range.
- B. The configuration of Gi0/1 is missing the ip helper-address 192.168.255.1 command.
- C. The DHCP server drops DHCP packets carrying Option 82 and an empty relay agent IP address.
- D. The excluded DHCP range contains the subnet address of the entire LAN network.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 1044

Which characteristic applies to a traditional WAN solution but not to a Cisco SD-WAN solution?

- A. lengthy installation times
- B. centralized reachability, security, and application policies
- C. low complexity and increased overall solution scale
- D. operates over DTLS/TLS authenticated and secured tunnels

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 1045

```
list = [1, 2]
list = list * 3
print(list)
```

What is the value of the variable list after the code is run?

- A. [1, 2], [1, 2], [1, 2]
- B. [1, 2] \* 3
- C. [1, 2, 1, 2, 1, 2]
- D. [3, 6]

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 1046

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

Why was the response code generated?

- A. The resource was unreachable.
- B. Access was denied based on the user permissions.
- C. Access was denied based on the credentials.
- D. The resource is no longer available on the server.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

HTTP 403 is an HTTP status code meaning access to the requested resource is forbidden. The resource may be blocked due to the IP address or the authenticated user account does not have permission to access the resource.

**Remarks:**

If the user has not been authenticated yet or the credentials are wrong, the server sends HTTP 401 to ask for user authentication.

#### QUESTION 1047

Which configuration saves the running configuration to the startup configuration and logs a "saving configuration automatically" message when a syslog message that contains "SYS-5-CONFIG\_I" is received?

- A. 

```
event manager applet save_config
event syslog pattern "SYS-5-CONFIG_I" period 1
event track 1
action 1.0 cli command "write mem"
action 2.0 syslog msg "saving configuration automatically"
```
- B. 

```
event manager applet save_config
action 1.0 string match "SYS-5-CONFIG_I" save_config
action 2.0 cli command "write mem"
action 3.0 syslog msg "saving configuration automatically"
```
- C. 

```
event manager applet save_config
event syslog pattern "SYS-5-CONFIG_I" period 1
action 1.0 cli command "end"
action 2.0 cli command "write mem"
action 3.0 syslog msg "saving configuration automatically"
```
- D. 

```
event manager applet save_config
event syslog pattern "SYS-5-CONFIG_I" period 1
action 1.0 cli command "write mem"
action 2.0 syslog msg "saving configuration automatically"
```

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The configuration should be:

```

event manager applet save_config
event syslog pattern "%SYS-5-CONFIG_I" period 1
action 1.0 cli command "enable"
action 2.0 cli command "write mem"
action 3.0 syslog msg "saving configuration automatically"
D is chosen as the suggested answer since it is the closest match.

```

Remarks:

There is no "end" command in user / privileged mode.

#### QUESTION 1048

Drag and drop the descriptions from the left onto the correct QoS components on the right.

What are the suitable characteristics for Traffic Policing? (Choose three)

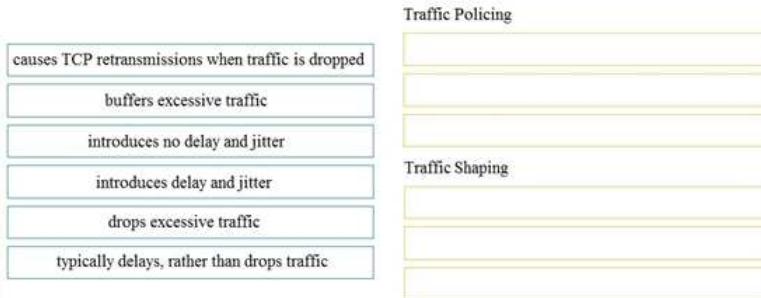
- A. causes TCP retransmissions when traffic is dropped
- B. buffers excessive traffic
- C. introduces no delay and jitter
- D. introduces delay and jitter
- E. drops excessive traffic
- F. typically delays, rather than drops traffic

**Correct Answer:** ACE

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 1049

Drag and drop the descriptions from the left onto the correct QoS components on the right.

What are the suitable characteristics for Traffic Shaping? (Choose three)

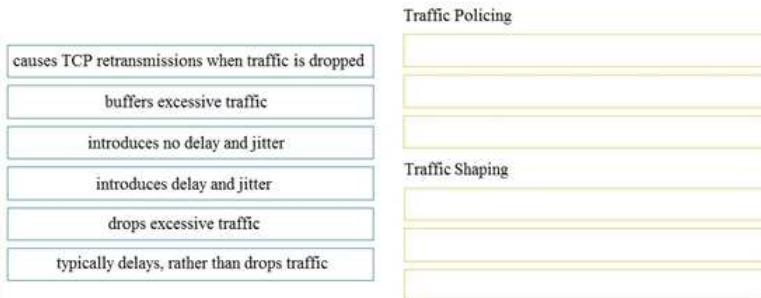
- A. causes TCP retransmissions when traffic is dropped
- B. buffers excessive traffic
- C. introduces no delay and jitter
- D. introduces delay and jitter
- E. drops excessive traffic
- F. typically delays, rather than drops traffic

**Correct Answer:** BDF

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 1050

Which device, in a LISP routing architecture, receives LISP map requests and determines which ETR should handle the map request?

- A. Map resolver
- B. Routing locator
- C. Map server
- D. Proxy ETR

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

When an MR is implemented concurrently with an MS in a private mapping system deployment, the concurrent MS forwards the encapsulated Map-Request messages to the authoritative ETRs.

#### QUESTION 1051

```

R1#show policy-map control-plane
Control Plane

Service-policy input: CoPP
Class-map: telnet_copp (match-all)
 33 packets, 1988 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group 100
Police:
  cir 8000 bps, bc 1500 bytes
  conformed 33 packets, 1998 bytes; actions:
    transmit
  exceeded 0 packets, 0 bytes; actions:
    drop
  conformed 0 bps, exceed 0 bps

Class-map: class-default (match-any)
 59 packets, 5516 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: any
R1#sh access-lists 100
Extended IP access list 100
  10 deny tcp host 10.0.0.5 any eq 22 (13 matches)
  20 permit tcp any any eq 22 (2 matches)
  30 deny tcp host 10.0.0.5 any eq telnet (18 matches)
  40 permit tcp any any eq telnet (31 matches)
R1#

```

Which result is achieved by the CoPP configuration?

- A. Traffic that matches entry 10 of ACL 100 is always dropped.
- B. Class-default is dropped.
- C. Traffic that matches entry 10 of ACL 100 is always allowed with a limited CIR.
- D. Traffic that matches entry 10 of ACL 100 is always allowed.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Traffic that matches entry 10 of ACL 100 is the SSH packets from 10.0.0.5.

#### QUESTION 1052

```

no aaa new-model
username admin privilege 15 secret cisco 123
ip http secure-port 445

```

Which command must be applied to complete the configuration and enable RESTCONF?

- A. ip http server
- B. ip http client username restconf
- C. ip http secure-port 443
- D. ip http secure-server

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In order to use the configured secure port, you need to enable secure server by the command "ip http secure-server".

**Remarks :**

Note that the port 445 actually cannot be configured as secure port.

```

R1(config)#ip http secure-port ?
  443          Default secure port
<1025-65535>  Secure port number range

```

**ip http secure-port**

To set the secure HTTP (HTTPS) server port number for listening, use the **ip http secure-port** command in global configuration mode. To return the HTTPS server port number to the default, use the **no** form of this command.

**ip http secure-port port-number**

**no ip http secure-port**

**Syntax Description**

<b>port-number</b>	Integer in the range of 0 to 65535 is accepted, but the port number must be higher than 1024 unless the default is used. The default is 443.
--------------------	--

However, since the question asks you to complete the configuration (instead of asking you to correct the mistake found in the configuration), therefore "ip http secure-server" is the suggested answer.

#### QUESTION 1053

Drag and drop the snippets onto the blanks within the code to construct a script that advertises the network prefix 192.168.5.0/24 into a BGP session. Not all options are used.

**Select and Place:****Answer Area**

```
<config xmlns:xo="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
<router>
<ios-bgp:bgp>
<ios-bgp:address-family>
<ios-bgp:no-vrf>
<ios-bgp:ipv4>
<ios-bgp:af-name>unicast</ios-bgp:af-name>
<ios-bgp:ipv4-unicast>
<ios-bgp:network>
<ios-bgp:with-mask>
<ios-bgp:number>[ ]</ios-bgp:number>
<ios-bgp:[ ]>[ ]</ios-bgp:mask>
</ios-bgp:with-mask>
</ios-bgp:network>
</ios-bgp:ipv4-unicast>
</ios-bgp:ipv4>
</ios-bgp:no-vrf>
</ios-bgp:address-family>
</ios-bgp:bgp>
</router>
</native>
</config>
```

192.168.5.0

255.255.255.0

with-mask

mask

subnet-mask

**Correct Answer:****Answer Area**

```
<config xmlns:xo="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
<router>
<ios-bgp:bgp>
<ios-bgp:address-family>
<ios-bgp:no-vrf>
<ios-bgp:ipv4>
<ios-bgp:af-name>unicast</ios-bgp:af-name>
<ios-bgp:ipv4-unicast>
<ios-bgp:network>
<ios-bgp:with-mask>
<ios-bgp:number>192.168.5.0</ios-bgp:number>
<ios-bgp:[ ]>255.255.255.0</ios-bgp:mask>
</ios-bgp:with-mask>
</ios-bgp:network>
</ios-bgp:ipv4-unicast>
</ios-bgp:ipv4>
</ios-bgp:no-vrf>
</ios-bgp:address-family>
</ios-bgp:bgp>
</router>
</native>
</config>
```

[ ]

with-mask

subnet-mask

**Section: (none)****Explanation****Explanation/Reference:****QUESTION 1054**

Which AP mode allows a supported AP to function like a WLAN client would, associating and identifying client connectivity issues?

- A. Sensor mode
- B. Client mode
- C. SE-connect mode
- D. Sniffer mode

**Correct Answer: A****Section: (none)****Explanation****Explanation/Reference:**

As these wireless networks grow especially in remote facilities where IT professionals may not always be on site, it becomes even more important to be able to quickly identify and resolve potential connectivity issues ideally before the users complain or notice connectivity degradation. To address these issues, Cisco introduced a Wireless Service Assurance and a new AP mode called sensor mode.

**QUESTION 1055**

Which template is used when multiple templates are grouped together to run in succession in Cisco DNA Center?

- A. Regular
- B. Configuration
- C. Composite
- D. Project

**Correct Answer: C****Section: (none)****Explanation****Explanation/Reference:**

Two or more regular templates are grouped into a composite sequence template. You can create a composite sequential template for a set of templates, which are applied collectively to devices.

**QUESTION 1056**

What is a common trait between Ansible and Chef?

- A. Both rely on NETCONF
- B. Both rely on a declarative approach
- C. Both are used for mutable infrastructure

D. Both require a client to be installed on hosts

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Mutable infrastructure refers to infrastructure that can be modified after it has been deployed. This might involve updating the configuration of a server, installing new software, or making other changes to the infrastructure. Configuration management tools like Ansible, Chef, and Puppet can be used to achieve Mutable infrastructure.

Immutable infrastructure, on the other hand, is the infrastructure that is designed and managed in a way that makes it difficult or impossible to make changes to existing infrastructure once it has been deployed. This is achieved by replacing existing resources with new ones, rather than modifying them in place. Provisioning tool such as Terraform is usually used for Immutable infrastructure.

**QUESTION 1057**

What is one method for achieving REST API security?

- A. Using built-in protocols known as Web Services Security
- B. Using HTTPS and TLS encryption
- C. Using a combination of XML encryption and XML signatures
- D. Using a MD5 has to verify the integrity

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1058**

What is a characteristic of Wi-Fi channels?

- A. The 2.4-GHz band has 24 non-overlapping channels
- B. Devices that connect to the same Wi-Fi channel reside in the same collision domain
- C. Wi-Fi channels are spaced 30 MHz apart
- D. The 5-GHz band offers 11 different channels for Wi-Fi clients

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Access points and wireless clients on the same channel who are also within range of each other form a single broadcast domain, similar to an Ethernet hub. All devices can hear each other's transmissions and if any two devices transmit at the same time, their radio signals will collide and become garbled resulting in data corruption or complete frame loss.

**QUESTION 1059**

Why does the vBond orchestrator have a public IP?

- A. to allow for global reachability from all WAN Edges in the Cisco SD-WAN and to facilitate NAT traversal
- B. to provide access to Cisco Smart Licensing servers for license enablement
- C. to enable vBond to learn the public IP of WAN Edge devices that are behind NAT gateways or in private address space
- D. to facilitate downloading and distribution of operational and security patches

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1060**

What is a benefit of MACsec in a multilayered LAN network design?

- A. Layer 3 links between switches can be secured
- B. There is no requirement to run IEEE 802.1X when MACsec is enabled on a switch port
- C. Layer 2 trunk links between switches can be secured
- D. Application flows between hosts on the LAN to remote destinations can be encrypted

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Multiple choices are true for MACsec. However, for "multilayered" LAN network, it seems that the use of MACsec for "Layer 3 links" is the best answer.

**Remarks:**

From a Cisco web page for Cisco Nexus 9000 Series NX-OS:

MACsec is supported on the N9K-X9736C-FX and the N9K-X9732C-EXM line cards, and on the following interface types:

- Layer 2 switch ports (access and trunk)

- Layer 3 routed interfaces (no subinterfaces)

Enabling MACsec on the Layer 3 routed interface also enables encryption on all the subinterfaces that are defined under that interface. However, selectively enabling MACsec on a subset of subinterfaces of the same Layer 3 routed interface is currently not supported.

**QUESTION 1061**

```

devices = []

file = open('devices.txt','r')
for line in file:

    device_info_list = line.strip().split(',')
    device_info = {}
    device_info['name'] = device_info_list[0]
    device_info['os-type'] = device_info_list[1]
    device_info['ip'] = device_info_list[2]
    device_info['username'] = device_info_list[3]
    device_info['password'] = device_info_list[4]

    devices.append(device_info)

print(devices)
file.close()

```

What is achieved when this Python script is executed?

- A. Each device that is looped through in the devices.txt file is put into its own dictionary that is appended to the parent list.
- B. All devices that are looped through in the devices.txt file are put into a list that is appended to the parent dictionary
- C. All devices that are looped through in the devices.txt file are put into a single dictionary that is appended to the parent list
- D. Each device that is looped through in the devices.txt file is put into its own list that is appended to the parent dictionary

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The device information in each row of the file is read to form a new dictionary. For each iteration of the “for” loop, a dictionary is created for a device and is stored temporarily as “device\_info”. At the end of each iteration, the temporary dictionary is appended to the parent list “devices”.

**QUESTION 1062**

A network engineer must configure the VTY lines on a router to achieve these results

- Remote access should be permitted for all feasible protocols
- Only a password should be required for device authentication.
- All idle EXEC sessions must be terminated in 60 minutes.

Which configuration should be applied?

- A. line vty 0 15  
password Cisco123  
transport input all  
exec-timeout 60
- B. line vty 0 15  
login  
password Cisco123  
transport input all  
absolute-timeout 60
- C. line vty 0 15  
transport input telnet ssh rlogin  
login local  
absolute-timeout 60
- D. line vty 0 15  
password Cisco123  
transport input ssh  
exec-timeout 60

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

“transport input all” allows all feasible protocols. For configuring timeout for “idle” sessions, “exec-timeout” has to be used.

**Remarks:**

You need to check carefully the results that need to be achieved within the question before answering since they may be different in different questions.

**QUESTION 1063**

```

from ncclient import manager

netconf_host = manager.connect(host= 'ios-xe-example.com',
                               port=22,
                               username= 'cisco',
                               password= 'cisco',
                               hostkey_verify=False,
                               device_params={'name':'iosxe'})

print (netconf_host.get_config ('running'))
netconf_host.close_session()

```

An engineer deploys a script to retrieve the running configuration from a NETCONF-capable Cisco IOS XE device that is configured with default settings. The script fails. Which configuration must be applied to retrieve the configuration using NETCONF?

- A. print (netconf\_host.get\_config('show running'))
- B. port=830
- C. device\_params={'name':'ios-xe'})
- D. hostkey\_verify=True,

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

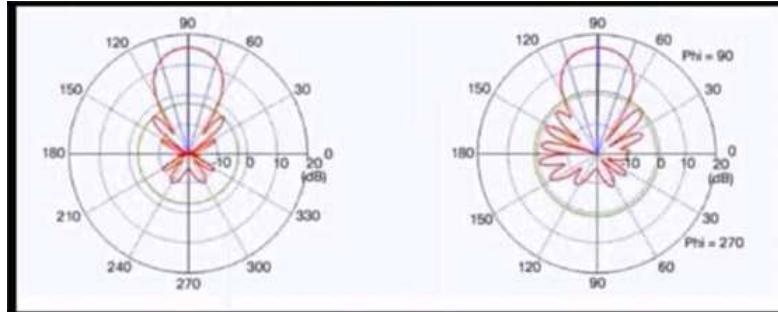
The default port is 830.

**Remarks:**

The followings show the settings of "device\_params" for different types of Cisco devices:

```
CSR: device_params={'name': 'csr'}  
Nexus: device_params={'name': 'nexus'}  
IOS XR: device_params={'name': 'iosxr'}  
IOS XE: device_params={'name': 'iosxe'}
```

**QUESTION 1064**



Which type of antenna is shown on the radiation patterns?

- A. patch
- B. dipole
- C. omnidirectional
- D. Yagi

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1065**

How does NETCONF YANG represent data structures?

- A. as strict data structures defined by RFC 6020
- B. in an XML tree format
- C. in an HTML format
- D. as modules within a tree

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1066**

Which function does a virtual switch provide?

- A. RAID storage for virtual machines
- B. connectivity between virtual machines
- C. CPU context switching for multitasking between virtual machines
- D. emulation of power for virtual machines

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1067**

An engineer must use flexible NetFlow on a group of switches. To prevent overloading of the flow connector, if the flow is idle for 20 seconds, the flow sample should be exported. Which command set should be applied?

- A. flow record recordflow  
exporter flowexport  
record recordflow  
cache timeout active 120  
cache timeout inactive 20  
cache type immediate
- B. flow monitor monitorflow  
exporter flowexport  
record recordflow  
cache timeout active 120  
cache timeout inactive 20

```

cache type immediate
C. flow monitor monitorflow
  exporter recordflow
  cache timeout active 120
  cache timeout inactive 20
  cache type permanent
D. flow record recordflow
  match ipv6 destination ip-address
  match ipv6 source ip-address
  match ipv6 protocol-type view
  match interface input
  match interface output
  match transport destination-port
  collect counter bytes long

```

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

For Flexible Netflow, you can configure cache timeout settings using the Flexible NetFlow **flow monitor configuration mode** command:

```
cache timeout inactive
```

This command controls the aging behavior of the normal type of cache. If a flow has not seen any activity for a specified amount of time, that flow will be aged out (for exporting). By default, this timeout is 15 seconds, but this value can be adjusted depending on the type of traffic expected.

Note that the above cache timeout setting is only effective for the default cache type i.e. "cache type normal". However, there is something wrong in the question and all choices with "flow monitor monitorflow" are not setup with this default cache type (i.e. either there is no "cache type" command or "cache type normal" is specified explicitly).

However, since one of the choices with "flow monitor monitorflow" is missing the command "record" within, therefore the one that includes the command "record" is chosen as the suggested answer although it is wrongly configured with "cache type immediate".

**QUESTION 1068**

```

R2(config)#event manager applet script_1
R2(config-applet)#action 1 cli command "enable"
R2(config-applet)#action 2 cli command "config t"
R2(config-applet)#action 3 cli command "interface ge0/0"
R2(config-applet)#action 4 cli command "ip add 172.16.1.1 255.255.255.0"
R2(config-applet)#action 5 cli command "no sh"
R2(config-applet)#action 6 cli command "end"
R2(config-applet)#exit

```

An engineer must create a manually triggered EEM applet to enable the R2 router interface and assign an IP address to it. What is required to complete this configuration?

- A. R2(config-apple)#action 4 cli command "ip add 172.16.1.1 0.0.0.255"
- B. R2(config)# event manager session cli username
- C. R2(config-applet)# event oir
- D. R2(config-applet)# event none sync yes

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In order to setup an applet for running manually, you need to configure "event none".

**QUESTION 1069**

```

client.connect(ip, port=22, username=usr, password=pswd)
stdin, stdout, stderr = client.exec_command('show ip bgp 192.168.101.0 bestpath\n')
print(stdout)

```

Which action does the Python script accomplish?

- A. connects to the device using Telnet and exports the routing table information
- B. connects to the device using SSH and exports the routing table information
- C. displays the output of the show command in an unformatted way
- D. displays the output of the show command in a formatted way

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The script connects to the device using SSH and send the command "show ip bgp ..." to obtain information about the BGP routing table. The output from the show command is then printed out without being formatted by Python.

Therefore, two of the choices are correct. However, since the script obtain the BGP routing table instead of the general routing table and the word "exports" usually means outputting the data through a media e.g. file. Therefore, it seems that "displays the output of the show command in an unformatted way" should be the better answer.

**QUESTION 1070**

```

import requests
import json

url='https://switchIP.firebaseio.com/ins'
switchuser='username'
switchpassword='password123'

myheaders=[{"content-type":'application/json-rpc'}
payload={}
{
    "jsonrpc": "2.0",
    "method": "cli",
    "params": {
        "cmd": "show clock",
        "version": 1
    },
    "id": 1
}
response = requests.post(url,data=json.dumps(payload), headers=myheaders,auth=(switchuser,switchpassword), verify=False) json()

```

Which Python code parses the response and prints "18:32:21.474 UTC Sun Mar 10 2019"?

- A. print(response['result'][0]['simple\_time'])
- B. print(response['result'][0]['body']['simple\_time'])
- C. print(response['body'][0]['simple\_time'])
- D. print(response['jsonrpc'][0]['body'][0]['simple\_time'])

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

The script sends cli command "show clock" in JSON-RPC format to the Nexus switch device through NX-API. For the response object obtained from the device, the method "json( )" is called to convert the JSON data included within the response into a Python dictionary which is then stored to the variable "response".

The dictionary stored is similar to the followings:

```
{
    "jsonrpc": "2.0",
    "result": {
        "body": {
            "simple_time": "18:32:21.474 UTC Sun Mar 10 2019\n",
            "time_source": "NTP"
        }
    },
    "id": 1
}
```

In order to get the datetime information from the above Python dictionary, you need to access it through the key names "result" à "body" à "simple\_time".

**Remarks :**

For sending other commands in NX-API's JSON-RPC format, the last key name for obtaining the required information will be different. However, the first two key names should always start with "result" à "body"

**QUESTION 1071**

What is stateful switchover?

- A. cluster protocol used to facilitate switch failover
- B. mechanism to take control from a failed RP while maintaining connectivity
- C. mechanism used to prevent routing protocol loops during an RP switchover
- D. First Hop Redundancy Protocol for host gateway connectivity

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

For preventing layer 3 problems (e.g. those related to routing) during switchover, another additional mechanism NonStop Forwarding (NSF) is required.

**QUESTION 1072**

In a Cisco SD-Access environment, which function is performed by the border node?

- A. Connect users and devices to the fabric domain.
- B. Group endpoints into IP pools.
- C. Provide reachability information to fabric endpoints.
- D. Provide connectivity to traditional Layer 3 networks.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1073**

How does a Type 1 hypervisor function?

- A. It runs directly on a physical server and depends on a previously installed operating system
- B. It runs directly on a physical server and includes its own operating system
- C. It runs on a virtual server and depends on a previously installed operating systems
- D. It runs on a virtual server and includes its own operating system

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1074**

In which way are EIGRP and OSPF similar?

- A. Both protocols support autosummarization.
- B. Both protocols use hello packets to discover neighbors.
- C. Both protocols support unequal-cost load balancing.
- D. Both protocols send updates using unicast addresses.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1075**

What are two characteristics of vManage APIs? (Choose two.)

- A. Northbound API is based on RESTCONF and JSON.
- B. Southbound API is based on NETCONF and XML.
- C. Southbound API is based on RESTCONF and JSON.
- D. Southbound API is based on OMP and DTLS.
- E. Northbound API is RESTful using JSON.

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1076**

How do MAC address table and TCAM differ?

- A. TCAM lookups can match only 1s and 0s, and MAC address lookups can match 1s, 0s, and a third "care/don't care" state
- B. TCAM is a type of memory, and the MAC address table is a logical structure
- C. TCAM is populated from the ARP file, and the MAC address table is populated from the switch configuration file
- D. TCAM stores Layer 2 forwarding information, and the MAC address table stores QoS information

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1077**

Which feature is offered by the Cisco Advanced Malware Protection for Endpoints solution?

- A. DNS Protection
- B. File Sandboxing
- C. TrustSec
- D. NetFlow

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1078**

A Cisco administrator deploys a new wireless network but CAPWAP APs cannot communicate with the wireless controller. IP connectivity in the network functions properly. Which action resolves the issue?

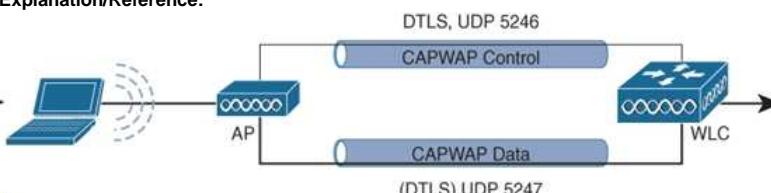
- A. Enable the UDP Lite feature on the WLC.
- B. Ensure that the controller is connected to a AAA server.
- C. Open CAPWAP UDP port 12222 in the network firewall.
- D. Open CAPWAP UDP ports 5246 and 5247 in the network firewall.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 1079**

Drag and drop the characteristics from the left onto the orchestration tools they describe on the right.  
Which are the correct characteristics of Ansible? (Choose two.)

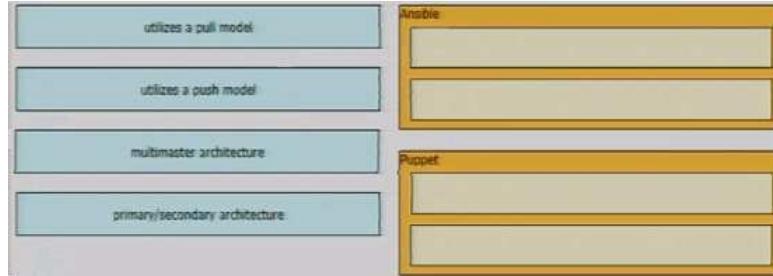
- A. utilizes a pull model
- B. utilizes a push model
- C. multimaster architecture
- D. primary/secondary architecture

**Correct Answer:** BD

**Section:** Selected

**Explanation**

**Explanation/Reference:**



**QUESTION 1080**

Drag and drop the characteristics from the left onto the orchestration tools they describe on the right.  
Which are the correct characteristics of Puppet? (Choose two.)

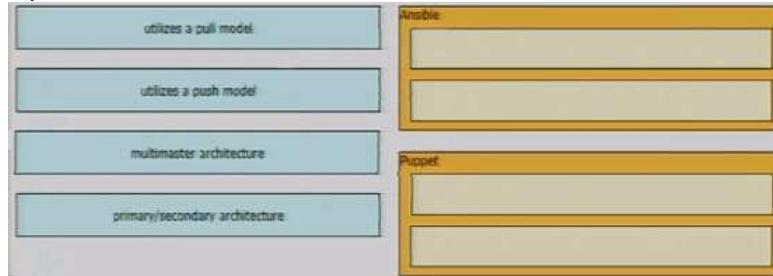
- A. utilizes a pull model
- B. utilizes a push model
- C. multimaster architecture
- D. primary/secondary architecture

**Correct Answer:** AC

**Section:** Selected

**Explanation**

**Explanation/Reference:**



**QUESTION 1081**

Drag and drop the descriptions from the left onto the QoS components on the right.  
Which are the correct descriptions of Traffic Policing? (Choose three.)

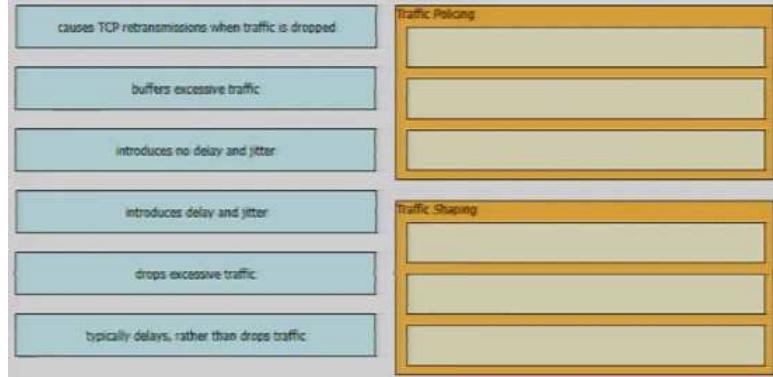
- A. causes TCP retransmissions when traffic is dropped
- B. buffers excessive traffic
- C. introduces no delay and jitter
- D. introduces delay and jitter
- E. drops excessive traffic
- F. typically delays, rather than drops traffic

**Correct Answer:** ACE

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 1082**

Drag and drop the descriptions from the left onto the QoS components on the right.  
Which are the correct descriptions of Traffic Shaping? (Choose three.)

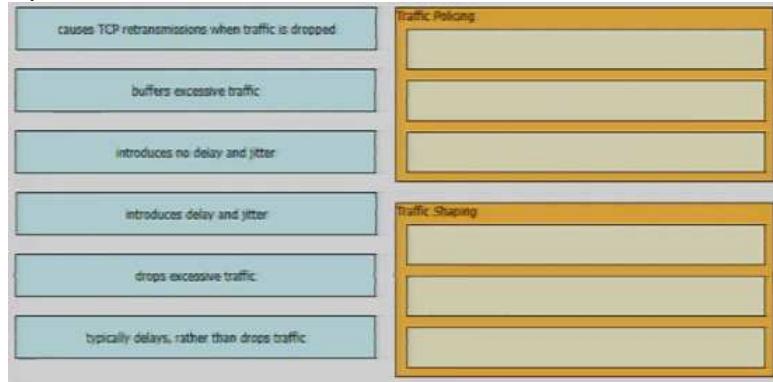
- A. causes TCP retransmissions when traffic is dropped
- B. buffers excessive traffic
- C. introduces no delay and jitter
- D. introduces delay and jitter
- E. drops excessive traffic
- F. typically delays, rather than drops traffic

**Correct Answer:** BDF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1083**

Which technique is used to protect end user devices and data from unknown file behavior?

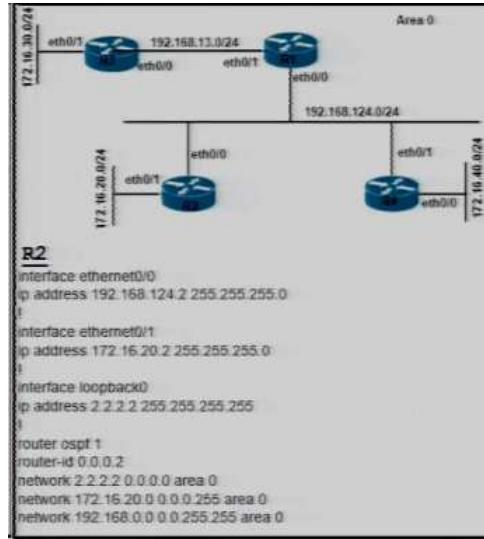
- A. file sandboxing using a protected environment to analyze and simulate the behavior of unknown files
- B. file retrospection using continuous scan and analyses
- C. phishing file quarantine using an internal environment to store attached files
- D. crypto file ransomware protection using a file hash calculation

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1084**

An attacker can advertise OSPF fake routes from 172.16.20.0 network to the OSPF domain and black hole traffic. Which action must be taken to avoid this attack and still be able to advertise this subnet into OSPF?

- A. Configure 172.16.20.0 as a stub network.
- B. configure a passive interface on R2 toward 172.16.20.0.
- C. configure graceful restart on the 172.16.20.0 interface.
- D. apply a policy to filter OSPF packets on R2.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Since OSPF fake routes are received through 172.16.20.0 network, there is probably a rogue router in that network advertising fake routes. Fake routes can be stopped by preventing R2 from forming neighbor with any router in that network.

**QUESTION 1085**

```
vlan_list = """\nvlan10 => 192.168.10.1\nvlan20 => 192.168.20.1\nvlan30 => 192.168.30.1\n"""\n\ndef print_vlan(vlans):\n    print(vlans)\n\ndef vlan():\n    vlan_list_dict = {} \n\n    for line in vlan_list.split("\n"):\n        if not line.strip():\n            continue\n        k, v = [word.strip() for word in line.split("=>")]\n        vlan_list_dict[k] = v\n    return vlan_list_dict\n\ndef main():\n    vlans = vlan()\n    print_vlan(vlans)\n\nif __name__ == "__main__":\n    main()
```

A network engineer must use a python script to convert data received from a network device. Which type of data is printed to the console when the script runs?

- A. dictionary with a key-value pair
- B. list of lists
- C. tuple list
- D. list of strings

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In the function "vlan()", data is extracted from the string "vlan\_list" in a for-loop to "vlan\_list\_dict". "vlan\_list\_dict" is a Python dictionary since:  
- It is created with "{}"  
- Data is added with "vlan\_list\_dict[k] = v"

After the dictionary "vlan\_list\_dict" is returned and stored in "vlans" in "main()", the dictionary is then passed to the function "print\_vlan()" for printing.

**QUESTION 1086**

Which configuration enables a cisco router to send information to a TACACS+ server for individual EXEC commands associated with privilege level 15?

- A. Router(config)# aaa accounting exec default start-stop group tacacs+
- B. Router(config)# aaa authorization exec default group tacacs+
- C. Router(config)# aaa authorization commands 15 default group tacacs+
- D. Router(config)# aaa accounting commands 15 default start-stop group tacacs+

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

When you configure the "aaa accounting command" command, each command of the specified privilege level entered by an administrator is recorded and sent to the accounting server.

**QUESTION 1087**

Which action controls the maximum cell size in a high-density wireless environment?

- A. disable low data rates
- B. decrease TX power on access points
- C. statically set TX power on access points to max
- D. set mandatory data rates

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

The reduction in cell size ensures that the clients are connected to the nearest access point using the highest possible data rates. In a high density environment, the smaller the cell size, the better. Cell size can be reduced by e.g. reducing the TX power or increasing the mandatory minimum data rate.

**QUESTION 1088**

Why are stateless calls executed by REST API useful in cloud applications?

- A. they use HTTPS to implement all calls
- B. they rely on data stored on the server for calls
- C. they are easy to redeploy and to scale
- D. they control URL decoding

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1089**

Which type of API enables Cisco Catalyst Center (formerly DNA Center) to focus on outcome instead of the individual steps that are required to achieve the outcome?

- A. northbound Intent
- B. eastbound Events and Notifications
- C. westbound Integration
- D. southbound Multivendor Support

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The Intent APIs are northbound REST APIs that expose specific capabilities of Cisco DNA Center platform. The Intent APIs provide policy-based abstraction of business intent, allowing you to focus on an outcome to achieve instead of struggling with the mechanisms that implement that outcome.

**QUESTION 1090**

What is a characteristic of Layer 3 roaming?

- A. it provides seamless client roaming between APs in different Layer 3 networks but within the same mobility group
- B. it is only supported on controllers that run SSO
- C. clients must obtain a new IP address when they roam between APs
- D. it provides seamless roaming between APs that are connected to different Layer 3 networks and different mobility groups

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

A mobility group is a set of controllers, identified by the same mobility group name, that defines the realm of seamless roaming for wireless clients.

However, with the "mobility list" feature, roaming between WLC in different mobility groups is also supported. WLCs supports up to 72 controllers in the mobility list of a controller and seamless roam across multiple mobility groups. Through seamless roaming, the client maintains its IP address across all mobility groups. However, Cisco Centralized Key Management (CCKM) and Proactive Key Caching (PKC) are supported only for intra-mobility-group roaming. When a client crosses a mobility group boundary while a roam, the client is fully authenticated, but the IP address is maintained, and EtherIP tunneling is initiated for Layer 3 roaming. Unlike before, seamless roaming here means the maintaining of the IP address only since authentication process must be performed during roaming.

The suggested answer is the basic characteristic of Layer 3 roaming i.e. without the additional setup of "mobility list".

**QUESTION 1091**

Which message type is valid for IGMPv3?

- A. graft
- B. hello
- C. source-specific membership report
- D. leave group

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1092**

Which type of roaming event occurs when a client roams across multiple mobility groups?

- A. layer 2
- B. layer 1
- C. layer 7
- D. layer 3

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1093**

Which feature allows HSRP to failover from the active route processor to the standby route processor without loss of data or path change?

- A. preemption
- B. stateful switchover
- C. HSRP tracking
- D. IP SLA tracking

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

SSO HSRP alters the behavior of HSRP when a device with redundant Route Processors (RPs) is configured for stateful switchover (SSO) redundancy mode. When an RP is active and the other RP is standby, SSO enables the standby RP to take over if the active RP fails. With this functionality, HSRP SSO information is synchronized to the standby RP, allowing traffic that is sent using the HSRP virtual IP address to be continuously forwarded during a switchover without a loss of data or a path change. Additionally, if both RPs fail on the active HSRP device, then the standby HSRP device takes over as the active HSRP device.

**QUESTION 1094**

Drag and drop the automation characteristics from the left onto the appropriate tools on the right. Not all options are used. Which are the correct automation characteristics for Chef?

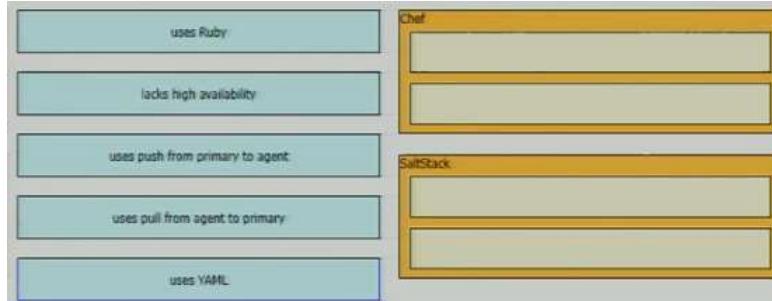
- A. uses Ruby
- B. lacks high availability
- C. uses push from primary to agent
- D. uses pull from agent to primary
- E. uses YAML

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1095**

Drag and drop the automation characteristics from the left onto the appropriate tools on the right. Not all options are used. Which are the correct automation characteristics for SaltStack?

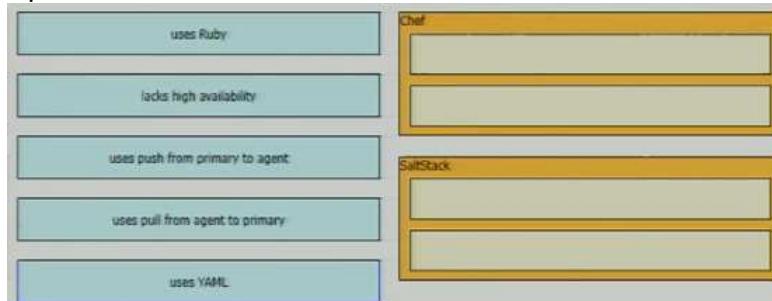
- A. uses Ruby
- B. lacks high availability
- C. uses push from primary to agent
- D. uses pull from agent to primary
- E. uses YAML

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1096**

Which mobility role is assigned to a client in the client table of the new controller after a layer 3 roam?

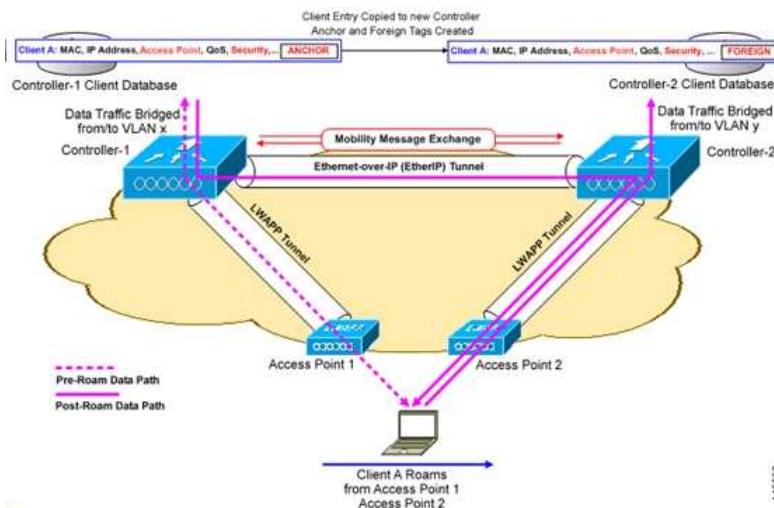
- A. transparent
- B. mobility
- C. foreign
- D. anchor

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**



#### QUESTION 1097

What occurs during a layer 2 inter-controller roam?

- A. The client retains the same IP address and security context.
- B. The client is marked as foreign in the database of each new controller to which it is connected.
- C. The client must be associated to a new controller where a new IP address and security context are applied.
- D. A new security context is applied for each controller to which the client is associated, but the IP address remains the same.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 1098

When deploying Cisco SD-Access Fabric APs, where does the data plane VXLAN tunnel terminate?

- A. directly on the fabric APs
- B. on the fabric border node switch
- C. on the first-hop fabric edge switch
- D. on the WLC node

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The AP forwards client traffic based on the forwarding table as programmed by the WLC. The VXLAN tunnel destination is always the Fabric Edge where the access tunnel is terminated. In case of an extended node the access tunnel is terminated on the Fabric Edge where the extended nodes are connected.

#### QUESTION 1099

Which two components are needed when a Cisco SD-Access fabric is designed? (Choose two.)

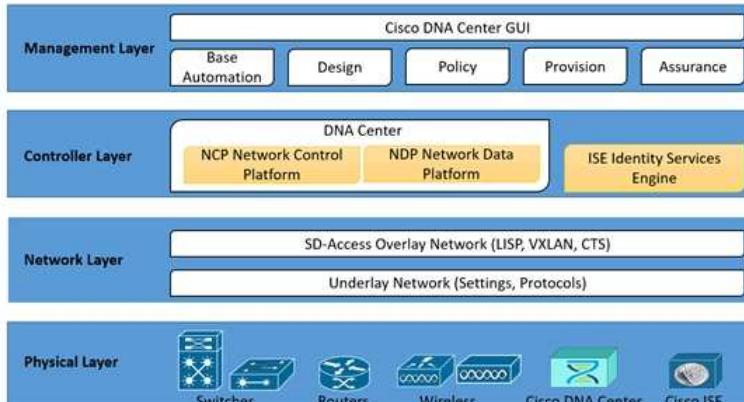
- A. Identity Service Engine
- B. Cisco Prime Infrastructure
- C. Cisco Data Center Network Manager
- D. Cisco Catalyst Center (formerly DNA center) application
- E. Firepower Threat Defense

**Correct Answer:** AD

**Section:** Selected

**Explanation**

**Explanation/Reference:**



**QUESTION 1100**

Which two sources cause interference for Wi-Fi networks? (Choose two.)

- A. fish tank
- B. mirrored wall
- C. DECT 6.0 cordless phone
- D. 900MHz baby monitor
- E. incandescent lights

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The wireless signal will degrade (or die completely) when going through brick (fireplace), metal (file cabinet), steel, lead, mirrors, water (fish tank), large appliances, glass, etc.

**Remarks:**

The new DECT 6.0 cordless phone standard has been allocated the 1.920 to 1.930GHz band in the US, so it should cause no interference at all.

The frequency used by 900MHz baby monitor does not interfere with Wi-Fi.

Unlike fluorescent lights, incandescent lights do not interfere with Wi-Fi.

**QUESTION 1101**

Which two operations are valid for RESTCONF? (Choose two.)

- A. ADD
- B. GET
- C. PUSH
- D. HEAD
- E. REMOVE
- F. PULL

**Correct Answer:** BD

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1102**

In which forms can Cisco Catalyst SD-WAN routers be deployed at the perimeter of a site to provide SD-WAN services?

- A. hardware, virtualized, and cloud instances
- B. hardware and virtualized instances
- C. hardware, software, cloud, and virtualized instances
- D. virtualized instances

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1103**

Which two characteristics apply to Type 1 hypervisors? (Choose two.)

- A. They provide a platform for running bare metal operating systems
- B. They can be used to create and manage virtual storage
- C. They are widely available to license for free
- D. They provide a platform for running guest operating systems
- E. They are a software layer that runs on top of a virtual server

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1104**

In a wireless network environment, which measurement compares the received signal to the background noise?

- A. free space path loss
- B. fading
- C. SNR
- D. link power budget

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1105**

Which two conditions occur when the primary route processor fails on a switch that is using dual route processors with stateful switchover? (Choose two.)

- A. User sessions are immediately recreated on the new active route processor.

- B. Data forwarding can continue along known paths until routing protocol information is restored.
- C. The standby route processor is fully initialized and state information is maintained.
- D. The standby route processor initialization is started when the primary router processor fails.
- E. Data forwarding is stopped until the routing protocols reconverge after the switchover.

**Correct Answer:** BC

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1106**

What is a characteristic of the Cisco Catalyst Center (formerly DNA Center) Template Editor feature?

- A. It facilitates software upgrades to network devices from a central point.
- B. It facilitates a vulnerability assessment of the network devices.
- C. It uses a predefined configuration through parameterized elements or variables.
- D. It provides a high-level overview of the health of every network device.

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1107**

Drag and drop the characteristics from the left onto the corresponding orchestration tool on the right. Which are the correct characteristics of Puppet? (Choose two.)

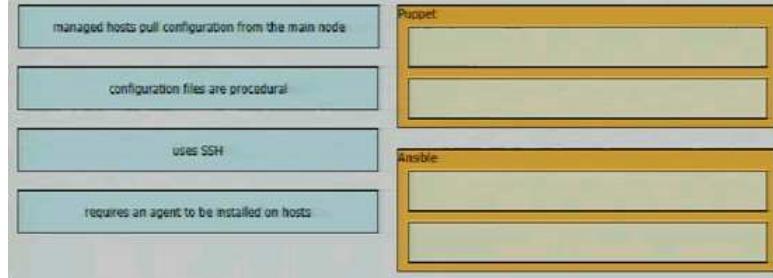
- A. managed hosts pull configuration from the main node
- B. configuration files are procedural
- C. uses SSH
- D. requires an agent to be installed on hosts

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 1108**

Drag and drop the characteristics from the left onto the corresponding orchestration tool on the right. Which are the correct characteristics of Ansible? (Choose two.)

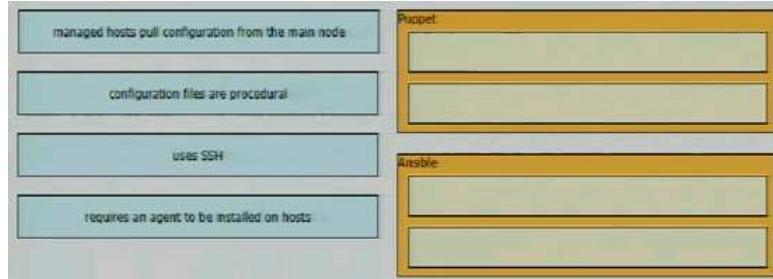
- A. managed hosts pull configuration from the main node
- B. configuration files are procedural
- C. uses SSH
- D. requires an agent to be installed on hosts

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 1109**

What are two benefits of using Cisco TrustSec? (Choose two.)

- A. simplified management of network access
- B. end-to-end traffic encryption

- C. unknown file analysis using sandboxing
- D. consistent network segmentation
- E. advanced endpoint protection against malware

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1110**

Which action reduces sticky clients in dense RF environments?

- A. Increase radio channel widths to 160 MHz.
- B. Decrease the mandatory minimum data rates.
- C. Increase the mandatory minimum data rates
- D. Decrease radio channel widths to 40 MHz.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

A client is referred as "Sticky" when it does not roam or move to a nearby AP connection that has stronger signal strength. Cisco Optimized Roaming addresses the sticky client challenge by proactively disconnecting clients, thus enabling the clients to move to a nearby AP that offers stronger connectivity. It achieves this functionality by actively monitoring Data RSSI packets, and enforcing client disassociation when the RSSI is lower than the set threshold for data rate.

**QUESTION 1111**

Which language can be used to model configuration and state data?

- A. XDR
- B. JSON
- C. YANG
- D. XML

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

YANG is a data modeling language used to model configuration data, state data, Remote Procedure Calls, and notifications for network management protocols.

**QUESTION 1112**

What is a benefit of implementing stateful switchover?

- A. flexibility
- B. resiliency
- C. scalability
- D. modularity

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Resiliency means "the capacity to withstand or to recover quickly from difficulties".

**QUESTION 1113**

```
event manager applet config-alert
  event cli pattern "conf t" sync yes
```

A network engineer must be notified when a user switches to configuration mode. Which script should be applied to receive an SNMP trap and a critical-level log message?

- A. action 1.0 snmp-trap strdata "Configuration change alarm"  
action 2.0 syslog msg "Configuration change alarm"
- B. action 1.0 snmp-trap strdata "Configuration change critical alarm"
- C. action 1.0 snmp-trap strdata "Configuration change alarm"  
action 1.0 syslog priority critical msg "Configuration change alarm"
- D. action 1.0 snmp-trap strdata "Configuration change alarm"  
action 1.1 syslog priority critical msg "Configuration change alarm"

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

If "priority critical" is not set, the syslog messages will be set to the informational priority level.

Remarks: If two "action" commands are entered with the same action label e.g. "1.0", the latter one will replace the former one.

**QUESTION 1114**

Which access control feature does MAB provide?

- A. simultaneous user and device authentication
- B. network access based on the physical address of a device
- C. allows devices to bypass authentication

D. user access based on IP address

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

MAC Authentication Bypass (MAB) uses the MAC address of a device to determine the level of network access to provide. MAB offers visibility and identity-based access control at the network edge for endpoints that do not support IEEE 802.1X.

**QUESTION 1115**

Which technology collects location information through data packets received by the APs instead of using mobile device probes?

- A. FastLocate
- B. RF fingerprinting
- C. detect and locate
- D. hyperlocation

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

FastLocate enables higher location refresh rates by collecting RSSI or location information through data packets received by the APs. Using these data packets, location-based services (LBS) updates are initiated by the network and are available more frequently.

**QUESTION 1116**

```
event manager applet config-alert  
event cli pattern "write mem.**" sync yes
```

Which EEM script generates a critical-level syslog message and saves a copy of the running configuration to the bootflash when an administrator saves the running configuration to the startup configuration?

- A. action 1.0 cli command copy running-config bootflash:/current\_config.txt  
action 2.0 syslog priority critical msg "Configuration saved and copied to bootflash"
- B. action 1.0 cli command copy running-config bootflash:/current\_config.txt  
action 2.0 syslog msg "Configuration saved and copied to bootflash"
- C. action 1.0 cli command "enable"  
action 2.0 cli command "configure terminal"  
action 3.0 cli command "file prompt quiet"  
action 4.0 cli command "end"  
action 5.0 cli command copy running-config bootflash:/current\_config.txt  
action 6.0 cli command "configure terminal"  
action 7.0 cli command "no file prompt quiet"  
action 8.0 syslog priority critical msg "Configuration saved and copied to bootflash"
- D. action 1.0 cli command "enable"  
action 2.0 cli command "file prompt quiet"  
action 3.0 cli command copy running-config bootflash:/current\_config.txt  
action 4.0 cli command "no file prompt quiet"  
action 5.0 syslog priority critical msg "Configuration saved and copied to bootflash"

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

In order to avoid the showing of user prompt to confirm the action when running the copy command, you can configure the global configuration mode command "file prompt quiet" before copying and then remove it after copying.

**QUESTION 1117**

The screenshot shows the '5 GHz Network Status' section with the following settings:

- Beacon Interval\*: 100
- Fragmentation Threshold (bytes)\*: 2346
- DTPC Support: checked
- Tri-Radio Mode: unchecked
- RSSI Low Check: checked
- RSSI Threshold (dBm)\*: -81

The 'Data Rates' section shows the following configuration:

Rate	Mode	Status
6 Mbps	Disabled	
9 Mbps	Supported	
12 Mbps	Mandatory	
18 Mbps	Supported	
24 Mbps	Mandatory	
36 Mbps	Supported	
48 Mbps	Supported	
54 Mbps	Mandatory	

A customer reports that many wireless clients cannot reliably receive multicast audio. Which action resolves this issue?

- Disable RSSI Low Check
- Set the RSSI Threshold to -67dBm
- Set the Fragmentation Threshold to 1250 bytes
- Set the 24 Mbps and 54 Mbps data rates to Supported

**Correct Answer: D**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

Data Rates on a Cisco AP can be configured in one of the three states:  
Mandatory: unless the client also supports this data rate, it will not be admitted  
Supported: client may or may not support his data rate  
Disabled: this rate is not used.

More than one mandatory data rate may be set since:

- Beacons and all management traffic are sent with the minimum mandatory rate.
- Multicast traffic is preferred to be sent with the highest mandatory rate (although the client can negotiate a lower mandatory rate later).

In order to avoid loss of multicast traffic, high data rates should not be set as "mandatory" e.g. changing them from "mandatory" to "supported"

**QUESTION 1118**

Why would an architect use an OSPF virtual link?

- to merge two existing Area 0s through a nonbackbone
- to connect a nonbackbone area to Area 0 through another nonbackbone area
- to allow a stub area to transit another stub area
- to connect two networks that have overlapping private IP address space

**Correct Answer: B**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

All areas in an Open Shortest Path First (OSPF) autonomous system must be physically connected to the backbone area (Area 0). In some cases, where this is not possible, you can use a virtual link to connect to the backbone through a non-backbone area. You can also use virtual links to connect two parts of a partitioned backbone through a non-backbone area.

According to the above, there are two possible choices. However:

- the wording "merge" in one of the choices may have a different meaning than "connect"; and
- Since OSPF two Area 0 is highly NOT recommended in OSPF network design, as an "architect", you should not design a OSPF network with two area 0 and use virtual link to connect them together.

**QUESTION 1119**

```
Router1#telnet 192.168.1.1
% telnet connections not permitted from this terminal
```

An engineer attempts to connect to another device from Router1's console port. Which configuration is needed to allow Telnet connections?

- Router1(config)# line console 0
 Router1(config-line)#transport output telnet
- Router1(config)# access-list 100 permit tcp any any eq telnet
 Router1 (config)# line vty
 Router1 (config-line)# access-class 100 out
- Router1(config)# access-list 100 permit tcp any any eq telnet

```
Router1(config)# line console 0
Router1(config-line)# access-class 100 in
D. Router1(config)# line vty 0 15
Router1(config-line)# transport output telnet
```

**Correct Answer:** A  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

**QUESTION 1120**

Which data format can be used for an API request?

- A. HTML
- B. PERL
- C. JSON
- D. Python

**Correct Answer:** C  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

**QUESTION 1121**

In a Cisco SD-Access network architecture, which access layer cabling design is optimal for the underlay network?

- A. Switches are cross-linked to devices at the same layer and at the upstream and downstream devices
- B. Switches are connected to each upstream distribution device
- C. Switches are cross-linked at the same layer and have a single connection to each upstream distribution device
- D. Switches are connected to each upstream distribution and core device

**Correct Answer:** B  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

**QUESTION 1122**

Which feature is available to clients using Layer 2 roaming in a wireless infrastructure?

- A. Roam to a different wireless controller that is on a different subnet and maintain the same IP address
- B. Associate to a new access point on a different wireless controller and change the IP address without connectivity interruption.
- C. Associate to a new access point on the same wireless controller and change the IP address without connectivity interruption.
- D. Roam to a different wireless controller that shares the same subnet and maintain the same IP address.

**Correct Answer:** D  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

**QUESTION 1123**

Which are the characteristics of PIM Sparse Mode? (Choose three.)

- A. builds source-based distribution trees
- B. uses a push model to distribute multicast traffic
- C. uses a pull model to distribute multicast traffic
- D. uses prune mechanisms to stop unwanted multicast traffic
- E. builds shared distribution trees
- F. requires a rendezvous point to deliver multicast traffic

**Correct Answer:** CEF  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

PIM sparse mode (PIM-SM) uses a pull model to deliver multicast traffic. Only network segments with active receivers that have explicitly requested the data will receive the traffic. PIM-SM distributes information about active sources by forwarding data packets on the shared tree. Because PIM-SM uses shared trees (at least initially), it requires the use of a rendezvous point (RP).

**QUESTION 1124**

In a high-density AP environment, which feature can be used to reduce the RF cell size and not demodulate radio packets above a given threshold?

- A. RRM
- B. FRA
- C. RX-SOP
- D. 802.11k

**Correct Answer:** C  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

Use the Rx SOP Threshold drop-down to set the Receiver Start of Packet Detection Threshold (Rx SOP) to determine the Wi-Fi signal level in dBm at which AP radios will demodulate and decode a packet. The higher the RXSOP level, the less sensitive the radio is and the smaller the receiver cell size will be. Reducing the cell size ensures that clients connect to the nearest access point using highest possible data rates. Choose auto to configure the device to use the radio's default threshold.

**Remarks:**

Another feature to reduce RF cell size is Transmit Power Control (TPC). However, the mechanism of TPC does not involve radio packets demodulation.

**QUESTION 1125**

Which tool functions in a push model, supports languages like Python or Ruby, and does not require an agent to be installed per host?

- A. Ansible
- B. Chef
- C. Puppet
- D. Saltstack

**Correct Answer: A****Section: Selected****Explanation****Explanation/Reference:****QUESTION 1126**

What is the function of an intermediate node in a Cisco SD-Access fabric?

- A. to provide an entry and exit point between the fabric and external resources
- B. to route packets within the fabric based on the Layer 3 information in the header
- C. to provide reachability between fabric clients and nonfabric clients on the same subnet
- D. to encapsulate and de-encapsulate packets with a VXLAN header

**Correct Answer: B****Section: Selected****Explanation****Explanation/Reference:**

Intermediate nodes are part of the Layer 3 network used for interconnections among the devices operating in a fabric role such as the interconnections between border nodes and edge nodes. Intermediate nodes do not have a requirement for VXLAN encapsulation/de-encapsulation, LISP control plane messaging support, or SGT awareness. Their requirement is to provide IP reachability, physical connectivity, and to support the additional MTU requirement to accommodate the larger-sized IP packets encapsulated with fabric VXLAN information. Intermediate nodes simply route and transport IP traffic between the devices operating in fabric roles.

**QUESTION 1127**

Which technology is the Cisco SD-Access control plane based on?

- A. CTS
- B. SGT
- C. LISP
- D. VRF

**Correct Answer: C****Section: Selected****Explanation****Explanation/Reference:**

SD-Access Operational Planes

Control Plane – LISP

Data Plane – VXLAN

Policy Plane – Cisco TrustSec

Management Plane – Cisco DNA Center

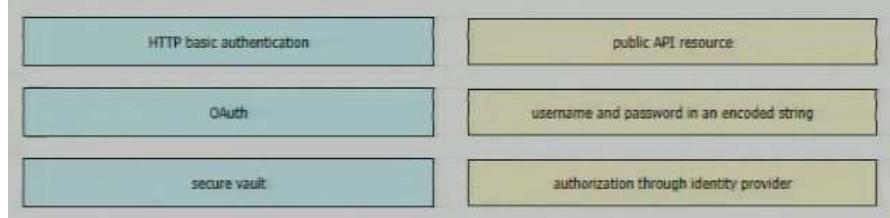
**QUESTION 1128**

How is Layer 3 roaming accomplished in a unified wireless deployment?

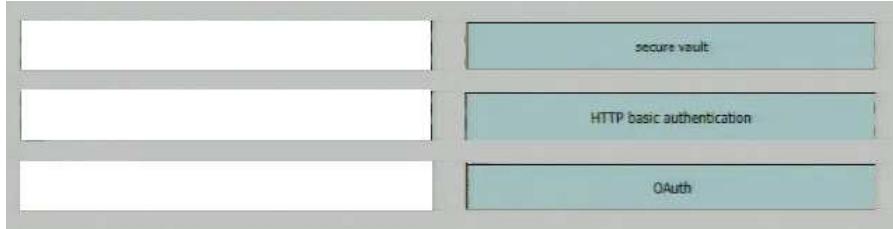
- A. The client entry on the original controller is passed to the database on the new controller.
- B. The new controller assigns an IP address from the new subnet to the client.
- C. An EoIP tunnel is created between the client and the anchor controller to provide seamless connectivity as the client is associated with the new AP.
- D. The client database on the original controller is updated with the anchor entry, and the new controller database is updated with the foreign entry

**Correct Answer: D****Section: Selected****Explanation****Explanation/Reference:****QUESTION 1129**

Drag and drop the REST API authentication methods from the left onto their descriptions on the right.

**Select and Place:**

**Correct Answer:**



**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 1130**

```
1 Status Code: 202
2 Body:
3 {
4   "response": [
5     "startTime": 1630851541471,
6     "endTime": 1630851541523,
7     "version": 1630851541514,
8     "servicetype": "Discovery Service",
9     "isError": false,
10    "lastUpdate": 1630851541514,
11    "progress": "1",
12    "rootId": "2ccb8965-7562-7832-a4c7-88a97594411c",
13    "instanceTenantId": "4cc6502496acb689cb4ca6be",
14    "id": "2ccb8965-7562-7832-a4c7-88a97594411c "
15  ],
16  "version": "1.0"
17 }
```

A POST /discovery request spawns an asynchronous task. After querying for more information about the task, the Cisco Catalyst Center (formerly DNA Center) platform returns the REST API response. What is the status of the discovery task?

- A. restarted
- B. successful
- C. failed
- D. stopped

**Correct Answer: B**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

In the response obtained:

- "`isError`": `false` means no error occurs.
- "`progress`": "`1`" means that the devices that were discovered can be obtained through the Discovery ID "`1`" using the following URL: `/dna/intent/api/v1/discovery/{discovery_id}/network-device`

**QUESTION 1131**

An engineer is reviewing a PCAP file that contains a packet capture of a four-way handshake exchange between a client and AP using WPA2 Enterprise. Which EAPOL message validates and confirms that the client device has successfully installed the GTK?

- A. M1-Message
- B. M3-Message
- C. M4-Message
- D. M2-Message

**Correct Answer: C**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

When Message-4 (final message) of the WPA/WPA2 4-Way handshake is successfully received from the client, it confirms the installation of the derived keys i.e. Pairwise Transient Key (PTK) and the Group Transient Key (GTK). They can now be used in order to encrypt data frames with current AP.

**QUESTION 1132**

Which AP mode analyzes the spectrum to detect sources of interference?

- A. Rogue detector
- B. Sniffer
- C. SE-Connect
- D. Monitor

**Correct Answer: C**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

SE-Connect mode enables an access point to dedicate a connection to Cisco CleanAir technology for spectrum analysis. This is utilized by PC software, such as Cisco Spectrum Expert and MetaGeek Chanalyzer, which can be remotely connected to the access point. The spectrum analysis data is collected and analyzed on all wireless channels to discover the sources of interference.

**QUESTION 1133**

Drag and drop the characteristics from the left onto the tools on the right. Not all options are used.  
Which are the characteristics for Configuration Management Tools? (Choose two.)

- A. Deploy and configure applications and software
- B. Works with mutable elements
- C. Deploy server instances
- D. Only works in a client-server architecture
- E. Works with immutable elements

**Correct Answer:** AB

**Section:** Selected

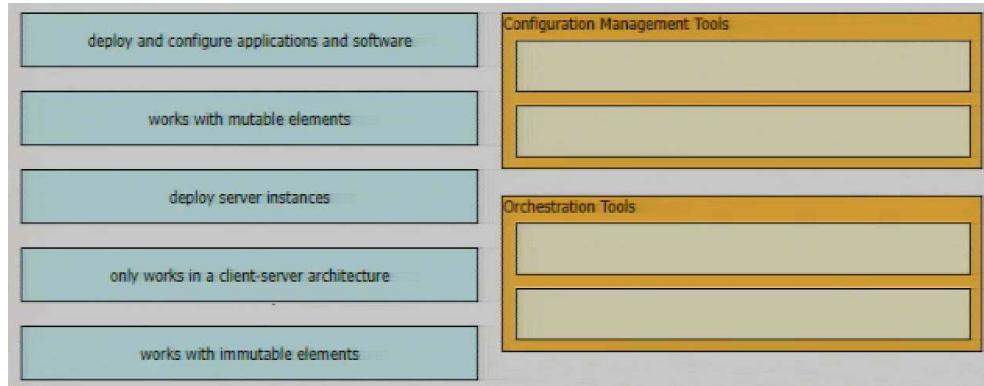
**Explanation**

**Explanation/Reference:**

Configuration management tools are used to install and manage deployments on existing server instances. These tools assign roles to instances without the user needing to specify exact instructions manually. Examples are Chef, Puppet, and Ansible.

Remarks:

Mutable refers to elements that can be modified or changed after it is provisioned



**QUESTION 1134**

Drag and drop the characteristics from the left onto the tools on the right. Not all options are used.  
Which are the characteristics for Orchestration Tools? (Choose two.)

- A. Deploy and configure applications and software
- B. Works with mutable elements
- C. Deploy server instances
- D. Only works in a client-server architecture
- E. Works with immutable elements

**Correct Answer:** CE

**Section:** Selected

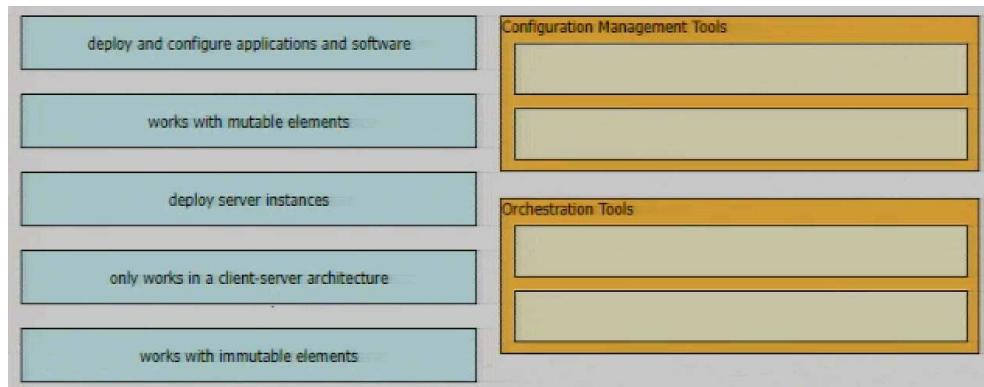
**Explanation**

**Explanation/Reference:**

Orchestration tools allow IT teams to provision server instances and leave configuration to other tools. Orchestration tools are better suited to complex deployments across multiple environments and clusters. Example is Terraform.

Remarks:

Immutable refers to elements that cannot be modified or changed after it is provisioned.



**QUESTION 1135**

What is the name of the numerical relationship of the wireless signal compared to the noise floor?

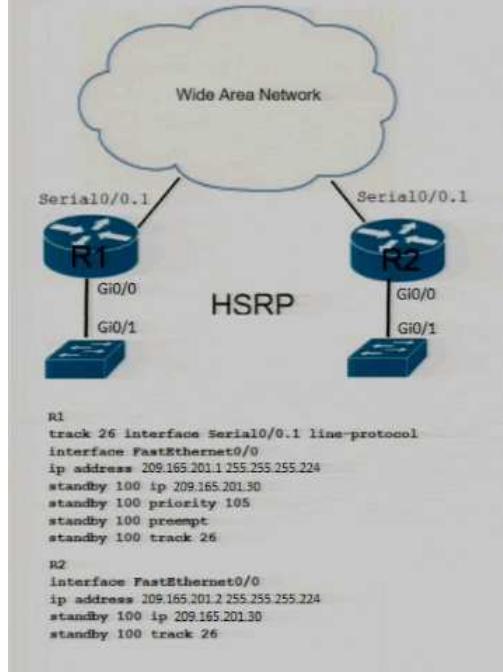
- A. SNR
- B. gain
- C. EIRP
- D. RSSI

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1136**

Which command must be added to enable R2 to take over as primary when Serial Interface 0/0.1 is down on R1?

- A. R2# no standby 100 track 26
- B. R2# standby 100 priority 100
- C. R1# no standby 100 track 26
- D. R2# standby 100 preempt

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1137**

Which set of actions is needed to present a user with a welcome message and/or a message that their password will expire after authentication?

- A. On the Security > Layer 2 tab, ensure no security is enabled  
On the Security > Layer 3 tab, ensure Passthrough is selected
- B. On the Security > Layer 2 tab, ensure WPA+WPA2 is enabled  
On the Security > Layer 3 tab, ensure Authentication is selected
- C. On the Security > Layer 2 tab, ensure WPA+WPA2 is enabled  
On the Security > Layer 3 tab, ensure Splash Web Redirect is selected
- D. On the Security > Layer 2 tab, ensure 802.1x is enabled  
On the Security > Layer 3 tab, ensure Conditional Web Redirect is selected

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

For the Layer3 settings:

Authentication—If you select this option, the user is prompted for username and password while connecting the client to the wireless network.

Passthrough—if you select this option, the user can access the network directly without the username and password authentication.

Conditional Web Redirect—if you select this option, the user can be conditionally redirected to a particular web page after 802.1X authentication successfully completes. You can specify the redirect page and the conditions under which the redirect occurs on your RADIUS server. Conditions might include the user's password reaching expiration or the user needing to pay his or her bill for continued usage.

Splash Page Web Redirect—if you select this option, the user is redirected to a particular web page after 802.1X authentication successfully completes. After the redirect, the user has full access to the network. You can specify the splash web page on your RADIUS server. Note that this requires 802.1x.

#### QUESTION 1138

Which must be configured to enable aWIPS for all radios in a specific site or location, when a Cisco Catalyst 9800 Series WLC is used?

- A. AP join profile
- B. RF tag
- C. policy tag
- D. rogue profile

**Correct Answer:** A

**Section:** (none)

**Explanation**

#### Explanation/Reference:

The Cisco Advanced Wireless Intrusion Prevention System (aWIPS) is a wireless intrusion threat detection and mitigation mechanism. The aWIPS uses an advanced approach to wireless threat detection and performance management. The AP detects threats and generates alarms. It combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention.

#### Procedure for enabling Advanced WIPS(GUI)

- Step 1: Choose Configuration > Tags & Profiles > AP Join.
- Step 2: Click Add. The Add AP Join Profile window is displayed.
- Step 3: In the Add AP Join Profile window, click the Security tab.
- Step 4: Under the aWIPS section, check the aWIPS Enable check box.
- Step 5: Click Apply to Device. You will go back the to General tab.
- Step 6: Click the Security tab.
- Step 7: Under the aWIPS section, check the Forensic Enable check box.
- Step 8: Click Apply to Device.

#### QUESTION 1139

```
import json

Devices={'Switches':
    [
        {'name': 'AccSw1', 'ip': '2001:db8:1:ffff::1'},
        {'name': 'AccSw2', 'ip': '2001:db8:1:ffff::2'}
    ],
    'Routers':
        {'CE1': {'ip': '2001:db8:1:ffff::1'},
         'CE2': {'ip': '2001:db8:1:ffff::2'}
    }
}
```

Which python snippet stores the data structure of the device in JSON format?

- A. with open("devices.json", "w") as OutFile:  
    Devices = json.load(OutFile)
- B. OutFile = open("devices.json", "w")  
    OutFile.write(str(Devices))  
    OutFile.close()
- C. OutFile = open("devices.json", "w")  
    json.dump(Devices, OutFile)  
    OutFile.close()
- D. with open("devices.json", "w") as OutFile:  
    json.dumps(Devices)

**Correct Answer:** C

**Section:** (none)

**Explanation**

#### Explanation/Reference:

`json.dump()` outputs a Python object to a file in JSON format. Two arguments: a Python object and a File object are required.

`json.dumps()` returns a Python object as a JSON string. One argument: a Python object is required.

Since all choices involved outputting to the file "devices.json", `json.dump()` should be used.

**Remarks:**

Without the use of "with ... as ...", you need to use "close()" command to close the file after outputting to it.

#### QUESTION 1140

A Cisco Catalyst Center (formerly DNA Center) REST API sends a PUT to the /dna/intent/api/v1/network-device endpoint. A response code of 504 is received. What does the code indicate?

- A. The response timed out based on a configured interval.
- B. The username and password are not correct.
- C. The web server is not available.
- D. The user does not have authorization to access this endpoint.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

HTTP code 504 i.e. Gateway Timeout error indicates that the upstream server cannot complete the request in a timely manner to deliver the website's content.

Remarks:

If the web server is not available, no HTTP code will be received.

**QUESTION 1141**

Which component transports data plane traffic across a Cisco Catalyst SD-WAN network?

- A. vBond
- B. vManage
- C. vSmart
- D. cEdge

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

In a Cisco SD-WAN deployment, there are two types of edge devices that can be provisioned: cEdge and vEdge.

- vEdge devices run on Viptela OS and are purpose-built for SD-WAN. It is a part of the Viptela acquisition by Cisco.

- cEdge devices run on Cisco's IOS XE OS are typically hardware-based and are part of Cisco's Integrated Services Routers (ISR) and Aggregation Services Routers (ASR) series.

Therefore, the answer can be either vEdge or cEdge.

**QUESTION 1142**

Which nodes require VXLAN encapsulation support in a Cisco SD-Access deployment?

- A. distribution nodes
- B. aggregation nodes
- C. border nodes
- D. core nodes

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

The type of nodes that involve VXLAN encapsulation / decapsulation are the Edge nodes and the Border nodes.

**QUESTION 1143**

At which plane does vBond operate in Cisco Catalyst SD-WAN solutions?

- A. management plane
- B. data plane
- C. control plane
- D. orchestration plane

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Cisco Catalyst SD-WAN consists of the following components:

vBond: Orchestration plane

vManage: Management Plane

vSmart: Control Plane

vEdge: data Plane

**QUESTION 1144**

Which mechanism can be used to enforce network access authentication against an AAA server if the endpoint does not support the 802.1X supplicant functionality?

- A. MAC Authentication Bypass
- B. MACsec
- C. private VLANs
- D. port security

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The MACAuthentication Bypass feature is a MAC-address-based authentication mechanism that allows clients in a network to integrate with the Cisco Identity Based Networking Services (IBNS) and Network Admission Control (NAC) strategy using the client MAC address. The MAC Authentication Bypass feature is applicable to the following network environments:

- Network environments in which a supplicant code is not available for a given client platform.
- Network environments in which the end client configuration is not under administrative control, that is, the IEEE 802.1X requests are not supported on these networks.

**QUESTION 1145**

In Cisco Catalyst Center (formerly DNA Center) Inventory, the Software Version of a network device displays a status of OUTDATED. What does it mean?

- A. There is a later software version available on Cisco Catalyst Center (formerly DNA Center)
- B. The current type of software image does not match the type of the network device.
- C. There is a later software version available at [www.cisco.com](http://www.cisco.com) website.
- D. The current software image does not match the selected Golden Image for this type of network device.

**Correct Answer:** D

**Section:** Selected

## Explanation

### Explanation/Reference:

Catalyst Center compares each device software image with the image that you have designated as golden for that specific device type. If there is a difference between the software image and the golden image, Catalyst Center specifies that the software image of the device is outdated.

### QUESTION 1146

What occurs when a Cisco SD-Access fabric is connected to a traditional campus network?

- A. A fabric intermediate node is used to connect the fabric with the traditional campus network.
- B. All clients must be migrated to new IP addresses that match the IP pool within the fabric.
- C. Traditional campus clients are seen as fabric clients when a Layer 2 border node is used for the VLAN segment.
- D. Only Layer 3 connectivity is supported between the fabric and the traditional campus network.

**Correct Answer:** C

**Section:** (none)

**Explanation**

### Explanation/Reference:

Both layer 3 and layer 2 is supported for the traditional campus network.

However, in port to support layer2, you need to configure a Border node with the Layer 2 handoff. Layer 2 Border Handoff can provide an overlay service between the SD-Access network and the traditional network, allowing hosts in both to communicate, ostensibly, at Layer 2. The Layer 2 Border Handoff allows the fabric site and the traditional network VLAN segment to operate using the same subnet. Communication between the two is provided across the border bode with handoff by providing a VLAN translation between fabric and non-fabric.

### QUESTION 1147

Which type of wireless antenna is used to provide a 360-degree radiation pattern?

- A. Dipole
- B. Yagi
- C. Patch
- D. Directional

**Correct Answer:** A

**Section:** (none)

**Explanation**

### Explanation/Reference:

The dipole radiation pattern is 360 degrees in the horizontal plane and 75 degrees in the vertical plane (assuming the dipole antenna is standing vertically) and resembles a doughnut in shape.

### QUESTION 1148

What is a characteristic of the HSRP SSO process?

- A. It allows the router IOS to detect an installed standby RP.
- B. It enables MD5 authentication within the HSRP group.
- C. It decrements standby router priority if the HSRP group active router fails.
- D. It reduces the amount of time routing table updates take when a failure occurs.

**Correct Answer:** D

**Section:** Selected

**Explanation**

### Explanation/Reference:

### QUESTION 1149

Which two management protocols can be used to modify a network device configuration by using YANG data models? (Choose two.)

- A. RESTCONF
- B. CMIP
- C. NETCONF
- D. CLI
- E. SNMP

**Correct Answer:** AC

**Section:** Selected

**Explanation**

### Explanation/Reference:

### QUESTION 1150

Which RF value represents the decline of the RF signal amplitude over a given distance?

- A. free space path loss
- B. signal-to-noise ratio
- C. effective isotropic radiated power
- D. received signal strength indicator

**Correct Answer:** A

**Section:** (none)

**Explanation**

### Explanation/Reference:

### QUESTION 1151

Drag and drop the automation characteristics from the left to the corresponding tools on the right.

Which are the correct automation characteristics for Ansible? (Choose two.)

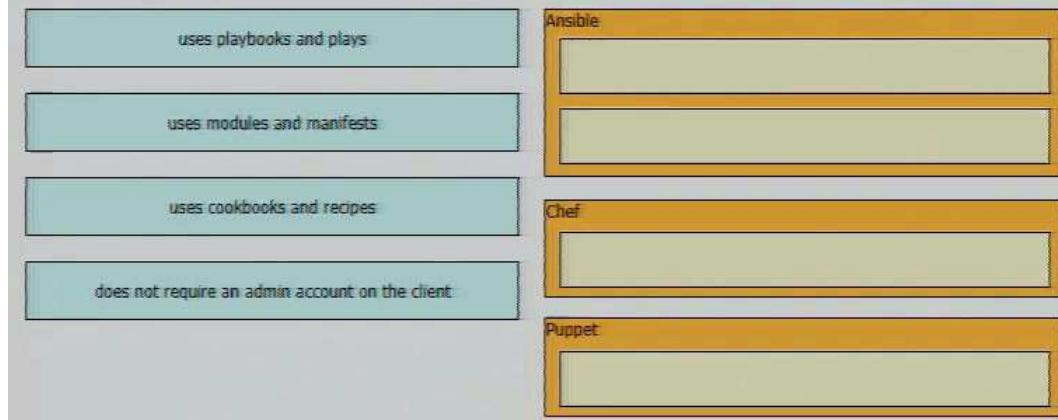
- A. uses playbooks and plays
- B. uses modules and manifests
- C. uses cookbooks and recipes
- D. does not require an admin account on the client

**Correct Answer:** AD

**Section:** Selected

**Explanation**

**Explanation/Reference:**



Based on the naming of the configuration:

"playbooks and "plays" --> "Ansible"

"modules and manifests" --> "Puppet"

"cookbooks and recipes" --> "Chef"

Since it is a drag and drop question and Ansible requires two answers, the remaining choice "does not require admin account on the client" is assigned to Ansible. However, in most cases, admin account is actually required in Ansible client.

**QUESTION 1152**

Which is the correct automation characteristic for Chef but not a characteristic for Puppet?

- A. uses playbooks and plays
- B. uses modules and manifests
- C. uses cookbooks and recipes
- D. does not require an admin account on the client

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1153**

Which is the correct automation characteristic for Puppet?

- A. uses playbooks and plays
- B. uses modules and manifests
- C. uses cookbooks and recipes
- D. does not require an admin account on the client

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1154**

Which tag defines the roaming domain and properties of an AP deployment?

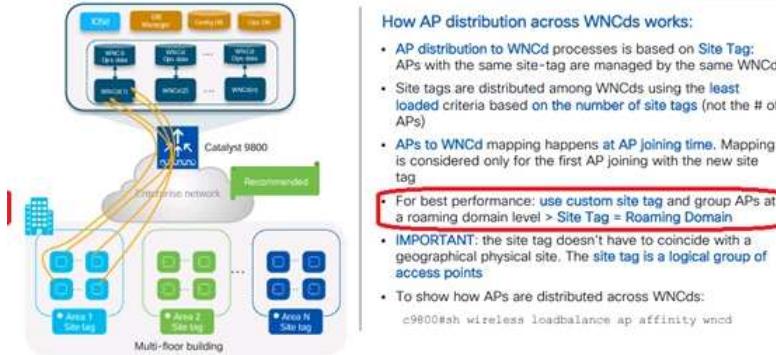
- A. RF tag
- B. policy tag
- C. AP tag
- D. site tag

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**



#### QUESTION 1155

What is required for a VXLAN tunnel endpoint to operate?

- a VXLAN network identifier
- at least one IP for the transit network and one IP for endpoint connectivity
- at least one Layer 2 interface and one Layer 3 interface
- a VXLAN tunnel endpoint identifier

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

#### QUESTION 1156

What is the function of the statement "import actions" in this script?

**import actions**

```
if process =='http':
    actions.http(site)
```

- It imports the functions that are not available natively in Python.
- It imports the functions of a third-party module.
- It imports an external reference.
- It imports a Python module.

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

"import actions" imports a Python module (may be a third party). Then you can use the imported module to access its functions by entering e.g. "actions.http(site)".

**Remarks:**

Python can also support the importing of functions through "from ... import ...".

- importing a specific function from a module e.g. "from actions import http"

- importing all functions from a module "from actions import \*"

When function(s) are imported in either one of the above ways, you can use the imported function e.g. "http(site)" directly.

#### QUESTION 1157

To support new clients in the environment, an engineer must enable Fast Transition on the corporate WLAN. Which command must be applied on a Cisco Catalyst 9800 Series WLC?

- security ft adaptive
- security wpa akm psk
- security wpa akm dot1x
- security wpa akm ft psk

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

```
config wlan security ft { adaptive | enable | disable} wlan-id
```

#### QUESTION 1158

Which tag/profile on a Cisco Catalyst 9800 Series WLC must be modified to allow Cisco ISE to dynamically assign VLANs to users on an 802.1X-based SSID?

- site tag
- interface tag
- WLAN profile
- policy profile

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

#### QUESTION 1159

A corporate policy mandates that a certificate-based authentication system must be implemented on the wireless infrastructure. All corporate clients will contain a certificate that will be used in conjunction with ISE and user credentials to perform authentication before the clients are allowed to connect to the corporate Wi-Fi. Which authentication key option must be selected to ensure that this authentication can take place?

- A. none
- B. PSK
- C. 802.1x
- D. CCKM

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

802.1x can be used with EAP-TLS in order to support certificate authentication.

#### QUESTION 1160

Which method requires a client to authenticate and has the capability to function without encryption?

- A. open
- B. PSK
- C. WEP
- D. WebAuth

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

WebAuth is a Layer 3 Security. It is an authentication method without encryption.

In order to encrypt client traffic, you have to combine it with layer 2 security e.g. PSK or 802.1x. However, the client also needs to enter the PSK or go through 802.1x authentication as well.

#### QUESTION 1161

What does a next-generation firewall that is deployed at the data center protect against?

- A. signature-based malware
- B. zero-day attacks
- C. DMZ web server vulnerabilities
- D. DDoS

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Cisco Firepower correlates all intrusion events to an impact of the attack, telling the operator what needs immediate attention. The assessment relies on information from passive device discovery, including OS, client and server applications, vulnerabilities, file processing, and connection events, etc.

#### QUESTION 1162

When deploying a Cisco Unified Wireless solution, what is a design justification for using a distributed WLC deployment model?

- A. It reduces the number of WLCs that network administrators must support, by locating them in a common location.

- B. It more evenly distributes MAC, ARP, and ND processing over multiple switches which helps with scalability.
- C. The number of wireless clients is low, and the size of the physical campus is small.
- D. There are no latency concerns about LWAPP and CAPWAP tunnels traversing the campus core network.

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

As a best practice Cisco recommends distributing the WLCs for large campus deployments supporting 25,000 or more wireless clients. Distributing the WLCs spreads the MAC, ARP and ND processing and table maintenance between the distribution layer switches reducing CPU load.

#### QUESTION 1163

Which protocol is used by vManage to push centralized policies to vSmart controllers?

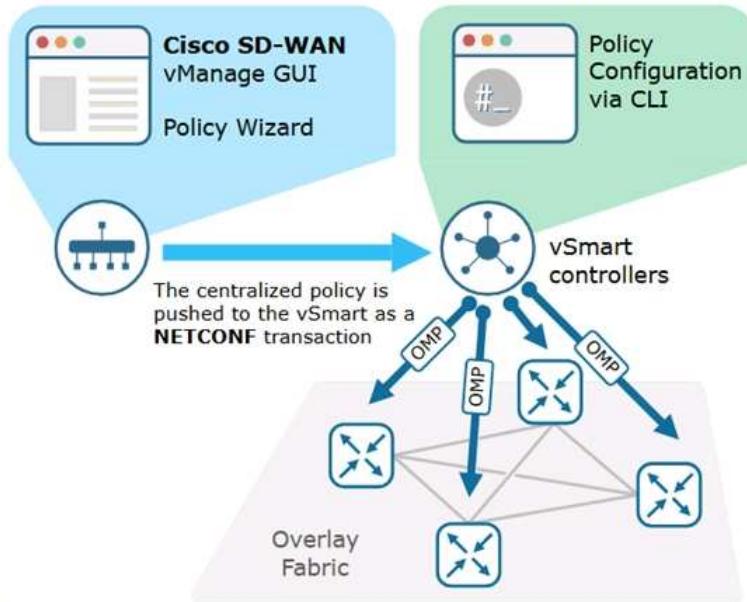
- A. NETCONF
- B. TLS
- C. STUN
- D. OMP

**Correct Answer:** A

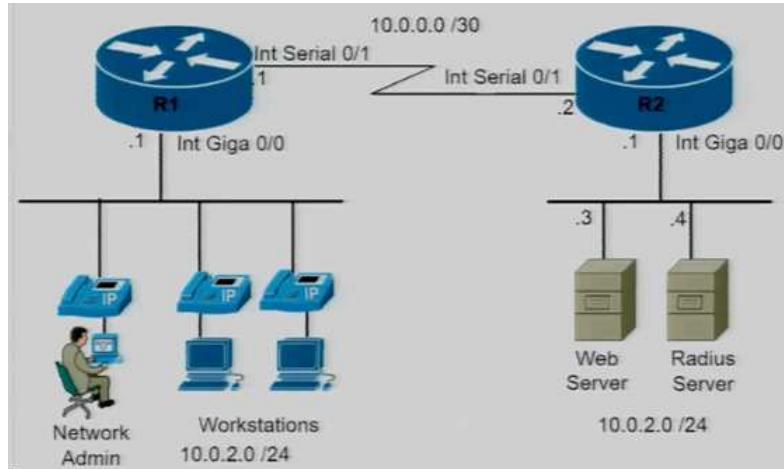
**Section:** Selected

**Explanation**

**Explanation/Reference:**



#### QUESTION 1164



Which command set is required on router R1 to allow the network administrator to authenticate via RADIUS?

- A. aaa new-model  
aaa authentication login console
- B. aaa new-model  
aaa authentication login default group radius
- C. aaa new-model  
aaa authorization exec default group radius
- D. aaa new-model  
aaa authentication login default

**Correct Answer:** B

**Section: Selected**  
**Explanation**

**Explanation/Reference:**

**QUESTION 1165**

What is a characteristic of VRRP?

- A. It is a Cisco proprietary protocol.
- B. It ensures symmetric traffic flow upstream and downstream.
- C. It uses a virtual IP address and a virtual MAC address to achieve redundancy.
- D. It inherently balances load amongst the available gateways.

**Correct Answer: C**

**Section: Selected**  
**Explanation**

**Explanation/Reference:**

VRRP is an open standard IEEE protocol (while HSRP and GLBP are Cisco proprietary protocols).

Remarks:

All First Hop Redundancy Protocols uses virtual IP and MAC address.

**QUESTION 1166**

Which AP mode allows administrators to generate pcap files to use for troubleshooting?

- A. Sniffer
- B. Local
- C. H-REAP
- D. Monitor

**Correct Answer: A**

**Section: Selected**  
**Explanation**

**Explanation/Reference:**

**QUESTION 1167**

How does a Type 2 hypervisor function?

- A. It runs directly on a physical server and includes its own operating system.
- B. It is installed as an application on an already installed operating system.
- C. It runs on a virtual server and includes its own operating system.
- D. It enables other operating systems to run on it.

**Correct Answer: B**

**Section: (none)**  
**Explanation**

**Explanation/Reference:**

**QUESTION 1168**

What is a characteristic of VXLAN?

- A. It extends Layer 2 and Layer 3 overlay networks over a Layer 2 underlay.
- B. Its frame encapsulation is performed by MAC-in-UDP.
- C. It has a 12-byte packet header.
- D. It uses TCP for transport.

**Correct Answer: B**

**Section: Selected**  
**Explanation**

**Explanation/Reference:**

VXLANs enable you to extend Layer 2 networks across the Layer 3 infrastructure by using MAC-in-UDP encapsulation and tunneling. A VXLAN uses a 24-bit segment ID called the VXLAN network identifier (VNID).

**QUESTION 1169**

A new security policy dictates that all corporate wireless devices must authenticate using an EAP method that uses a certificate and user credentials. Wireless devices will be allowed to attempt EAP key negotiation twice. More attempts will cause the authentication to fail. Which configuration must be applied?

- A. EAP-Identity Request Max Retries
- B. EAP-Identity Request Timeout
- C. EAPOL-Key Timeout
- D. EAPOL-Key Max Retries

**Correct Answer: D**

**Section: Selected**  
**Explanation**

**Explanation/Reference:**

**QUESTION 1170**

An engineer is implementing a new SSID on a Cisco Catalyst 9800 Series WLC, which must be advertised on the 6 GHz radios. Users authenticate using a computer certificate. Which wireless Layer 2 security method must be used to support the requirements?

- A. WPA3 Personal
- B. WPA3 Enterprise
- C. WPA2 Enterprise
- D. WPA2 Personal

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1171**

What is a characteristic of omnidirectional antennas?

- A. They include dish antennas.
- B. They have high gain.
- C. They are well suited for point-to-multipoint environments.
- D. They provide the most focused and narrow beamwidth

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 1172**

In a Cisco Mobility Express wireless deployment. Which AP takes over if the primary AP fails?

- A. AP with highest controller up time
- B. AP with the lowest IP address
- C. AP with lowest MAC address
- D. AP with highest IP address

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

To have redundancy in the Mobility Express network, it must have two or more Mobility Express capable Access Points. When an active Primary Access Point fails, the election process gets initiated and it elects the Access Point with the highest priority as the Primary AP.

The Primary AP election priorities are as follows:

1. User Defined Primary—User can select an Access Point to be the Primary Access Point. If such a selection is made, no new Primary will be elected in case of a reboot of the Primary Access Point. After five minutes, if the current Primary is still not active, it will be assumed dead and Primary Election will begin to elect a new Primary.
2. Most capable Access Point- If the user priority is not set, Primary AP Election algorithm will select the new Primary based on capability of the Access Point. For example, 3800 is the most capable followed by 2800 and then 1850 and finally 1830.
3. Least Client Load—if there are multiple Access Points with the same capability i.e. multiple 3800 Access points, the one with least client load is elected as the Primary AP.
4. Lowest MAC Address—if the User defined priority is not configured and everything else is the same, then Access Point with the lowest MAC gets elected as the Primary AP.

**QUESTION 1173**

Which multicast operational mode sends a PIM prune message toward the source after receiving unsolicited traffic when there is no connected receiver or downstream PIM neighbor?

- A. PIM dense mode
- B. IGMPv3
- C. PIM sparse mode
- D. IGMPv2

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Although both Dense mode and Sparse mode use Prune messages, Prune messages are sent towards the RP in Sparse mode.

**QUESTION 1174**

What are two characteristics of Cisco Catalyst SD-WAN? (Choose two.)

- A. centralized reachability, security, and application policies
- B. unified data plane and control plane
- C. control plane operates over DTLS/TLS authenticated and secured tunnels
- D. time-consuming configuration and maintenance
- E. distributed control plane

**Correct Answer:** AC

**Section:** Selected

**Explanation**

**Explanation/Reference:**

SD-WAN separate the control plane from the data plane, therefore the two are not unified.

**QUESTION 1175**

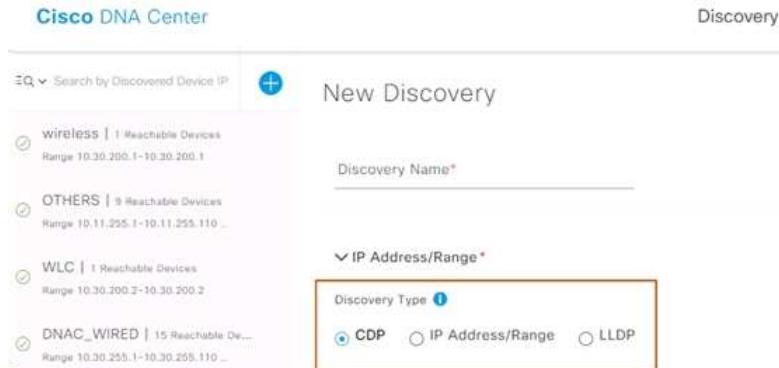
Which protocol does Cisco Catalyst Center (formerly DNA center) SDK use to discover the topology of non-Cisco devices in a network?

- A. LLDP

- B. Telnet
- C. CDP
- D. SSH

**Correct Answer:** A  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**



The screenshot shows the Cisco DNA Center interface under the 'Discovery' tab. At the top, there's a search bar labeled 'Search by Discovered Device IP' and a 'New Discovery' button. Below these are several device categories with their counts: 'wireless' (1 Reachable Devices, Range 10.30.200.1-10.30.200.1), 'OTHERS' (9 Reachable Devices, Range 10.11.255.1-10.11.255.110 ...), 'WLC' (1 Reachable Devices, Range 10.30.200.2-10.30.200.2), and 'DNAC\_WIRED' (15 Reachable Devices, Range 10.30.255.1-10.30.255.110 ...). A highlighted section shows the 'Discovery Type' dropdown with three options: 'CDP' (selected), 'IP Address/Range', and 'LLDP'. The 'IP Address/Range' option is preceded by a checkmark and the text 'IP Address/Range\*'. The 'Discovery Name\*' field is empty.

**QUESTION 1176**

Which characteristic applies to Cisco SD-Access?

- A. It uses dynamic routing to discover and provision the border and edge switches
- B. It uses VXLAN for the control plane
- C. It uses GRE for the policy plane
- D. It uses PnP to discover and provision border and access switches

**Correct Answer:** D  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

The PnP agent is a Cisco Catalyst switch with factory-default settings. The switch leverages the built-in day-0 mechanism to communicate with Catalyst Center and support the integrated PnP server function. Catalyst Center dynamically builds the PnP profile and configuration sets that enable complete day-0 automation.

**QUESTION 1177**

Which framework is used for third-party authorization?

- A. custom tokens
- B. API keys
- C. OAuth
- D. SOAP

**Correct Answer:** C  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

**QUESTION 1178**

Which feature allows clients to perform Layer 2 roaming between wireless controllers?

- A. mobility groups
- B. RF grouping
- C. N+1 high availability
- D. SSO

**Correct Answer:** A  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

**QUESTION 1179**

What is modularity in network design?

- A. ability to scale and accommodate future needs of the network
- B. ability to self-heal the network to prevent service outages
- C. ability to create self-contained, repeatable sections of the network
- D. ability to bundle several functions into a single layer of the network

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

As the complexity of the network increased to meet these demands, it became necessary to adjust the network design to one that uses a more modular approach. A modular network design separates the network into various functional network modules, each targeting a specific place or purpose in the network. The modules represent areas that have different physical or logical connectivity.

**QUESTION 1180**

Which action occurs during a Layer 3 roam?

- A. The client is marked as "Foreign" on the original controller
- B. The client database entry is moved from the old controller to the new controller
- C. Client traffic is tunneled back to the original controller after a Layer 3 roam occurs
- D. The client receives a new IP address after authentication occurs

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1181**

Which solution should be used in a high-density wireless environment to increase bandwidth for each user?

- A. increase antenna size
- B. increase the cell size of each AP
- C. increase TX power
- D. increase the mandatory minimum data rate

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1182**

How does IGMP function with multicast routing and PIM?

- A. IGMP is enabled automatically when multicast routing and PIM are configured on a router.
- B. IGMP is incompatible with multicast routing.
- C. IGMP must be enabled manually when multicast routing and PIM are configured on a router.
- D. IGMP is incompatible with PIM.

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Enabling PIM on an interface also enables IGMP. IGMP provides a means to automatically control and limit the flow of multicast traffic throughout your network with the use of special multicast queriers and hosts.

**QUESTION 1183**

In a virtual environment, what is an OVA file?

- A. A file containing information about snapshots of a virtual machine.
- B. A configuration file containing settings for a virtual machine such as a guest OS.
- C. A file containing a virtual machine disk drive.
- D. A zip file connecting a virtual machine configuration file and a virtual disk.

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1184**

Which IEEE standard provides the capability to permit or deny network connectivity based on the user or device identity?

- A. 802.1d
- B. 802.1q
- C. 802.1w
- D. 802.1x

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1185**

Which two nodes comprise a collapsed core in a two-tier Cisco SD-Access design? (Choose two.)

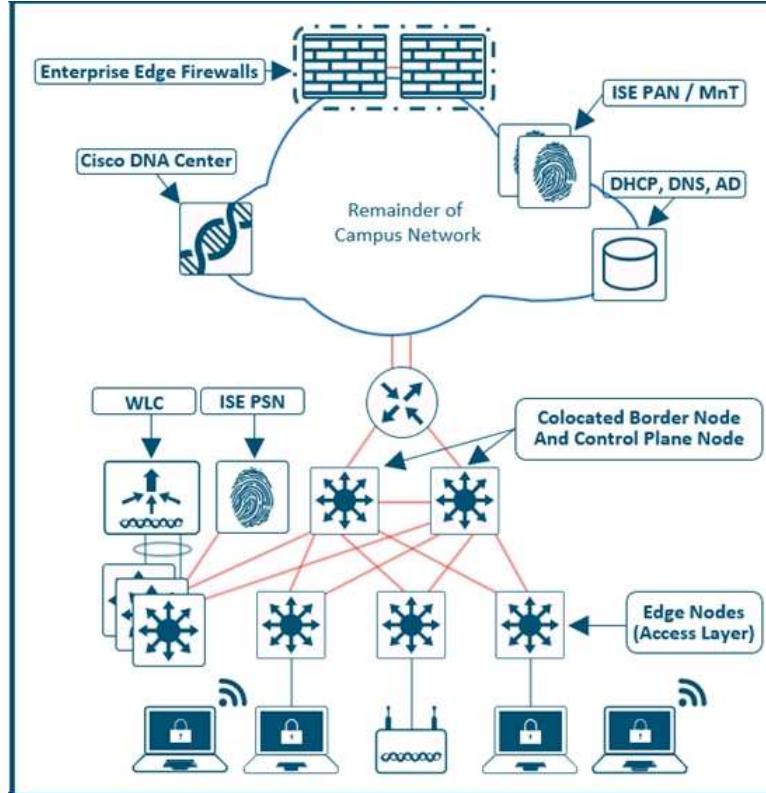
- A. border nodes
- B. distribution nodes
- C. edge nodes
- D. extended nodes
- E. core nodes

**Correct Answer:** AC

**Section:** Selected

## Explanation

### Explanation/Reference:



For smaller deployments, an SD-Access fabric site is implemented using a two-tier design. The same design principles for a three-tier network applicable, though there is no need for an aggregation layer (intermediate nodes). In a small site, high availability is provided in the fabric nodes by colocating the border node and control plane node functionality on the collapsed core switches and deploying these as a pair.

### QUESTION 1186

Why would a network engineer configure an AP in SE-Connect mode?

- A. to monitor the VLAN traffic for rogue APs
- B. to redirect WLAN traffic to an endpoint for protocol analysis
- C. to analyze the RF spectrum surrounding the AP
- D. to connect the wired LAN with the wireless infrastructure

**Correct Answer: C**

**Section: Selected**

**Explanation**

### Explanation/Reference:

### QUESTION 1187

Which feature provides data-plane security for Cisco Catalyst SD-WAN networks?

- A. IPS
- B. SSH
- C. IPsec
- D. TLS/DTLS

**Correct Answer: C**

**Section: Selected**

**Explanation**

### Explanation/Reference:

### QUESTION 1188

Which DNS record type is needed to allow a Cisco AP to discover a WLC when using IPV4?

- A. CNAME record
- B. NS record
- C. A record
- D. SOA record

**Correct Answer: C**

**Section: Selected**

**Explanation**

### Explanation/Reference:

### QUESTION 1189

What are two of benefits of using VXLAN? (Choose two.)

- A. It has fewer devices to manage.
- B. It allows for an unlimited number of segments.
- C. It uses a MAC in IP/TCP encapsulation technique.
- D. It uses all available Layer 3 paths in the underlying network.
- E. It allows multi-tenanted segmentation.

**Correct Answer:** CE

**Section:** Selected

**Explanation**

**Explanation/Reference:**

VXLANs enable you to extend Layer 2 networks across the Layer 3 infrastructure by using MAC-in-UDP encapsulation and tunneling. In addition, you can use a VXLAN to build a multitenant data center by decoupling tenant Layer 2 segments from the shared transport network.

**QUESTION 1190**

```
from requests.auth import HTTPBasicAuth
import requests

ROUTER="192.0.2.1"
BASEURI="restconf/data/Cisco-IOS-XE-native:native"
SUBURI="router/router-bgp"

response = requests.get(
    f"https://(ROUTER)/(BASEURI)/(SUBURI)",
    auth=HTTPBasicAuth('admin', 'S3cr3tP4ss'),
    verify=False)

print(f"HTTP Response: {response.status_code} ({response.reason})\n")
print(response.text)
```

---

```
admin@linux:/tmp$ python3 get-bgp.py
HTTP Response: 404 Not Found

<errors xmlns="urn:ietf:params:xml:ns:yang:ietf-restconf">
  <error>
    <error-message>uri keypath not found</error-message>
    <error-tag>invalid-value</error-tag>
    <error-type>application</error-type>
  </error>
</errors>
admin@linux:/tmp$
```

An engineer is creating a Python script to fetch the BGP configuration from a device using RESTCONF. What does the output indicate?

- A. The BGP data resource identifier in the URI is incorrect.
- B. The HTTPS connection to the device could not be established.
- C. There is no BGP process running on the device.
- D. RESTCONF is not enabled on the device.

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1191**

Which tag defines the properties to be applied to each specific WLAN?

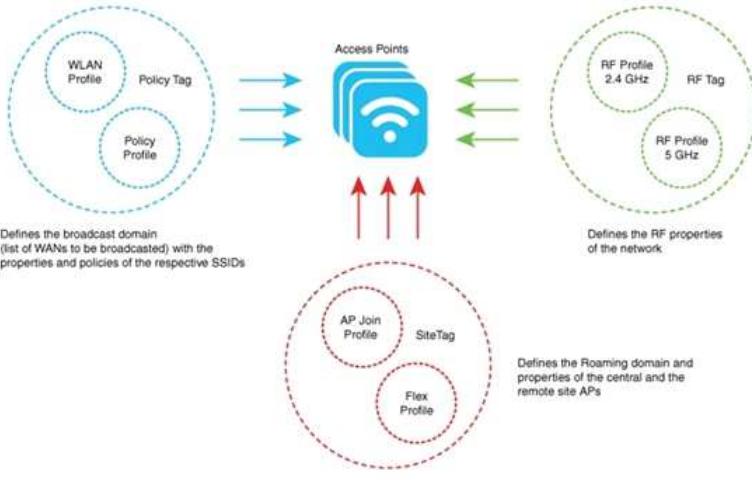
- A. policy tag
- B. AP tag
- C. RF tag
- D. site tag

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**



#### QUESTION 1192

Which location tracking method is used when locating client devices using Cisco hyperlocation?

- A. location patterning
- B. line of sight
- C. TTL
- D. angle of arrival

**Correct Answer: D**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

The Hyperlocation methodology of calculating location using Angle of Arrival (AoA) tracks 802.11 OFDM clients (meaning 802.11a/g/n/ac clients) that are associated (connected) on the network and is able to do so with much higher accuracy than conventional Real Time Location Systems (RTLS) that rely on only RSSI (RF Signal Strength).

#### QUESTION 1193

Which are the correct Cisco Catalyst Center (formerly DNA Center) southbound API characteristics? (Choose three.)

- A. uses XML exclusively
- B. multivendor focus
- C. uses JSON exclusively
- D. referred to as Intent API
- E. supports NETCONF, SSH, SNMP, and others
- F. extendable by device packages

**Correct Answer: BEF**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

#### QUESTION 1194

Which feature does the Cisco Catalyst Center (formerly DNA Center) User-Defined Network workflow provide?

- A. automatic segmentation of IoT devices
- B. automatic provisioning of AP devices
- C. replacement of malfunctioning devices
- D. interface for AP configuration

**Correct Answer: A**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

The User-Defined Network service provides the following solution:

- Easy and secure onboarding of client devices.
- Automatic segmentation of client devices that belong to a particular user.
- Ability to invite other users to share their devices.

#### QUESTION 1195

Which feature is needed to maintain the IP address of a client when an inter-controller Layer 3 roam is performed between two WLCs that are using different mobility groups?

- A. AAA override
- B. auto anchor
- C. RF groups
- D. interface groups

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 1196**

Which AAA wireless authentication method uses MAB and a PSK av-pair to complete the authentication?

- A. WPA2-Personal
- B. WPA2-Enterprise
- C. iPSK
- D. EAP-TLS

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

iPSK solution:

During client authentication, the AAA server would authorize the client mac address and send the passphrase (if configured) as part of the Cisco-AVPair list. The WLC would receive this as part of the radius response and would process this further for the computation of PSK.

**QUESTION 1197**

What is one characteristic of an AP that is operating in Mobility Express mode?

- A. it requires an AP to act as a WLC.
- B. it requires a centralized WLC.
- C. At least three APs are needed for WLC redundancy.
- D. it is recommended for large scale deployments.

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1198**

Which method does FastLocate use to collect location-based information?

- A. beacons
- B. client probing
- C. data packets
- D. RFID

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

FastLocate enables higher location refresh rates by collecting RSSI or location information through data packets received by the APs.

**QUESTION 1199**

Router A

```
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# ip address 10.1.0.1 255.0.0.0
Router(config-if)# vrrp 1 priority 100
Router(config-if)# vrrp 1 authentication cisco
Router(config-if)# vrrp 1 timers advertise 3
Router(config-if)# vrrp 1 timers learn
Router(config-if)# vrrp 1 ip 10.1.0.10
```

Router B

```
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# ip address 10.1.0.2 255.0.0.0
Router(config-if)# vrrp 1 priority 110
Router(config-if)# vrrp 1 authentication cisco
Router(config-if)# vrrp 1 timers advertise 3
Router(config-if)# vrrp 1 timers learn
Router(config-if)# vrrp 1 ip 10.1.0.11
```

An engineer must adjust the configuration so that Router A becomes the active router. Which two commands should be applied to Router A? (Choose two.)

- A. vrrp 1 ip 10.1.0.11
- B. vrrp 1 timers advertise 1
- C. vrrp 1 priority 120
- D. ip address 10.1.0.11 255.0.0.0
- E. vrrp 1 priority 90

**Correct Answer:** AC

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Other than configuring a higher priority i.e. 120, the Virtual IP configured for the two routers must be the same. (Note that VRRP has the preemption enabled by default.)

**QUESTION 1200**

What is used by vManage to interact with Cisco Catalyst SD-WAN devices in the fabric?

- A. IPsec
- B. RESTCONF
- C. northbound API
- D. southbound API

**Correct Answer: D**  
Section: Selected  
Explanation

Explanation/Reference:

**QUESTION 1201**

Which two benefits result from a network design that uses small and repeatable sections? (Choose two.)

- A. lower monitoring requirements
- B. improved throughput
- C. scalability
- D. low latency
- E. quick failure isolation

**Correct Answer: CE**  
Section: Selected  
Explanation

Explanation/Reference:

**QUESTION 1202**

An engineer must configure a new 6 GHz only SSID on a Cisco Catalyst 9800 Series WLC, with these requirements:

- Provide 802.11ax data rates for supported devices.
- All users authenticate using a certificate.

Which wireless Layer 2 security mode meets the requirements?

- A. WPA3 Enterprise
- B. WPA2 Enterprise
- C. WPA3 Personal
- D. WPA2 Personal

**Correct Answer: A**  
Section: Selected  
Explanation

Explanation/Reference:

**QUESTION 1203**

Edit WLAN

General		Security		Advanced		Add To Policy Tags	
Coverage Hole Detection	<input checked="" type="checkbox"/>	Universal Admin	<input type="checkbox"/>	Aironet IE	<input type="checkbox"/>	OKC	<input checked="" type="checkbox"/>
Advertise AP Name	<input type="checkbox"/>	Load Balance	<input type="checkbox"/>	P2P Blocking Action	Disabled	Band Select	<input type="checkbox"/>
Multicast Buffer	<input checked="" type="checkbox"/> DISABLED	IP Source Guard	<input type="checkbox"/>	Media Stream Multicast-direct	<input type="checkbox"/>	WMM Policy	Allowed
11ac MU-MIMO	<input checked="" type="checkbox"/>	mDNS Mode	Gateway	WiFi to Cellular Steering	Off Channel Scanning Defer		
Max Client Connections				Defer Priority	<input type="checkbox"/> 0	<input checked="" type="checkbox"/> 1	<input checked="" type="checkbox"/> 2
Per WLAN	0	3	4	5	<input type="checkbox"/>	<input checked="" type="checkbox"/> 5	
Per AP Per WLAN	0	6	7		<input type="checkbox"/>	<input checked="" type="checkbox"/> 7	
Per AP Radio Per WLAN	200	Scan Defer Time	100				

A customer reports occasional brief audio dropouts on its Cisco Wi-Fi phones. The environment consists of a Cisco Catalyst 9800 Series WLC with Catalyst 9120 APs running RRM. The phones connect on the 5-GHz band. Which action resolves this issue?

- A. Disable Coverage Hole Detection
- B. Enable Defer Priority 6.
- C. Set WMM Policy to Required.
- D. Enable Media Stream Multicast-direct.

**Correct Answer: B**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

RRM automatically detects and configures new controllers and lightweight access points as they are added to the network. It then automatically adjusts associated and nearby lightweight access points to optimize coverage and capacity.

A lightweight access point, in normal operational conditions, periodically goes off-channel and scans another channel. This is in order to perform RRM operations such as the following:

- Transmitting and receiving Neighbor Discovery Protocol (NDP) packets with other APs.
- Detecting rogue APs and clients.
- Measuring noise and interference.

During the off-channel period, which normally is about 70 milliseconds, the AP is unable to transmit or receive data on its serving channel. Therefore, there is a slight impact on its performance and some client transmissions might be dropped.

While the AP is sending and receiving important data, it is possible to configure off-channel scanning deferral so that the AP does not go off-channel and its normal operation is not impacted. You can configure off-channel scanning deferral on a per-WLAN basis, per WMM UP class basis, with a specified time threshold in milliseconds. If the AP sends or receives, on a particular WLAN, a data frame marked with the given UP class within the specified threshold, the AP defers its next RRM off-channel scan.

By default, phone audio data is marked with WMM UP Class 6. Therefore, the box "6" has to be checked.

**QUESTION 1204**

Drag and drop the configuration management tools from the left onto the configuration styles they use on the right.

Which is the correct configuration management tool for "Procedural"?

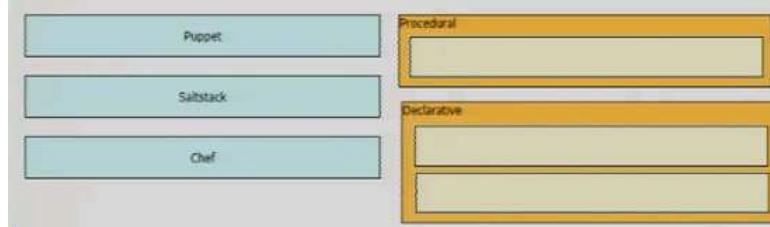
- A. Puppet
- B. Saltstack
- C. Chef

**Correct Answer: C**

**Section: Selected**

**Explanation**

**Explanation/Reference:**



**QUESTION 1205**

Drag and drop the configuration management tools from the left onto the configuration styles they use on the right.

Which are the correct configuration management tools for "Declarative" ? (Choose two.)

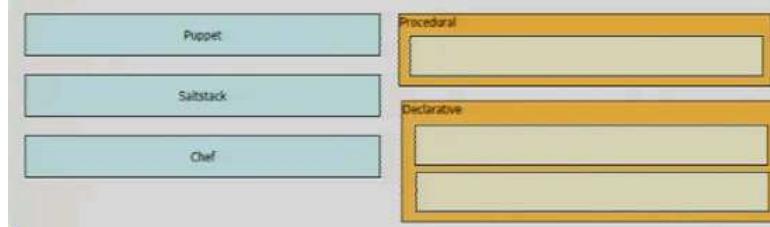
- A. Puppet
- B. Saltstack
- C. Chef

**Correct Answer: AB**

**Section: Selected**

**Explanation**

**Explanation/Reference:**



**QUESTION 1206**

What is one characteristic of Cisco SD-Access networks?

- A. Virtual networks are used for microsegmentation.
- B. Devices are assigned to virtual networks based on their VLAN membership.
- C. Scalable group tags are used for macrosegmentation
- D. All traffic is Layer 3 within the fabric.

**Correct Answer: B**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

**Macro segmentation** is accomplished using **Virtual Networks** (VN's). Virtual networks provide complete isolation between traffic and devices in one VN and those in other VNs. Within the SD-Access fabric, information identifying the virtual network is carried in the VXLAN Network Identifier (VNI) field within the VXLAN header.

**Micro segmentation** simplifies the provisioning and management of network access control using groups to classify network traffic and enforce policies. This allows more granular security policies within the virtual networks in an SD-Access fabric. Cisco Group-Based Policy **SGTs** provide logical segmentation based on group membership. Cisco Group-Based Policy provides an additional layer of granularity, allowing you to use multiple SGTs within a single VN providing micro-segmentation within the VN.

**QUESTION 1207**

```
Router# show running-config
! lines omitted for brevity

username cisco password 0 cisco
aaa authentication login group1 group radius line
line con 0
password 0 cisco123
login authentication group1
line vty 0 4
password 0 cisco111
```

Authentication for users must first use RADIUS, and fall back to the local database on the router if the RADUS server is unavailable. Which two configuration sets are needed to achieve this result? (Choose two.)

- A. aaa authentication login group2 group radius local
- B. line vty 0 4  
  login authentication group2
- C. aaa authentication login group2 group radius enable
- D. line con 0  
  login authentication group2
- E. aaa authentication login group2 group radius none

**Correct Answer:** AB

**Section:** Selected

**Explanation**

**Explanation/Reference:**

For applying the new login authentication list "group2", there are two choices. However, applying "group2" to line vty seems to be more logical if the authentication list is configured for "users".

**QUESTION 1208**

Drag the command snippets from the bottom onto the boxes to create an EEM script to enable OSPF debugging in the event the OSPF neighborship goes down. Options may be used more than once.

**Select and Place:**

event [ ]	ENABLE_OSPF_DEBUG
event [ ]	"%OSPF-5-ADJCHG: Process 6, Nbr 192.168.10.1 on Serial0/0 from FULL to DOWN"
action 1.0 [ ]	"enable"
action 2.0 [ ]	"debug ip ospf event"
action 3.0 [ ]	"debug ip ospf adj"
action 4.0 [ ]	priority informational msg "ENABLE_OSPF_DEBUG"

[manager applet](#)   [syslog pattern](#)   [di command](#)   [syslog priority](#)

**Correct Answer:**

event [ ] manager applet	ENABLE_OSPF_DEBUG
event [ ] syslog pattern	"%OSPF-5-ADJCHG: Process 6, Nbr 192.168.10.1 on Serial0/0 from FULL to DOWN"
action 1.0 [ ] di command	"enable"
action 2.0 [ ] di command	"debug ip ospf event"
action 3.0 [ ] di command	"debug ip ospf adj"
action 4.0 [ ] syslog priority	priority informational msg "ENABLE_OSPF_DEBUG"

[manager applet](#)   [syslog pattern](#)   [di command](#)   [syslog priority](#)

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 1209**

```

import requests

def get_device_info(device_ip):
    url = f"http://{device_ip}/api/device/info"
    response = requests.get(url)
    if response.status_code == 200:
        return response.json()
    else:
        return "Error: Unable to retrieve device information."

device_ip = "192.168.100.1"
device_info = get_device_info(device_ip)
print(device_info)

```

When this Python script, which uses the requests module to communicate with a network device, is executed, what is the anticipated result?

- A. The script retrieves device information by sending HTTP requests to the device's API endpoints.
- B. The script configures network device settings by establishing a secure connection with the device.
- C. The script establishes an SSH connection with the network device.
- D. The script parses JSON data received from the network device to format it into a tabular structure.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Printing the JSON response received does NOT format the printout data in tabular structure.

#### QUESTION 1210

Drag and drop the wireless elements on the left to their definitions on the right.

**Select and Place:**

beamwidth	a graph that shows the relative intensity of the signal strength of an antenna within its space
polarization	the relative increase in signal strength of an antenna in a given direction
radiation patterns	measures the angle of an antenna pattern in which the relative signal strength is half-power below the maximum value
gain	radiated electromagnetic waves that influence the orientation of an antenna within its electromagnetic field

**Correct Answer:**

	radiation patterns
	gain
	beamwidth
	polarization

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 1211

What is a characteristic of omnidirectional antennas?

- A. it includes dipole antennas
- B. it includes dish antennas
- C. it provides the most focused and narrow beamwidth
- D. it has high gain

**Correct Answer:** A  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

**QUESTION 1212**

What is the measure of the difference between the received signal and the noise floor in a wireless environment?

- A. XOR
- B. SNR
- C. RSSI
- D. RRM

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 1213**

Drag and drop the command snippets from the bottom onto the boxes to configure an EEM applet to enable a previously shutdown interface and send an alert to alert@cisco.com.

**Select and Place:**

		Enable_Interface_And_Alert
		"Interface GigabitEthernet0/1, changed state to administratively down"
action 1.0 cli command "enable"		
action 2.0 cli command "configure terminal"		
action 3.0 cli command "interface GigabitEthernet0/1"		
action 4.0 cli command "no shutdown"		
action 5.0 cli command "end"		
action 6.0	mail server	"smtp.cisco.com" to "alert@cisco.com" from "router@cisco.com" subject "Int G0/1 Enabled" body "GigabitEthernet0/1 was shutdown and has been enabled."
pattern event manager mail server event syslog applet		

**Correct Answer:**

event manager	applet	Enable_Interface_And_Alert
event syslog	pattern	"Interface GigabitEthernet0/1, changed state to administratively down"
action 1.0 cli command "enable"		
action 2.0 cli command "configure terminal"		
action 3.0 cli command "interface GigabitEthernet0/1"		
action 4.0 cli command "no shutdown"		
action 5.0 cli command "end"		
action 6.0	mail server	"smtp.cisco.com" to "alert@cisco.com" from "router@cisco.com" subject "Int G0/1 Enabled" body "GigabitEthernet0/1 was shutdown and has been enabled."

**Section:** Selected  
**Explanation**

**Explanation/Reference:**

**QUESTION 1214**

Which AP mode only scans other channels to measure noise and interference, discover rogue devices, and check for IDS events?

- A. sniffer
- B. mesh
- C. monitor
- D. local

**Correct Answer:** C  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

**QUESTION 1215**

What is the primary responsibility of the vBond orchestrator?

- A. to facilitate start-up by performing authentication and authorization of all elements into the network

- B. to provide configuration synchronization of all WAN Edge devices
- C. to provide centralized management and provisioning of all elements into the network
- D. to configure NAT communication on WAN Edge routers

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1216**

Drag and drop the characteristics of Cisco Catalyst SD-WAN from the left onto the right. Not all options are used. Which are the correct characteristics for "Cisco Catalyst SD-WAN"? (Choose three.)

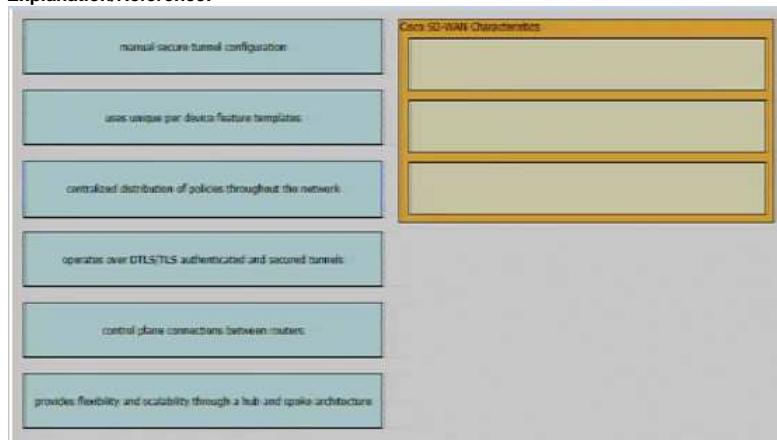
- A. manual secure tunnel configuration
- B. uses unique per device feature templates
- C. centralized distribution of policies throughout the network
- D. operates over DTLS/TLS authenticated and secured tunnels
- E. control plane connections between routers
- F. provides flexibility and scalability through a hub and spoke architecture

**Correct Answer:** CDF

**Section:** Selected

**Explanation**

**Explanation/Reference:**



- A feature template can be applied to multiple devices (instead of per device template)
- Each Cisco SD-WAN Controller establishes and maintains a control plane connection with each edge router in the overlay network. If "control plane connections between router" mean a router maintain a control plane connection with another router, then it is not correct.
- Hub-and-spoke configuration simplifies the process of configuring a hub-and-spoke topology, making complex centralized control policy unnecessary. Instead, the configuration requires only a few simple configurations: a single command each on (a) the Cisco SD-WAN Controllers serving a network, (b) a router that serves as a hub, and (c) the routers that operate as spokes. Therefore, hub-and-spoke architecture is more scalable than SD-WAN fully-meshed architecture.

**QUESTION 1217**

Which two components function together in a Cisco SD-Access solution?

- A. Cisco vSmart controller and Cisco Catalyst Center (formerly DNA Center)
- B. Cisco vBond orchestrator and Cisco Catalyst Center (formerly DNA Center)
- C. Cisco ISE and Cisco Catalyst Center (formerly DNA Center)
- D. Cisco campus fabric and Cisco vManage

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

vSmart, vBond and vManager are components of SD-WAN.

**QUESTION 1218**

Which next generation firewall feature supports separate security services for multiple departments?

- A. virtual switch mode to provide traffic inspection capabilities for the flows entering the firewall and dropping packets based on policy configuration
- B. multicontext mode with specific logical or physical interface allocation within each context and grouped into security zones
- C. Layer 3 mode with resource tracking capabilities and automatic configuration synchronization between the nodes and security zones
- D. state sharing mode to track the user data sessions and replication to the neighbor firewall using a failover link

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

You can partition a single security appliance into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management. Some features are not supported, including VPN and dynamic routing protocols.

**QUESTION 1219**

Which technology is the Cisco SD-Access fabric control plane based on?

- A. LISP
- B. IS-IS
- C. VXLAN
- D. Cisco TrustSec

**Correct Answer:** A  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**  
 Overlay control plane – LISP  
 Data plane – VXLAN

#### QUESTION 1220

Which task is mandatory when provisioning a device through the plug-and-play workflow in Cisco Catalyst Center (formerly DNA Center)?

- A. golden image upgrade
- B. stack serial number assignment
- C. site assignment
- D. template configuration application

**Correct Answer:** D  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

#### QUESTION 1221

```
Edge-3#show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID      Local Intf      Hold-time   Capability      Port ID
Core-SW.cisco.lab  Gi0/3        120          R            Gi0/3
Edge-2.cisco.lab  Gi0/2        120          R            Gi0/2
Edge-1.cisco.lab  Gi0/1        120          R            Gi0/1

Total entries displayed: 3
=====
u2= []
client = paramiko.SSHClient()
client.load_system_host_keys()
client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
client.connect('192.168.1.1', port=22, username='cisco', password='cisco', allow_agent=False)
stdin, stdout, stderr = client.exec_command('show lld neighbors\n')
u = 0
for u in stdout:
    if 'Router' not in u and 'Capability' not in u and 'Repeater' not in u:
        if 'Device ID' not in u and 'displayed' not in u:
            u101 = u.split()
            if len(u101) != 0:
                u2.append(u101)
```

What does this code achieve?

- A. It generates a count of the LLDP neighbors.
- B. It generates a list of routers with the Repeater capability
- C. It generates a list of the LLDP neighbors and their capabilities.
- D. It generates a list containing only the hostname of the LLDP neighbor.

**Correct Answer:** C  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

Paramiko is a Python implementation of the SSHv2 protocol, providing both client and server functionality. In the script, the lines with "Router", "Capability", "Repeater", "Device ID" or "displayed" are excluded. For each remaining line (i.e. the 3 lines of the devices forming the table content in the output), it is split into a list of substrings which are the columns / fields (e.g. "Hold-tme", "Capability" ... etc). If the list created for each remaining line is not empty (for excluding the blank line in the output), it is appended to the list "u2".

#### QUESTION 1222

Which architectural component enables a zero-trust security model?

- A. plug-and-play
- B. management plane
- C. data plane
- D. control plane

**Correct Answer:** D  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

The Cisco Catalyst SD-WAN fabric incorporates a zero-trust security model within its control plane, ensuring that all elements of the fabric are authenticated and authorized prior to admittance to the network.

#### QUESTION 1223

Which two Cisco SD-Access components provide communication between traditional network elements and the controller layer? (Choose two.)

- A. network data platform
- B. network control platform

- C. partner ecosystem
- D. network underlay
- E. fabric overlay

**Correct Answer:** AB

**Section:** Selected

**Explanation**

**Explanation/Reference:**

[Cisco Network Control Platform \(NCP\)](#)

The NCP is a subsystem of Cisco DNA Center, and it provides the SDA physical and network layers with fabric and underlay network automation and orchestration services. It configures and manages the network devices using SNMP, SSH/Telnet, NETCONF/YANG, etc. It also provides network automation status and other relevant information to the management layer.

[Cisco Network Data Platform \(NDP\)](#)

The NDP assurance subsystem is directly integrated into the Cisco DNA Center. It collects data, identifies historical trends, and analyzes and correlates network events from various sources, such as SPAN and NetFlow. The collected information provides contextual information for Cisco NCP and ISE. It also provides the management layer's network operational status and other relevant information.

**QUESTION 1224**

Which API does Cisco Catalyst Center (formerly DNA Center) use to retrieve information about images?

- A. Client Health
- B. PnP
- C. Img-Mgmt
- D. SWIM

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

[Software Image Management \(SWIM\)](#) manages software upgrades and controls the consistency of image versions across your network.

**QUESTION 1225**

Which feature works with SSO to continue forwarding packets after a route processor failure until the control plane recovers?

- A. HSRP
- B. ECMP
- C. RSVP
- D. NSF

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1226**

What is a characteristic of a virtual machine?

- A. It shares the host OS kernel, binaries, and libraries
- B. It is more lightweight than a container
- C. It provides an environment completely isolated from the host OS
- D. It is more resource efficient than a container

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1227**

What is the purpose of a data modelling language?

- A. to specify the rules for transcoding between text and binary data encodings
- B. to describe the structure and meaning of exchanged data
- C. to establish a framework to process data by using an object-oriented programming approach
- D. to standardize the procedures that are executed when parsing sent and received data

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**QUESTION 1228**

```

>>> URL="https://dna-center/api/v1/network-device/ip-address/10.0.0.100"
>>> Response = requests.get(URL, headers=Headers, verify=False)
>>> Response.status_code
200
>>> Response.json()['response']['id']
'93f6be77-abc6-1020-8fab-d5c0110bfd81'
>>>
>>> URL="https://dna-center/api/v1/network-device/ip-address/10.0.0.200"
>>> Response = requests.get(URL, headers=Headers, verify=False)
>>> Response.status_code
404
>>> Response.json()['response']['id']
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
KeyError: 'id'

```

What is determined from the output?

- A. 10.0.0.100 is managed by Cisco Catalyst Center (formerly DNA Center).
- B. The authentication for the second query fails.
- C. The URL for the second query is syntactically incorrect.
- D. 10.0.0.200 is known to DNA Center, but its ID is an empty string.

**Correct Answer:** A

**Section:** Selected  
**Explanation**

**Explanation/Reference:**

The 404 (Not found) error in the 2nd HTTPs request means that the device with IP address 10.0.0.200 is not found in DNA center. Therefore, no device information (e.g. "id") can be obtained.

**QUESTION 1229**

Which network design principle should be followed to improve Layer 2 stability in an enterprise campus design?

- A. Extend only required user VLANs throughout the aggregation layer.
- B. Extend only required user VLANs throughout the access layer.
- C. Extend all user VLANs throughout the core layer.
- D. Extend all user VLANs throughout the access layer.

**Correct Answer:** D

**Section:** Selected  
**Explanation**

**Explanation/Reference:**

VLAN extension—The Layer 2 access topology provides the flexibility to extend VLANs between switches that are connected to a common aggregation module. This makes provisioning of servers to a particular subnet/VLAN simple, and without the worry of physical placement of the server in a particular rack or row.

**QUESTION 1230**

An Engineer must create an EEM applet to automate the process of updating the interface descriptions on a switch when it detects a connection to a newly discovered CDP neighbor. The applet should perform these steps:

- Trim the domain from the neighbor's name
- Extract the port ID
- Enter configuration mode
- Update the interface description
- Save the configuration
- Log a message indicating the changes

Drag and drop the configuration snippets from the bottom onto the boxes in the configuration to complete the applet. Not all options are used.

**Select and Place:**

```

event manager applet update-port-description
event [ ] interface regexp ."Ethernet.* cdp add
action 1.0 string trimright "$_nd_cdp_entry_name" ".cisco.com"
action 1.1 set _host "$_string_result"
action 2.0 [ ] "port ID Ethernet([0-9])/([0-9])" "$_nd_port_id" match _int
action 2.1 set _int "$_nd_port_id"
action 3.0 cli command "enable"
action 3.1 cli command "config t"
action 3.2 cli command "interface $_nd_local_intf_name"
action 3.3 cli command "description Connected to $_host $_int"
action 3.4 cli command "do write memory"
action 4.0 [ ] "EEM updated description on $_nd_local_intf_name and saved config"
action 5.0 exit

```

neighbor-discovery	cns-event	regexp	publish-event	syslog pattern	syslog msg
--------------------	-----------	--------	---------------	----------------	------------

**Correct Answer:**

```

event manager applet update-port-description
event neighbor-discovery interface regexp ."Ethernet.* cdp add
action 1.0 string trimright "$_nd_cdp_entry_name" ".cisco.com"
action 1.1 set _host "$_string_result"
action 2.0 regexp "port ID Ethernet([0-9]/[0-9])" "$_nd_port_id" match _int
action 2.1 set _int "$_nd_port_id"
action 3.0 cli command "enable"
action 3.1 cli command "config t"
action 3.2 cli command "interface $_nd_local_intf_name"
action 3.3 cli command "description Connected to $_host $_int"
action 3.4 cli command "do write memory"
action 4.0 syslog msg "EEM updated description on $_nd_local_intf_name and saved config"
action 5.0 exit

```

cns-event

publish-event

syslog pattern

**Section: Selected Explanation**

**Explanation/Reference:**

**QUESTION 1231**

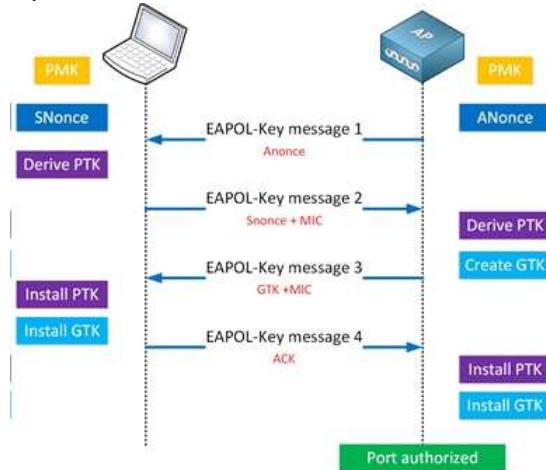
Which key is used to encrypt multicast and broadcast traffic and is generated in message 3 of the WPA/WPA2 four-way handshake?

- A. GTK
- B. PTK
- C. MSK
- D. PMK

**Correct Answer: A**

**Section: Selected Explanation**

**Explanation/Reference:**



In the 4-way handshake, the PMK is used to derive the PTK, and the GMK is used to derive the GTK. The PTK is then used to encrypt unicast communication and the GTK is used to encrypt multicast and broadcast traffic.

**QUESTION 1232**

Which FHRP should be chosen if vendor interoperability and support for IPv6 are required?

- A. HSRP
- B. GLBP
- C. VRRP v2
- D. VRRP v3

**Correct Answer: D**  
**Section: Selected Explanation**

**Explanation/Reference:**

VRRP (Virtual Router Redundancy Protocol) is an industry-standard, fault-tolerant network protocol that enhances network reliability by providing automatic default gateway redundancy. VRRPv3 supports usage of IPv4 and IPv6 addresses while VRRPv2 only supports IPv4 addresses.

**QUESTION 1233**

A customer wants to enable WPA3 Enterprise and requires all devices to use mutual certificate authentication. Which EAP method should be used?

- A. EAP-Fastv1
- B. EAP-MD5

- C. LEAP with GTC
- D. PEAP-TLS

**Correct Answer:** D  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

PEAP-TLS probably means "PEAP with inner EAP-TLS": This is the most secure method because another TLS authentication happens inside the encrypted TLS tunnel. This inner TLS authentication, requires both server- and client-side certificate authentication.

**QUESTION 1234**

What is a client considered when it is in web authentication state and roams between two controllers with mobility tunnels?

- A. foreign
- B. mobile
- C. anchor
- D. new

**Correct Answer:** D  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

If a client roams in web authentication state (i.e. not authenticated by 802.1x), the client is considered as a new client on another controller instead of being identified as a mobile client.

**QUESTION 1235**

Which new security enhancement is introduced by deploying a next-generation firewall at the data center in addition to the Internet edge?

- A. firewall protection of the east-west traffic at the data center
- B. virtual private network for remote access
- C. firewall protection of the south-north traffic at the data center
- D. DDoS protection

**Correct Answer:** A  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

The two typical types of data flows in data center are north-south and east-west. North-south refers to data flow that enters or leaves the data center and east-west refers to the data flows within the data center. Adding additional NGFWs within the data center can protect traffic between servers within the data center.

**QUESTION 1236**

In a fabric-enabled wireless network, which device is responsible for maintaining the endpoint ID database?

- A. fabric border node
- B. fabric edge node
- C. fabric wireless controller
- D. control plane node

**Correct Answer:** D  
**Section:** Selected  
**Explanation**

**Explanation/Reference:**

### Control Plane Node (MSMR)

- Control Plane Node acts as both Map Server and Map resolver (MSMR)
- Keeps database of all EID registrations for all AF(Ethernet/IPv4/IPv6)
- No synchronization between Control Plane nodes
- Show lisp site command gives overview of all IPv4/IPv6 registrations

Border-CP#sh lisp site instance-id 4099					
LISP Site Registration Information					
Site Name	Last Register	Up	Who Last Registered	Inst ID	EID Prefix
site_uci	never	no	--	4099	0.0.0.0/0
	never	no	--	4099	172.30.2.128/25
	05:17:04	yes#	172.30.233.6:43136	4099	172.30.2.131/32
	00:00:07	yes#	172.30.233.1:4342	4099	172.30.2.132/32
	never	no	--	4099	172.30.3.0/24
	00:00:07	yes#	172.30.233.1:4342	4099	172.30.3.2/32
	05:17:04	yes#	172.30.233.6:43136	4099	172.30.3.3/32
	never	no	--	4099	172.30.4.0/24

cisco live!

**QUESTION 1237**

```
Router#sh run | b vty
line vty 0 4
  login local
line vty 5 15
  login local
```

The existing configuration must be updated to terminate all EXEC sessions after 120 minutes. Which command set should be applied?

- A. line vty 0 15

- A. absolute-timeout 120
- B. line vty 0 15  
  session-timeout 120
- C. line vty 0 15  
  session-limit 120
- D. line vty 0 15  
  exec-timeout 120

**Correct Answer:** A

**Section:** Selected

**Explanation**

**Explanation/Reference:**

"absolute-timeout" is the absolute timeout for line disconnection (The EXEC session will be disconnected even if it is still active).  
 "exec-timeout" is the interval that the idle EXEC session will be disconnected.  
 "session-timeout" is the timeout interval for all outgoing connection.

Unlike all other questions, the keyword "idle" is not included in this question. Therefore, the question may require "absolute-timeout".

```
Router(config-line)#absolute-timeout ?
<0-10000> Absolute timeout interval in minutes

Router(config-line)#session-timeout ?
<0-35791> Session timeout interval in minutes

Router(config-line)#session-limit ?
<0-4294967295> Maximum number of sessions

Router(config-line)#exec-timeout ?
<0-35791> Timeout in minutes
```

**QUESTION 1238**

```
device_ip = [
    "site1-cedge01": "10.10.1.11",
    "site2-cedge01": "10.10.1.12",
    "site3-vedge01": "10.10.1.13"
]
```



The key value pairs must be extracted by iterating through a list of tuples. Which statement completes the snippet and prints each key value pair as a tuple?

- A. for device in device\_ip: print(device)
- B. for device in device\_ip.values(): print(device)
- C. for device in device\_ip.items(): print(device)
- D. for device, value in device\_ip.items(): print(device)

**Correct Answer:** C

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Note that the variable name is "device\_ip" (not two individual words in the diagram).

```
for device in device_ip: print(device)
#The above line outputs the following words:
# site1-cedge01
# site2-cedge01
# site3-cedge01

for device in device_ip.values(): print(device)
#The above line outputs the following words:
# 10.10.1.11
# 10.10.1.12
# 10.10.1.13

for device in device_ip.items(): print(device)
#The above line outputs the following "tuples":
# ('site1-cedge01', '10.10.1.11')
# ('site1-cedge02', '10.10.1.12')
# ('site1-cedge03', '10.10.1.13')

for device,value in device_ip.items(): print(device)
#The above line outputs the following words:
# site1-cedge01
# site2-cedge01
# site3-cedge01
```

**QUESTION 1239**

What is a benefit of Cisco TrustSec in a multilayered LAN network design?

- A. Policy can be applied on a hop-by-hop basis.
- B. Application flows between hosts on the LAN to remote destinations can be encrypted.
- C. Policy or ACLs are not required.
- D. There is no requirement to run IEEE 802.1x when TrustSec is enabled on a switch port.

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Other than 802.1x, MAC Authentication Bypass (MAB) or Web Authentication Proxy (WebAuth) are also supported.

Between MACsec-capable devices, packets are encrypted on egress from the transmitting device, decrypted on ingress to the receiving device, and in the clear within the devices. However, this feature is only available between TrustSec hardware-capable devices.

In a multilayered LAN network, Cisco TrustSec implements scalable, role-based access control using Security Group Tags (SGTs) to replace traditional VLANs and ACLs. However, policy is required.

#### QUESTION 1240

What are two best practices when designing a campus Layer 3 infrastructure? (Choose two.)

- A. Configure passive-interface on nontransit links.
- B. Summarize routes from the aggregation layer toward the core layer.
- C. Implement security features at the core.
- D. Tune Cisco Express Forwarding load balancing hash for ECMP routing.
- E. Summarize from the access layer toward the aggregation layer.

**Correct Answer:** AE

**Section:** Selected

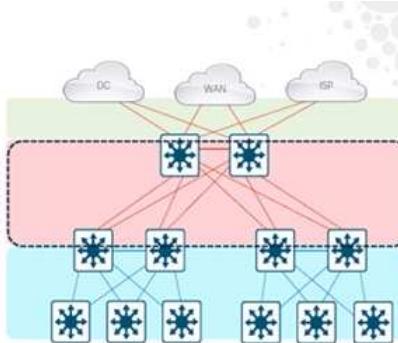
**Explanation**

**Explanation/Reference:**

### Best Practices

#### Layer 3 Routing Protocols

- Typically deployed in distribution to core, and core-to-core interconnections
- Used to quickly reroute around failed node/links while providing load balancing over redundant paths
- Build triangles not squares for deterministic convergence
- Only peer on links that you intend to use as transit



cisco Live!

10/15/2021 10:46 AM Cisco Confidential - Cisco Policy 48

For point 2 above:

"Per-destination load balancing is enabled by default when you enable Cisco Express Forwarding. To use per-destination load balancing, you do not perform any additional tasks once Cisco Express Forwarding is enabled. Per-destination is the load-balancing method of choice for most situations." Since it is enabled by default, you do not need to tune it for ECMP (equal-cost multi-path) routing.

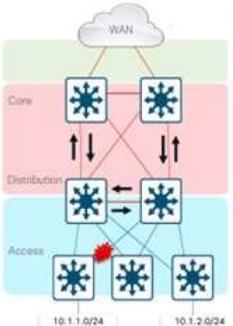
### Why You Want to Summarize at the Distribution

#### Limit EIGRP Queries and OSPF LSA Propagation

- It is important to force summarization at the distribution towards the core
- For return path traffic an OSPF or EIGRP re-route is required
- By limiting the number of peers an EIGRP router must query or the number of LSAs an OSPF peer must process we can optimize this reroute

**EIGRP Example:**

```
interface Port-channel1
description to Core1
ip address 10.122.0.34 255.255.255.252
ip hello-interval eigrp 100 1
ip hold-time eigrp 100 3
ip summary-address eigrp 100 10.1.0.0 255.255.0.0 5
```



cisco Live!

10/15/2021 10:46 AM Cisco Confidential - Cisco Policy 52

#### QUESTION 1241

Which security feature does stateless authentication and authorization use for REST API calls?

- A. SSL/TLS certificate encryption
- B. API keys
- C. cookie-based session authentication
- D. OAuth 2 tokens

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

**Cisco DevNet** Documentation Learn Technologies Community Events  SIGN UP FREE LOG IN

Documentation > All > Intersight > Intersight  BETA

## Cisco Intersight RESTful API

- Overview
- Authentication
  - API Authorization Schemes
    - API Keys
      - Benefits of using API Keys
      - Generating API Keys
      - Authentication Process for API keys
      - Role-Based Access Control Policy and API Keys
      - Audit Log and API Keys
      - Deleting API keys
      - HTTP Signature Algorithms
      - Session Cookies
      - TLS Security
      - Client-Side Verification of the TLS Connection
      - Server-Side Certificate Revocation Status

**cisco DevNet** Documentation Learn Technologies Community Events  SIGN UP FREE LOG IN

Documentation > All > AppDynamics > Cisco Observability Platform API Authentication  BETA

## Cisco Observability Platform OAuth API

- Overview
- OAuth 2.0 Security
  - Use Case for Access Tokens
  - Get an Access Token
  - Generate an Access Token
  - Generate Additional Access Tokens
  - OpenID Connect Discovery Endpoint

**OAuth 2.0**, or Open Authorization, is a standard designed to allow a website or an application to access resources hosted by other web applications. OAuth 2.0 provides access and restricts actions to a client application, without sharing user credentials. OAuth2.0 is an authorization protocol and not an authentication protocol. As such, it is designed to grant access to a set of resources; for example, remote APIs or a user's data. OAuth2.0 uses access tokens. An access token is a piece of data that represents the authorization to access resources on behalf of a user.

OAuth 2.0 access tokens are not inherently stateless. However, the framework allows for both stateless and stateful implementations depending on the token format and security requirements.

### QUESTION 1242

What is MACsec?

- A. open-source link encryption technology
- B. technology that allows guest access to wireless networks without using a PSK
- C. Layer 4 security protocol
- D. technology that makes wired networks at least as secure as wireless networks

**Correct Answer:** A

**Section:** Selected

**Explanation**

#### Explanation/Reference:

MACsec is an IEEE 802.1AE standards based Layer 2 hop-by-hop encryption that provides data confidentiality and integrity for media access independent protocols.

### QUESTION 1243

How do FHRPs differ from SSO?

- A. FHRPs influence bandwidth allocation, and SSO influences routing decisions.
- B. FHRPs use OTV for redundancy, and SSO uses VXLAN for state synchronization.
- C. FHRPs maintain state information within a single device, and SSO manages state information across multiple devices.
- D. FHRPs provide gateway redundancy, and SSO provides failover within a single device.

**Correct Answer:** D

**Section:** Selected

**Explanation**

#### Explanation/Reference:

### QUESTION 1244

```
import json
from requests import get

Headers = { "Content-Type" : "application/yang-data+json",
            "Accept" : "application/yang-data+json" }

Devices = open("devices.txt", "r")

for Device in Devices.readlines():
    Hostname, IP, Login, Pass = Device.strip().split(",")
    URL = f"https://{IP}/restconf/data/Cisco-IOS-XE-native:native"
    Creds = (Login, Pass)
    Response = get(URL, auth = Creds, headers = Headers, verify = False)
```

How should the script be completed so that each device configuration is saved into a JSON-formatted file under the device name?

A. Append to the body of the for loop:

```
with open(f'{Hostname}.json', "w") as OutFile:  
    OutFile.write(Response.text)
```

B. Insert after the for loop:

```
with open(f'{Hostname}.json', "w") as OutFile:  
    OutFile.write(json.dumps(Response.text))
```

C. Insert immediately before the for loop:

```
with open(f'{Hostname}.json', "w") as OutFile:  
    OutFile.write(json.load(Devices))
```

D. Insert after the for loop:

```
with open(f'{Hostname}.json', "w") as OutFile:  
    OutFile.write(Response)
```

**Correct Answer: B**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

The function "json.dumps()" is required for converting a Python object into JSON-formatted string.

**QUESTION 1245**

In a LISP topology, which component does the ITR send a resolution request to when it does not know the path to a specific EID?

- A. proxy ingress tunnel router
- B. map resolver
- C. routing locator
- D. proxy egress tunnel router

**Correct Answer: B**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

The function of the LISP map resolver (MR) is to accept encapsulated Map-Request messages from ingress tunnel routers (ITRs), decapsulate those messages, and then forward the messages to the map server (MS).

**QUESTION 1246**

Which data type does YANG support for reference values from a set of assigned names?

- A. array
- B. object
- C. decimal64
- D. enumeration

**Correct Answer: D**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

```
typedef ip-version {  
    type enumeration {  
        enum unknown {  
            value "0";  
            description  
                "An unknown or unspecified version of the Internet  
                protocol.";  
        }  
        enum ipv4 {  
            value "1";  
            description  
                "The IPv4 protocol as defined in RFC 791.";  
        }  
        enum ipv6 {  
            value "2";  
            description  
                "The IPv6 protocol as defined in RFC 2460.";  
        }  
    }  
}
```

In the above example, "ip-version" is a enumeration that can only accept a value from the set of assigned names consisting of "unknown", "ipv4" or "ipv6".

**QUESTION 1247**

```

from ncclient import manager
from jinja2 import Template

m= manager.connect(host='192.168.1.10', port=830, username='admin',
password='admin', device_params={'name': 'csr'})

interface_filter = """
<filter>
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
    <interface>
      <GigabitEthernet>
        <name>1</name>
      </GigabitEthernet>
    </interface>
  </native>
</filter>
"""

result = m.get_config('running', interface_filter)
print(result)

```

What is the result of running the script?

- A. It prints the XML output of "show running" on the device with IP 192.168.1.0.
- B. It prints the XML output of "show running interface GigabitEthernet 1" on the device with IP 192.168.1.10.
- C. It opens interface config mode on the router and prompts for further XML commands from the user.
- D. It configures the IP address 192.168.1.10 on the GigabitEthernet 1 interface and prints the new XML configuration.

**Correct Answer:** B

**Section:** Selected

**Explanation**

**Explanation/Reference:**

#### QUESTION 1248

Which benefit does Cisco Catalyst SD-WAN provide over a traditional WAN solution?

- A. distributed date plane
- B. distributed control plane
- C. reduced training requirements
- D. centralized operation and security policies

**Correct Answer:** D

**Section:** Selected

**Explanation**

**Explanation/Reference:**

Cisco SD-WAN utilizes a centralized control plane and a distributed data plane. However, traditional WAN solution also uses distributed data plane (the choice may have mis-spell "data"). Hence, distributed data plane is not a benefit over traditional WAN solution.

#### QUESTION 1249

Which action is a LISP map server responsible for?

- A. accepting registration requests from ETRs
- B. forwarding requests to the map server
- C. forwarding user data traffic
- D. accepting registration requests from ITRs

**Correct Answer:** A

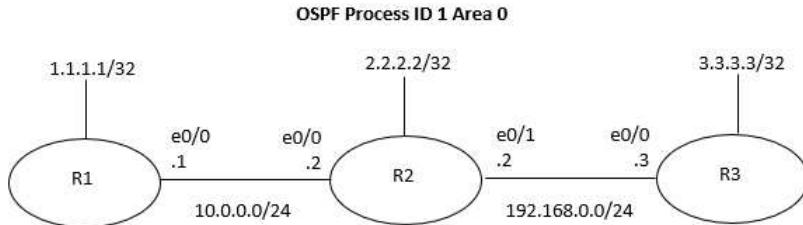
**Section:** Selected

**Explanation**

**Explanation/Reference:**

## Simulation Questions

### QUESTION 1



Configure OSPF on all three routers according to the topology to achieve these goals:

1. Configure OSPF without using the "network" statement under the "router ospf" configuration section.
2. Ensure that all networks are advertised between the routers.
3. Configure a single command under each Ethernet interface to prevent OSPF neighbors from participating in a DR/BDR election and ensure that no extra host routes are generated.

**Correct Answer:**

Section: (none)

Explanation

Explanation/Reference:

Tasks to perform:

1. Use a command to find the interface that is assigned with the /32 IP address in each router e.g. "sh ip int brief". We shall assume that that IP address of host network is configured as "lo0" in all routers.
2. Without network command, you can enable OSPF by "ip ospf 1 area 0" in each of the concerned interface e.g. "e0/0" and "lo0" in R1.
3. Since DR/BDR election is not allowed, the OSPF network type "broadcast" (default for Ethernet) and "NBMA" is not appropriate. the OSPF network "Point-to-Multipoint" will generate additional host routes. Hence, you can only change the OSPF network type to "point-to-point" in each Ethernet interface. Assume the IP address of host network is loopback interface, it is not needed since question says only on Ethernet interface.
4. You can use "sh ip route ospf" in each router to ensure the networks in other routers are learnt.
5. Finally remember to save the configuration with "copy run start" (or "wr") in each router.

**Summarized configuration commands:**

**R1:**

```
en
config t
int lo0
ip ospf 1 area 0
int e0/0
ip ospf 1 area 0
ip ospf network point-to-point
end
copy run start
```

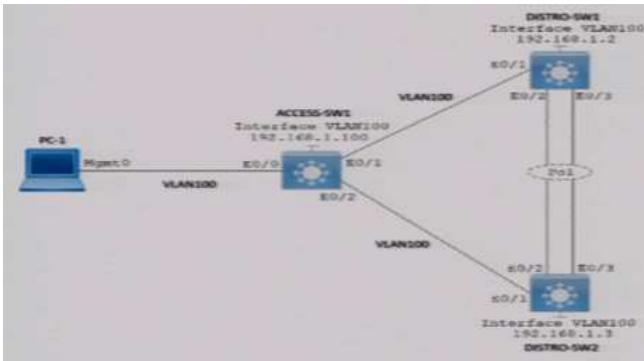
**R2:**

```
en
config t
int lo0
ip ospf 1 area 0
int e0/0
ip ospf 1 area 0
ip ospf network point-to-point
int e0/1
ip ospf 1 area 0
ip ospf network point-to-point
end
copy run start
```

**R3:**

```
en
config t
int lo0
ip ospf 1 area 0
int e0/0
ip ospf 1 area 0
ip ospf network point-to-point
end
copy run start
```

### QUESTION 2



Implement VRRP between DISTRO-SW1 and DISTRO-SW2 on VLAN100 for hosts connected to ACCESS-SW1 to achieve these goals:

1. Configure group number 1 using the virtual IP address of 192.168.1.1/24.
2. Configure DISTRO-SW1 as the active router using a priority value of 110 and DISTRO-SW2 as the standby router.
3. DISTRO-SW1 and DISTRO-SW2 should exchange VRRP hello packets every 15 seconds.

**Correct Answer:**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Tasks to perform:**

- Configure VRRP on the concerned layer 3 interfaces i.e. vlan100 of both DISTRO-SW1 and DISTRO-SW2 with VRRP group 1 and VIP 192.168.1.1
- Add the command for VRRP priority 110 to DISTRO-SW1's interface vlan 100
- Change the timers of VRRP in interface vlan 100 of both switches to 15 seconds
- Use "sh vrrp" in each switches to verify the settings.
- Enter "copy run start" in both switches to save the configuration.

**Summarized configuration commands:**

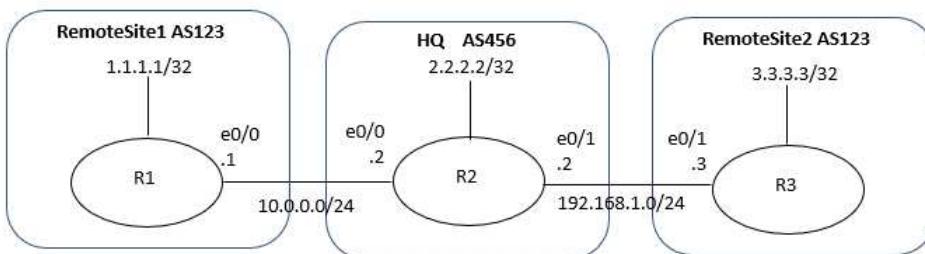
**DISTRO-SW1**

```
en
config t
int vlan 100
vrrp 1 ip 192.168.1.1
vrrp 1 priority 110
vrrp 1 timers advertise 15
end
copy run start
```

**DISTRO-SW2**

```
en
config t
int vlan 100
vrrp 1 ip 192.168.1.1
vrrp 1 timers advertise 15
end
copy run start
```

### QUESTION 3



BGP connectivity exists between Headquarters and both remote sites; however, Remote Site 1 cannot communicate with Remote Site 2. Configure BGP according to the topology to achieve these goals:

1. Configure R1 and R3 under the BGP process to provide reachability between Remote Site 1 and Remote Site 2. No configuration changes are permitted on R2.
2. Ensure that the /32 networks at Remote Site 1 and Remote Site 2 can ping each other.

**Correct Answer:**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Problem is obvious since Remote Site 1 and Remote Site 2 are not directly connected but they are having the same AS number. Therefore BGP routes from one site learning through HQ will be rejected by the other site since the AS path in the BGP route contains its own AS number "123".

**Tasks to perform:**

- Use "sh ip route bgp" in R1 and R3 to ensure BGP is properly configured. The BGP route for "2.2.2.2/32" should be found in both routers.
- Enter the BGP configuration command "neighbor ... allowas-in" in both R1 and R3 so that both routers will accept BGP route having its own AS number.
- Use "sh ip route bgp" in R1 and R3 to ensure that the host route of the other router can be found.

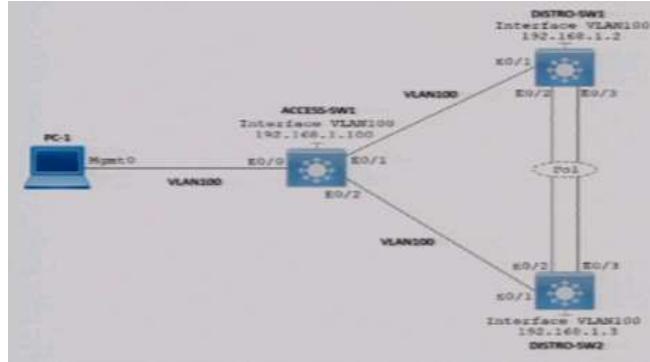
- Use "ping 3.3.3.3 source 1.1.1.1" in R1 and "ping 1.1.1.1 source 3.3.3.3" in R3 verify they can ping each other.
- Enter "copy run start" in both routers to save the configuration.

**Summarized configuration commands:**

```
R1
en
config t
router bgp 123
neighbor 10.0.0.2 allowas-in
end
copy run start
```

```
R3
en
config t
router bgp 123
neighbor 192.168.1.2 allowas-in
end
copy run start
```

**QUESTION 4**



Implement GLBP between DISTRO-SW1 and DISTRO-SW2 on VLAN100 for hosts connected to ACCESS-SW1 to achieve these goals:

1. Configure group 1 using the virtual IP address of 192.168.1.254.
2. Configure DISTRO-SW1 as the AVG using a priority value of 110.
- 3- If DISTRO-SW1 suffers a failure and recovers, ensure that it automatically resumes the AVG role after waiting for a minimum of 15 seconds.

**Correct Answer:**  
Section: (none)  
Explanation

**Explanation/Reference:**

**Tasks to perform:**

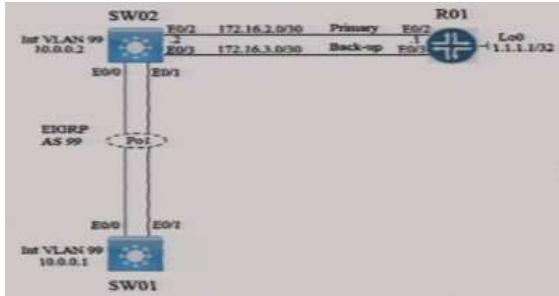
- Configure GLBP on the concerned layer 3 interfaces i.e. vlan100 of both DISTRO-SW1 and DISTRO-SW2 with group 1 and VIP 192.168.1.254
- Add the command for GLBP priority 110 to DISTRO-SW1's interface vlan 100
- Add the preempt setting with 15 seconds delay to DISTRO-SW1's interface vlan 100.
- Use "sh vrrp" in each switches to verify the settings.
- Enter "copy run start" in both switches to save the configuration.

**Summarized configuration commands:**

```
DISTRO-SW1
en
config t
int vlan 100
glbp 1 ip 192.168.1.254
glbp 1 priority 110
glbp 1 preempt delay minimum 15
end
copy run start
```

```
DISTRO-SW2
en
config t
int vlan 100
glbp 1 ip 192.168.1.254
end
copy run start
```

**QUESTION 5**



Configure logging on SW01 and NetFlow on R01 to achieve these goals:

1. Enable archive logging on SW01 to track each time a change is made to the configuration and the user who made the change.
2. The NetFlow Top Talkers feature has been preconfigured on R01. Enable the feature for all inbound traffic on interface E0/2 of R01.

**Correct Answer:**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Tasks to perform:**

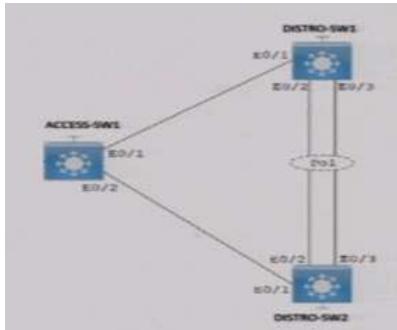
- Configure Config Log Archive in SW01.
- Configure NetFlow on R01's e0/2 interface.
- Enter "copy run start" to save the configuration.

**Summarized configuration commands:**

```
SW01
en
config t
archive
log config
logging enable
end
```

```
R01
en
config t
int e0/2
ip flow ingress
end
```

#### QUESTION 6



The operations team started configuring network devices for a new site. Complete the configurations to achieve these goals:

- 1 . Ensure that port channel Po1 between DISTRO-SW01 and DISTRO-SW02 is operational using the LACP protocol. Configuration changes for this task must be made on DISTRO-SW01.
2. Ensure that traffic on VLAN 10 is carried as untagged traffic between DISTRO-SW01 and DISTRO-SW02.
- 3- Complete the Rapid-PVST+ configuration on DISTRO-SW2 by ensuring it is the secondary root switch for all VLANs in the range of 1 to 1005.

**Correct Answer:**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Tasks to perform:**

- Use "sh etherchannel", "sh run int e0/2" and "sh run int e0/3" in both DISTRO-SW01 and DISTRO-SW02 to view the problem in existing configuration. Assume the problem is due to the fact that the interfaces of both switches are configured as " mode passive".
- Change the two interfaces "e0/2" and "e0/3" in DISTRO-SW01 to "mode active".
- Use "sh etherchannel" to verify the EtherChannel becomes Up.
- Configure the native vlan in the trunk link formed by interface Po1 to VLAN 10. Note that many error logging messages about mismatch VLAN may appear after completing the configuration of one switch but before the configuration of the other switch.
- Both switches should already be configured with "spanning-tree mode rapid-pvst".
- Use "sh spanning-tree" in DISTRO-SW1 to find its priority in "Bridge ID".
- In DISTRO-SW2, configure one of the priority values below that is larger than the one found in DISTRO-SW1. (The following can be found by entering an invalid priority value e.g. 1 i.e "spanning-tree vlan 1-1005 priority 1"
 

0	4096	8192	12288	16384	20480	24576	28672
32768	36864	40960	45056	49152	53248	57344	61440

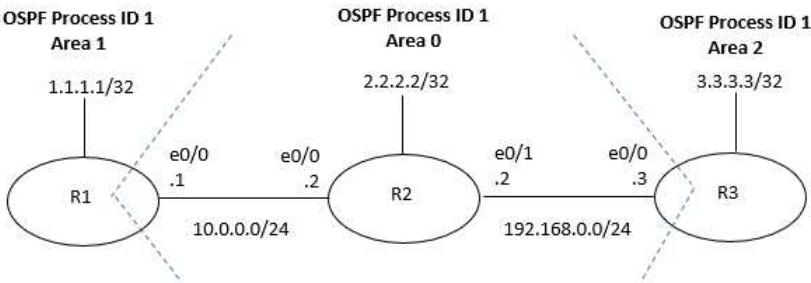
 For example if DISTRO-SW1 is 24576, you can use 28672 as priority in DISTRO-SW2.
- Enter "copy run start" to save the configuration in both switches.

**Summarized configuration commands:**

```
DISTRO-SW01
en
config t
int e0/2
channel-group 1 mode active
int e0/3
channel-group 1 mode active
int Po1
switchport trunk native vlan 10
end
copy run start
```

```
DISTRO-SW02
en
config t
int Po1
switchport trunk native vlan 10
spanning-tree vlan 1-1005 priority 28672
end
copy run start
```

**QUESTION 7**



Configure OSPF on all three routers according to the topology diagram to achieve these goals:

1. Enable OSPF on all interfaces using the network statement and match the network mask of each interface.
- 2- Ensure that all networks are advertised between the routers.
3. Ensure that all routers use OSPF process ID 1 and that the Lo0 interface is used for the router ID.
4. Configure OSPF MDS authentication on every physical interface running OSPF using key 1 and the password CISCO123.

**Correct Answer:**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**Tasks to perform:**

- Use e.g. "sh ip int brief" to find the interface having IP address with host network. Assume the findings show that they are all "lo0" in all routers.
- Configure OSPF for lo0 and the Ethernet interfaces shown in the diagram in each router. Note that all Ethernet interfaces should be in Area 0 and therefore R1 and R3 are the ABRs.
- Use "sh ip ospf" to ensure that the Lo0's IP address is being used as the OSPF Router ID. However, it will be safer to configure the router ID manually with "router-id x.x.x.x". However, since this requires "clear ip ospf process" to make it effective immediately, we enter the "router-id x.x.x.x" immediately after "router ospf 1" in the following summarized commands.
- Configure MD5 authentication on every concerned Ethernet interfaces in all routers.
- Use "sh ip ospf nei" to ensure all OSPF neighboring are formed properly after adding authentication.
- Enter "copy run start" to save the configuration in all routers.

**Summarized configuration commands:**

```
R1
en
config t
router ospf 1
router-id 1.1.1.1
network 10.0.0.0 0.0.0.255 area 0
network 1.1.1.1 0.0.0.0 area 1
int e0/0
ip ospf message-digest-key 1 md5 CISCO123
ip ospf authentication message-digest
end
copy run start
```

```
R2
en
config t
router ospf 1
router-id 2.2.2.2
network 10.0.0.0 0.0.0.255 area 0
network 192.168.0.0 0.0.0.255 area 0
network 2.2.2.2 0.0.0.0 area 0
int e0/0
ip ospf message-digest-key 1 md5 CISCO123
ip ospf authentication message-digest
int e0/1
ip ospf message-digest-key 1 md5 CISCO123
```

```

ip ospf authentication message-digest
end
copy run start

R3
en
config t
router ospf 1
router-id 3.3.3.3
network 192.168.0.0 0.0.0.255 area 0
network 3.3.3.3 0.0.0.0 area 2
int e0/0
ip ospf message-digest-key 1 md5 CISCO123
ip ospf authentication message-digest
copy run start

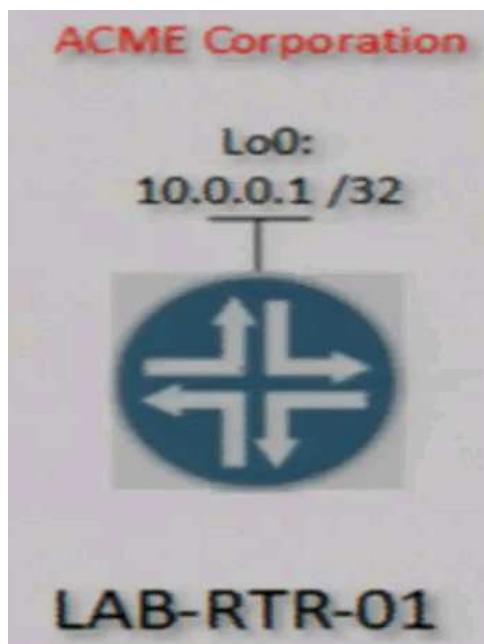
```

#### QUESTION 8

##### Guidelines:

- This is a lab item in which tasks will be performed on virtual devices.
- Refer to the Tasks tab to view the tasks for this lab item.
  - Refer to the Topology tab to access the device console(s) and perform the tasks.
  - Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
  - All necessary preconfigurations have been applied.
  - Do not change the enable password or hostname for any device.
  - Save your configurations to NVRAM before moving to the next item.**
  - Click Next at the bottom of the screen to submit this lab and move to the next question.
  - When Next is clicked, the lab closes and cannot be reopened.

##### Topology:



##### Tasks:

- Configure an EEM applet on LAB-RTR-01 that will automatically re-enable interface Loopback0 if it is administratively shut down.

##### Correct Answer:

Section: (none)

Explanation

##### Explanation/Reference:

##### Summarized configuration commands:

```

event manager applet noshut-lo0
event syslog pattern "%LINK-5-CHANGED: Interface Loopback0, changed state to administratively down"
action 1.0 cli command "enable"
action 2.0 cli command "configure terminal"
action 3.0 cli command "int lo0"
action 4.0 cli command "no shut"
end
copy run start

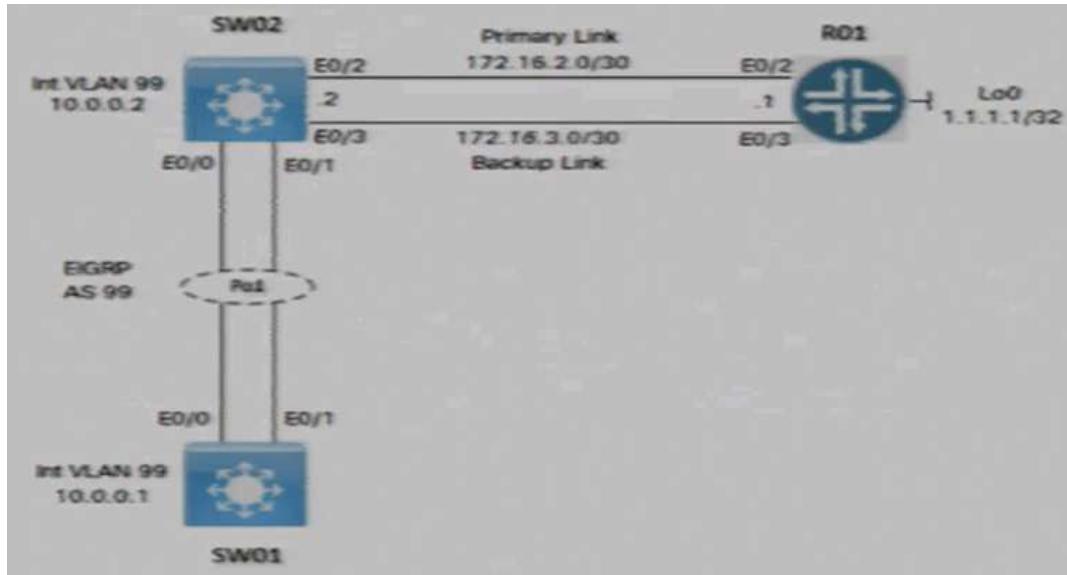
```

##### Explanations:

- You can use any other name you like for the applet.
- There are other ways to detect if lo0 is down (down means administratively down for loop back interface since it cannot be link down only) e.g. using SNMP, Track object through IP SLA, check wordings within output from commands such as "sh int lo0" or "sh run int lo0". However, reading syslog is the simplest.
- For safety, you should manually shut down the lo0 interface and check the logging message if the wordings are the same as above. Remember to "no shut" it before configuring since our EEM has one drawback : it cannot unshut lo0 if it is already shutdown before setting the EEM.

#### QUESTION 9

##### Topology:



**Tasks:**

Configure the devices according to the topology to achieve these goals:

1. Configure a SPAN session on SW01 using these parameters:

- Session Number: 20
- Source Interface: VLAN 99
- Traffic Direction: Transmitted Traffic
- Destination Interface: Ethernet 0/1

2. Configure the NetFlow Top Talkers feature for outbound traffic on interface E0/2 of R01 with these parameters:

- Number of Top Talkers: 50
- Sort Type: Packets
- Cache Timeout: 30 seconds

3. Configure an IP SLA operation on SW02 and start the ICMP probe with these parameters:

- Entry Number: 10
- Target IP: 1.1.1.1
- Source IP: 172.16.2.2
- Frequency: 5 seconds
- Threshold: 250 milliseconds
- Timeout : 3000 milliseconds
- Lifetime: Forever

**Correct Answer:**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Summarized configuration commands:**

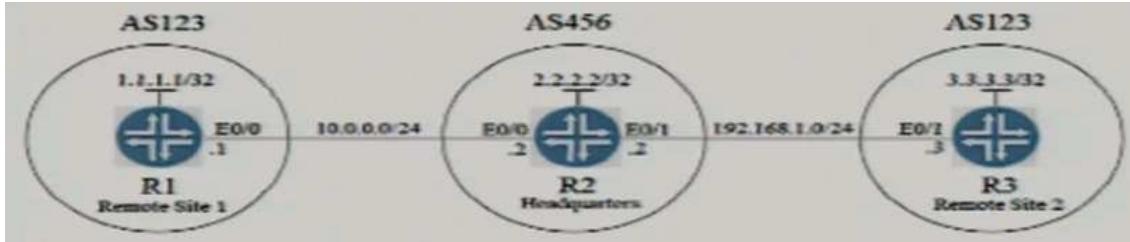
```
SW01
en
config t
monitor session 20 source vlan 99 tx
monitor session 20 destination int e0/1
end
copy run start
```

```
R01
en
config t
int e0/2
ip flow egress
exit
ip flow-top-talkers
top 50
sort-by packets
cache-timeout 30000
end
copy run start
```

```
SW02
en
config t
ip sla 10
icmp-echo 1.1.1.1 source-ip 172.16.2.2
frequency 5
threshold 250
timeout 3000
exit
ip sla schedule 10 start-time now life forever
end
copy run start
```

**QUESTION 10**

**Topology:**



**Tasks:**

BGP connectivity exists between Headquarters and both remote sites, however Remote Site 1 cannot communicate with Remote Site 2. Configure BGP according to the topology to achieve these goals:

1. Configure R2 under the BGP process to provide reachability between Remote Site 1 and Remote Site 2. No configuration changes are permitted on R1 or R3.
2. Ensure that the /32 networks at Remote Site 1 and Remote Site 2 can ping each other.

**Correct Answer:**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**Summarized configuration commands:**

**Task1:**

```
R2
en
config t
router bgp 456
  address-family ipv4
    neighbor 10.0.0.1 as-override
    neighbor 192.168.1.3 as-override
end
clear ip bgp * soft out
copy run start
```

**Task2:**

```
R1
ping 3.3.3.3 source 1.1.1.1
```

```
R3
ping 1.1.1.1 source 3.3.3.3
```

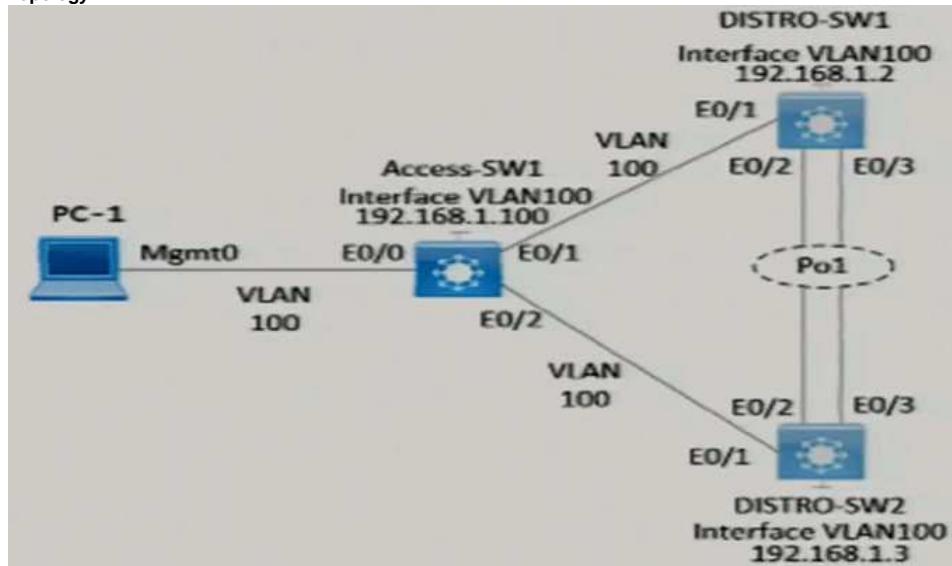
**Explanations:**

In this question, you can use "Sh run" in the three routers and check the BGP configuration in them. They should be properly configured. However, since R1 and R3 are both AS 123 but not connecting directly. BGP routes from R1 will be rejected by R3 and BGP routes from R3 will be rejected by R1. In this situation, there are two options:

- i. Configure "neighbor 10.0.0.2 allowas-in" in R1 and configure "neighbor 192.168.1.2 allowas-in" in R3. However, this is not applicable to this question since you can only configure R2.
- ii. Configure "neighbor x.x.x.x as-override" for the two neighbors in R2. When the BGP route 1.1.1.1/32 learnt from R1 is sending by R2 to R3, instead of having the AS path "456 123", the AS path will be changed to "456 456". Hence R3 will not reject the route. This applies to BGP routes learnt from R3 and sent to R1. For Troubleshooting, you can enter "sh ip bgp" in all three routers to check the BGP routes learnt and the AS numbers shown in the BGP routes.

**QUESTION 11**

**Topology:**



**Tasks:**

Configure HSRP between DISTRO-SW1 and DISTRO-SW2 on VLAN100 for hosts connected to ACCESS-SW1 to achieve these goals:

1. Configure group number 5 using the virtual IP address 192.168.1.75 /24.
2. Configure DISTRO-SW1 as the active router using a priority value of 105 and DISTRO-SW2 as the standby router.
3. Ensure that DISTRO-SW2 will take over the active role when DISTRO-SW1 goes down, and when DISTRO-SW1 recovers, it automatically resumes the active role.

**Correct Answer:**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**Summarized configuration commands:**

```
DISTRO-SW1
en
config t
int vlan 100
  standby 5 ip 192.168.1.75
  standby 5 priority 105
  standby 5 preempt
end
copy run start
```

**DISTRO-SW2**

```
en
config t
int vlan 100
  standby 5 ip 192.168.1.75
end
copy run start
```

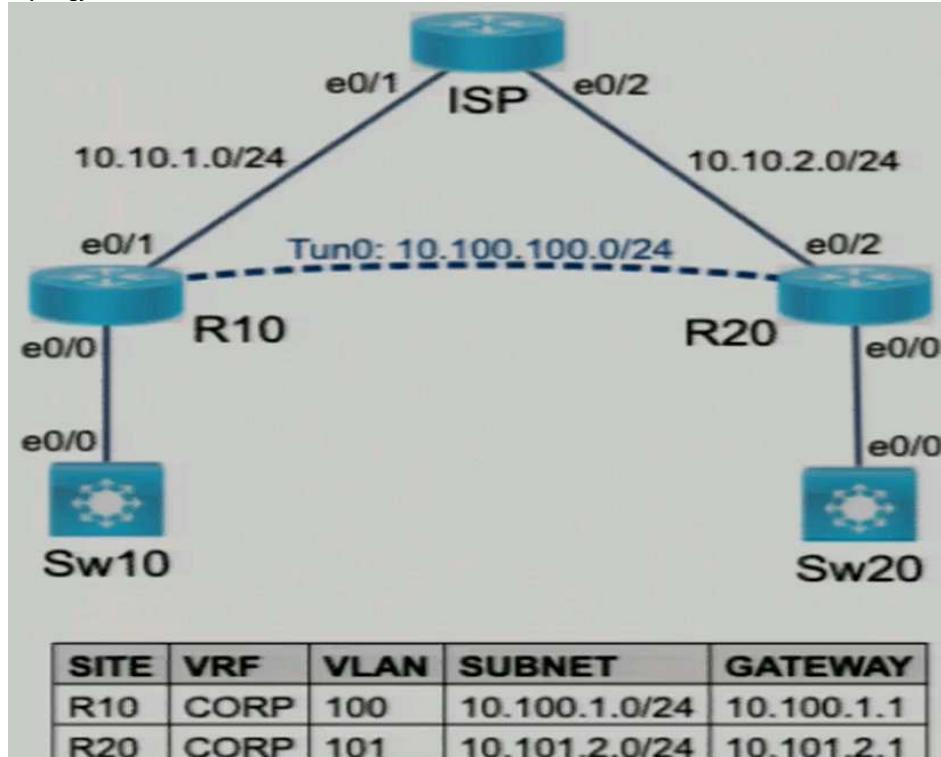
**Explanations:**

In the exiting configuration, only an IP address is configured in the interface VLAN 100 in both routers.

Since there is no tracking requirement, if "DISTRO-SW1" is alive, it will always have a higher priority and therefore there is no need to configure "preempt" in "DISTRO-SW2". However if priority decrement is required in the question, then you should configure "preempt" in both routers.

#### QUESTION 12

**Topology:**



**Tasks:**

The operations team started configuring network devices for a new site. R10 and R20 are preconfigured with the CORP VRF. R10 has network connectivity to R20. Complete the configurations to achieve these goals:

1. Extend the CORP VRF between R10 and R20 using Tunnel0.
2. Protect Tunnel0 using the preconfigured profile.

**Correct Answer:**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

**Summarized configuration commands:**

```
R10
en
config t
int tu0
  tunnel source 10.10.1.1
  tunnel destination 10.10.2.1
  tunnel protection ipsec profile MyProfile
end
copy run start
```

```

R20
en
config t
int tu0
  tunnel source 10.10.2.1
  tunnel destination 10.10.1.1
  tunnel protection ipsec profile MyProfile
end
copy run start

```

For verification:  
 You use the following for verification.

```

R10
ping vrf CORP 10.101.2.1 source 10.100.1.1

```

```

R20
ping vrf CORP 10.100.1.1 source 10.101.2.1

```

Explanations:  
 You should use "sh run" in R10 and R20 to check if their configuration settings are as follows:

```

R10
vrf definition CORP
  address-family ipv4
  exit-address-family
!
crypto isakmp policy 10
  encr aes
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco address 10.10.2.1
!
crypto ipsec transform-set MYSET esp-aes esp-md5-hmac
  mode tunnel
!
crypto ipsec profile MyProfile
  set transform-set MYSET
!
int tu0
  vrf forwarding CORP
  ip addr 10.100.100.1 255.255.255.0
!
int e0/0
  no ip addr
int e0/0.100
  encapsulation dot1Q 100
  vrf forwarding CORP
  ip addr 10.100.1.1 255.255.255.0
!
int e0/1
  ip addr 10.10.1.1 255.255.255.0
  ip ospf network point-to-point
  ip ospf 100 area 0.0.0.0
!
ip route vrf CORP 10.101.2.0 255.255.255.0 Tunnel0 10.100.100.2

```

```

R20
vrf definition CORP
  address-family ipv4
  exit-address-family
!
crypto isakmp policy 10
  encr aes
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco address 10.10.1.1
!
crypto ipsec transform-set MYSET esp-aes esp-md5-hmac
  mode tunnel
!
crypto ipsec profile MyProfile
  set transform-set MYSET
!
int tu0
  vrf forwarding CORP
  ip addr 10.100.100.2 255.255.255.0
!
int e0/0
  no ip addr
int e0/0.101
  encapsulation dot1Q 101
  vrf forwarding CORP
  ip addr 10.101.2.1 255.255.255.0
!
int e0/2
  ip addr 10.10.2.1 255.255.255.0
  ip ospf network point-to-point
  ip ospf 100 area 0.0.0.0
!
ip route vrf CORP 10.100.1.0 255.255.255.0 Tunnel0 10.100.100.1

```

In the existing configuration:

- The vrf CORP has been properly configured for all interfaces in R10 and R20.

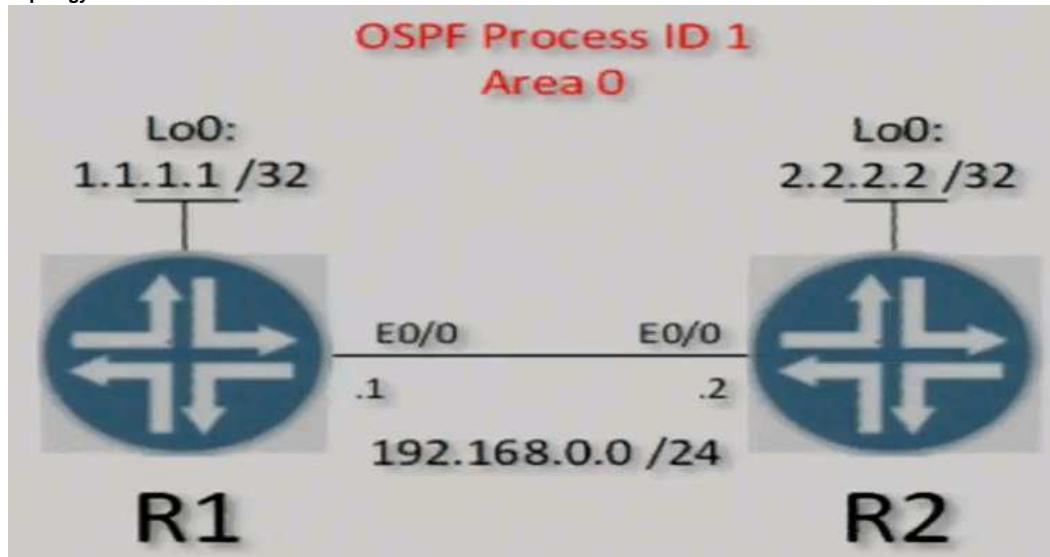
- The interface tu0 in R10 and R20 has not been configured properly since they miss "tunnel source" and "tunnel destination".
- After setting up the interface tu0, no configuration for routing is required since an existing static route has been properly configured in vrf CORP in both R10 and R20 to access the subnets of each other.

For task 1, since vrf has been configured in the tunnel 0 interface, you just need to configure the properly tunnel source and tunnel destination using the IP addresses of the R10's e0/1 and the R20's e0/2 in the two routers.

For task 2, you just need to apply the existing IPSec profile to the tunnel 0 interfaces in the two routers.

#### QUESTION 13

Topology:



#### Tasks:

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.

Correct Answer:

Section: (none)

Explanation

#### Explanation/Reference:

Summarized configuration commands:

##### Task1:

```
R1
en
config t
int lo0
 ip ospf 1 area 0
int e0/0
 ip ospf 1 area 0
end
copy run start
```

```
R2
en
config t
int lo0
 ip ospf 1 area 0
int e0/0
 ip ospf 1 area 0
end
copy run start
```

##### Task2:

```
R1
en
config t
int e0/0
 ip ospf network point-to-point
end
copy run start
```

```
R2
en
config t
int e0/0
 ip ospf network point-to-point
end
copy run start
```

#### For verification:

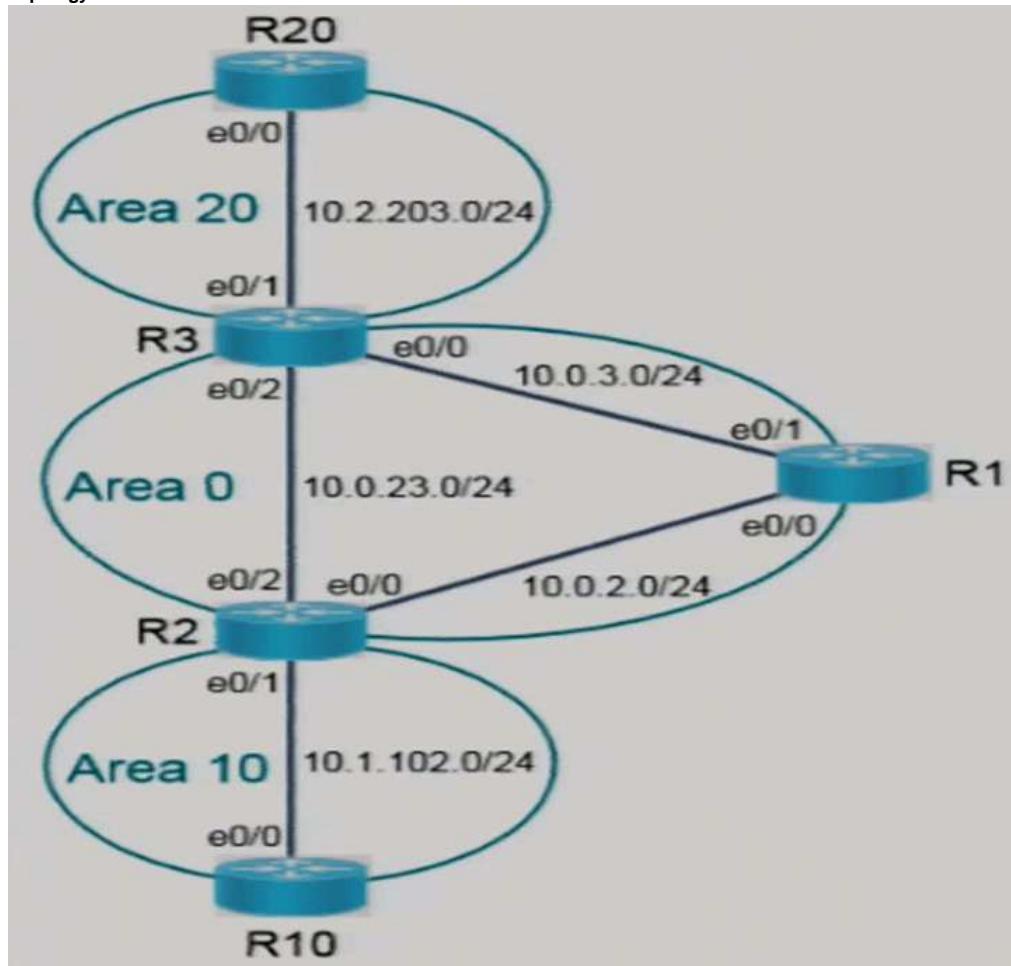
You can use "sh ip route ospf" in R1 and R2 to find the route for each other's loopback 0.

**Explanations:**

For task 2, you can use the OSPF network type "point-to-point" or "point-to-multipoint" to prevent the election of DR/BDR. However, the use of "point-to-multipoint" will generate an additional host route. Hence, "point-to-point" must be used.

**QUESTION 14**

Topology:

**Tasks:**

OSPF is partially configured. Complete the OSPF configurations on the ABR routers to achieve these goals:

- The route for R1 Loopback 0 should not be advertised into Area 10. Use the partially configured prefix list to accomplish the task. Do not use the area 0 command under the router ospf configuration section to accomplish this task.
- The route for R20 loopback 0 should not be advertised out of area 20. Use the partially configured prefix list to accomplish this task. Do not use the area 0 command under the router ospf configuration section to accomplish this task.

**Correct Answer:**

Section: (none)

Explanation

**Explanation/Reference:**

Summarized configuration commands:

**Task1:**

```
R2
en
config t
ip prefix-list deny_R1_Lo0 seq 1 deny 10.0.1.1/32
router ospf 10
  area 10 filter-list prefix deny_R1_Lo0 in
end
copy run start
```

**Task2:**

```
R3
en
config t
ip prefix-list deny_R20_Lo0 seq 1 deny 10.2.1.1/32
router ospf 10
  area 20 filter-list prefix deny_R20_Lo0 out
end
copy run start
```

**For verification:**

In R10 (the router in Area 10), enter "sh ip route ospf". The OSPF route "10.0.1.1/32" (R1's lo0) should not be found.  
In R2 (a router in Area 0), enter "sh ip route ospf". The OSPF route "10.2.1.1/32" (R20's lo0) should not be found.

**Explanations:**

The following configuration should be found in the routers. You can verify them through "sh run" in the concerned router.

**R1**

```
interface Loopback0
  ip address 10.0.1.1 255.255.255.0
!
interface Ethernet0/0
  ip address 10.0.2.1 255.255.255.0
!
interface Ethernet0/1
  ip address 10.0.3.1 255.255.255.0
!
router ospf 10
  router-id 10.0.1.1
  network 10.0.1.0 0.0.0.255 area 0
  network 10.0.2.0 0.0.0.255 area 0
  network 10.0.3.0 0.0.0.255 area 0
```

**R20**

```
interface Loopback0
  ip address 10.2.1.1 255.255.255.0
!
interface Loopback100
  ip address 10.2.100.20 255.255.255.0
!
interface Loopback200
  ip address 10.2.200.20 255.255.255.0
!
interface Ethernet0/0
  ip address 10.2.203.20 255.255.255.0
!
router ospf 10
  router-id 10.2.1.1
  network 10.2.1.0 0.0.0.255 area 20
  network 10.2.100.0 0.0.0.255 area 20
  network 10.2.200.0 0.0.0.255 area 20
  network 10.2.203.0 0.0.0.255 area 20
```

**R3**

```
interface Loopback0
  ip address 10.0.1.3 255.255.255.0
!
interface Ethernet0/0
  ip address 10.0.3.3 255.255.255.0
!
interface Ethernet0/1
  ip address 10.2.203.3 255.255.255.0
!
interface Ethernet0/2
  ip address 10.0.23.3 255.255.255.0
!
router ospf 10
  router-id 10.0.1.3
  network 10.0.1.0 0.0.0.255 area 0
  network 10.0.3.0 0.0.0.255 area 0
  network 10.0.23.0 0.0.0.255 area 0
  network 10.2.203.0 0.0.0.255 area 20
!
ip prefix-list deny_R20_Lo0 seq 2 permit 0.0.0.0/0 le 32
```

**R2**

```
interface Loopback0
  ip address 10.0.1.2 255.255.255.0
!
interface Ethernet0/0
  ip address 10.0.2.2 255.255.255.0
!
interface Ethernet0/1
  ip address 10.1.102.2 255.255.255.0
!
interface Ethernet0/2
  ip address 10.0.23.2 255.255.255.0
!
router ospf 10
  router-id 10.0.1.2
  network 10.0.1.0 0.0.0.255 area 0
  network 10.0.2.0 0.0.0.255 area 0
  network 10.0.23.0 0.0.0.255 area 0
  network 10.1.102.0 0.0.0.255 area 10
!
ip prefix-list deny_R1_Lo0 seq 2 permit 0.0.0.0/0 le 32
```

**R10**

```
interface Loopback0
  ip address 10.1.1.1 255.255.255.0
!
interface Loopback100
  ip address 10.1.100.10 255.255.255.0
!
interface Loopback200
  ip address 10.1.200.10 255.255.255.0
!
interface Ethernet0/0
  ip address 10.1.102.10 255.255.255.0
!
router ospf 10
  router-id 10.1.1.1
  network 10.1.1.0 0.0.0.255 area 10
  network 10.1.100.0 0.0.0.255 area 10
```

```
network 10.1.102.0 0.0.0.255 area 10
network 10.1.200.0 0.0.0.255 area 10
```

Since the question asks you to complete the OSPF configurations on the ABR routers, you should configure in R2 and R3 only.

#### Task 1:

Before making any configuration change for task 1, if you enter "sh ip route ospf" in R10, you should be able to find the OSPF router of the R1's lo0 i.e. "10.0.1.32" (**NOT 10.0.1.24 since the network of loopback interface is advertised by OSPF as host route by default !!!**)

In order to filter this route from entering Area 10, the following prefix list is needed in R2:

```
ip prefix-list deny_R1_Lo0 seq 1 deny 10.0.1.1/32
ip prefix-list deny_R1_Lo0 seq 2 permit 0.0.0.0/0 le 32
```

However, seq 2 is already configured in R2, therefore you just need to enter the rule seq 1. (**Remember to add "seq 1" in the rule! Otherwise the rule will be appended at the end of the prefix list**)

After configuring the sequence 1 rule, you should use "sh ip prefix-list" in R2 to ensure that you have type the prefix-list name correctly and the rule you added is inserted as the first rule:

```
R2#sh ip prefix-list
ip prefix-list deny_R1_Lo0: 2 entries
    seq 1 deny 10.0.1.1/32      <-----
    seq 2 permit 0.0.0.0/0 le 32
R2#
```

Then for filtering, you can configure one of the following in R2's OSPF configuration:

```
area 0 filter-list prefix deny_R1_Lo0 out
OR
area 10 filter-list prefix deny_R1_Lo0 in
```

However, since the task does not allow you to enter the "area 0" command. You can only enter the command "area 10 filter-list prefix deny\_R1\_Lo0 in".

After configuring the filter, you should use "sh run | s router ospf" (or just "sh run") in R2 to ensure that you have entered it in the existing OSPF process.

```
R2#sh run | s router ospf
router ospf 10
  router-id 10.0.1.2
  area 10 filter-list prefix deny_R1_Lo0 in      <-----
  network 10.0.1.0 0.0.0.255 area 0
  network 10.0.2.0 0.0.0.255 area 0
  network 10.0.23.0 0.0.0.255 area 0
  network 10.1.102.0 0.0.0.255 area 10
R2#
```

#### Task 2:

Before making any configuration change for task 1, if you enter "sh ip route ospf" in R2, you should be able to find the OSPF router of the R20's lo0 i.e. "10.2.1.32". (**NOT 10.2.1.24 since the network of loopback interface is advertised by OSPF as host route by default !!!**)

In order to filter this route from leaving Area 20, the following prefix list is needed in R3:

```
ip prefix-list deny_R20_Lo0 seq 1 deny 10.2.1.1/32
ip prefix-list deny_R20_Lo0 seq 2 permit 0.0.0.0/0 le 32
```

However, seq 2 is already configured in R3, therefore you just need to enter the rule seq 1. (**Remember to add "seq 1" in the rule! Otherwise the rule will be appended at the end of the prefix list**)

After configuring the sequence 1 rule, you should use "sh ip prefix-list" in R3 to ensure that you have type the prefix-list name correctly and the rule you added is inserted as the first rule:

```
R3#sh ip prefix-list
ip prefix-list deny_R20_Lo0: 2 entries
    seq 1 deny 10.2.1.1/32      <-----
    seq 2 permit 0.0.0.0/0 le 32
R3#
```

Then for filtering, you can configure one of the following in R3's OSPF configuration:

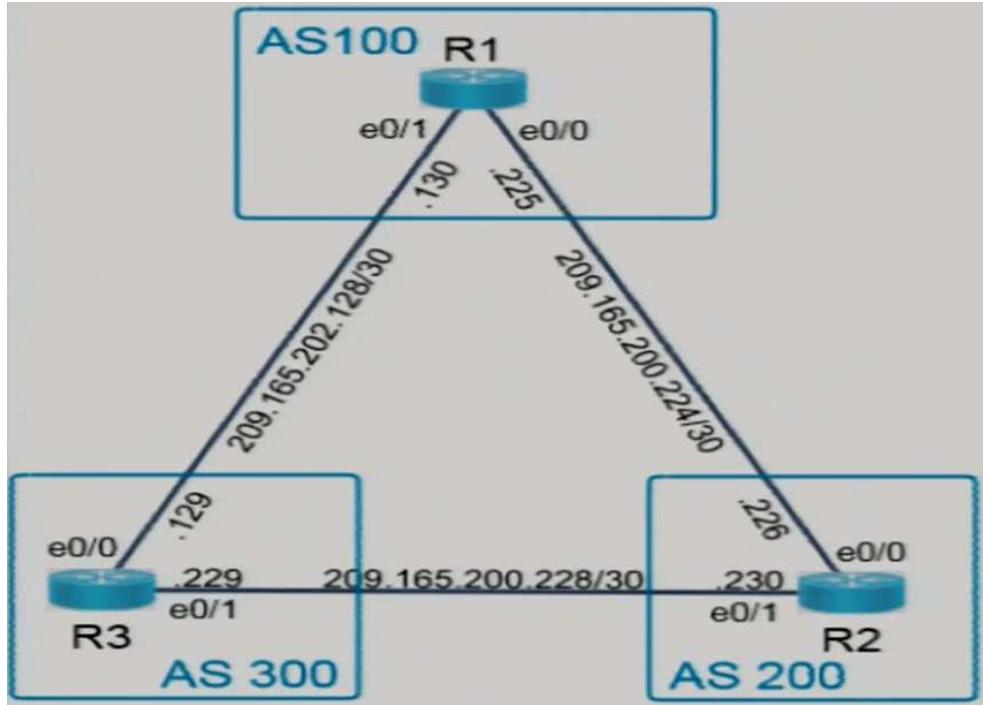
```
area 20 filter-list prefix deny_R20_Lo0 out
OR
area 0 filter-list prefix deny_R20_Lo0 in
```

However, since the task does not allow you to enter the "area 0" command. You can only enter the command "area 20 filter-list prefix deny\_R20\_Lo0 out".

After configuring the filter, you should use "sh run | s router ospf" (or just "sh run") in R3 to ensure that you have entered it in the existing OSPF process.

```
R3#sh run | s router ospf
router ospf 10
  router-id 10.0.1.3
  area 20 filter-list prefix deny_R20_Lo0 out      <-----
  network 10.0.1.0 0.0.0.255 area 0
  network 10.0.3.0 0.0.0.255 area 0
  network 10.0.23.0 0.0.0.255 area 0
  network 10.2.203.0 0.0.0.255 area 20
R3#
```

#### QUESTION 15 Topology:



**Tasks:**

Configure R1 according to the topology to achieve these results:

1. Configure eBGP using Loopback 0 for the router-id. Do not use the address-family command to accomplish this.
2. Advertise R1's Loopback 100 and Loopback 200 networks to AS200 and AS300.

**Correct Answer:**

Section: (none)

Explanation

**Explanation/Reference:**

Summarized configuration commands:

```
R1
en
config t
router bgp 100
  bgp router-id 10.1.1.1
  neighbor 209.165.200.226 remote-as 200
  neighbor 209.165.202.129 remote-as 300
  network 209.165.201.1 mask 255.255.255.255
  network 209.165.201.2 mask 255.255.255.255
end
copy run start
```

**For verification:**

You can use "sh ip bgp" in R1 to find the local router ID is "10.1.1.1".

You can use "sh ip route bgp" in R2 and R3 to find the two BGP routes "209.165.201.1/32" and "209.165.201.2/32" learnt from R1.

**Explanations:**

The following configuration should be found in the routers. You can verify them through "sh run" in the concerned router.

```
R1
interface Loopback0
  ip address 10.1.1.1 255.255.255.255
!
interface Loopback100
  ip address 209.165.201.1 255.255.255.255
!
interface Loopback200
  ip address 209.165.201.2 255.255.255.255
```

```
R2
router bgp 200
  neighbor 209.165.200.225 remote-as 100
  neighbor 209.165.200.229 remote-as 300
!
  address-family ipv4
    neighbor 209.165.200.225 activate
    neighbor 209.165.200.229 activate
  exit-address-family
```

```
R3
router bgp 300
  neighbor 209.165.200.230 remote-as 200
  neighbor 209.165.202.130 remote-as 100
!
  address-family ipv4
    neighbor 209.165.200.230 activate
    neighbor 209.165.202.130 activate
  exit-address-family
```

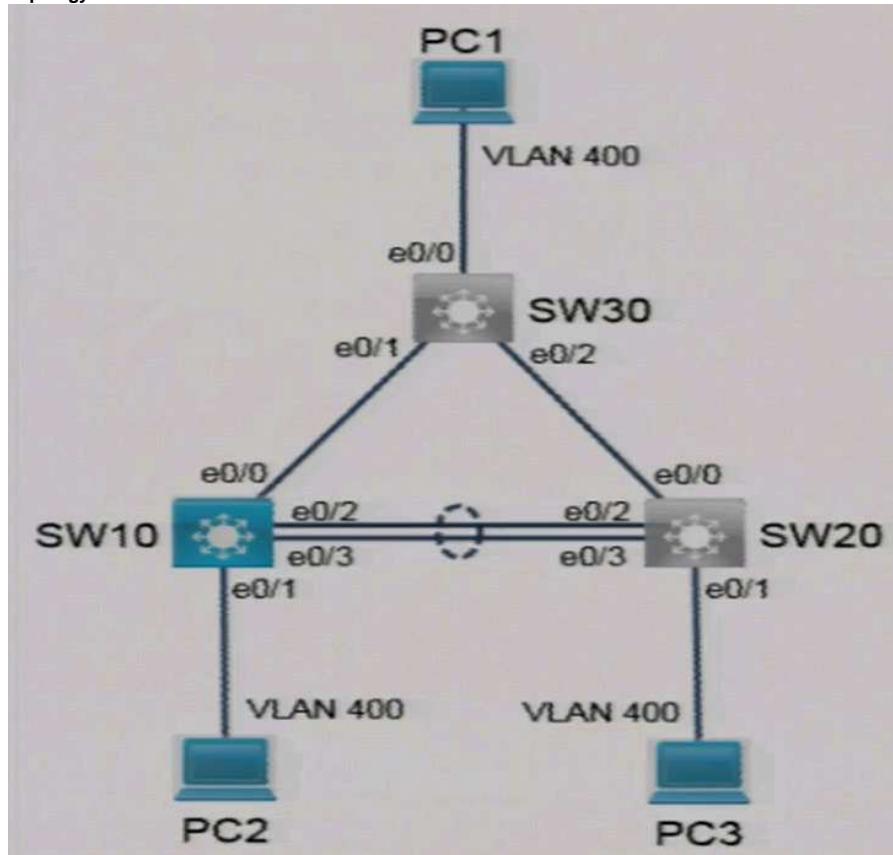
BGP has already been configured in R2 and R3. From their configurations, they are configured to form neighbor with R1 using R1's Ethernet interface's IP address ("209.165.200.225" or "209.165.202.130"). Hence when configure BGP in R1, you should configure the IP address of the Ethernet interfaces of R2 and R3 for forming neighbor.

For configuring Router ID, you need to use "bgp router-id" command with the IP address configured for the R1's Loopback0 interface.

In order to advertise Loopback100 and Loopback200, you can just configure the "network" command for them. Note that the mask in the "network" command must match the IP subnet mask of the loopback interface.

#### QUESTION 16

Topology:



#### Tasks:

The operations team started configuring network devices for a new site. Complete the configurations to achieve these goals:

1. Configure SW10 to utilize 32-bit values when calculating spanning-tree port cost.
2. The trunk between SW10 and SW30 is not operational. Troubleshoot the issue and ensure PC2 can ping PC1 (10.10.100.10) across the link.
3. The port channel between SW10 and SW20 is not operational. The switches should negotiate the port channel but this is not occurring. Troubleshoot the issue and ensure PC2 can ping PC3 (10.10.100.30) across the port-channel.

**Note:** No access is provided to SW20 or SW30. Resolve these issues by making changes only to SW10. Traffic on all trunks should be restricted to only active VLANs.

**Correct Answer:**

**Section:** (none)

**Explanation**

**Explanation/Reference:**  
Ans:

#### Task 1:

```
SW10
en
config t
spanning-tree pathcost method long
end
copy run start
```

#### Task 2:

```
SW10
en
config t
int e0/0
switchport trunk encapsulation dot1q
switchport mode trunk
end
copy run start
```

For verification, after a while (or you can check the status of spanning tree with "sh spanning-tree"

vlan 400" to see if int e0/0 reaches Forwarding state), then you can ping PC1 from PC2 using the following command:

```
PC2
ping 10.10.100.10
```

**Task 3:**

```
SW10
en
config t
int range e0/2-3
  channel-group 10 mode active
end
copy run start
```

For verification, after a while (or you can check the status of spanning tree with "sh spanning-tree vlan 400" to see if int Po10 reaches Forwarding state), then you can ping PC3 from PC2 using the following command:

```
PC2
ping 10.10.100.30
```

**Explanations:**

**Task 1** is straight-forward since you just need to enter the global configuration command "spanning-tree pathcost method long" in SW10.

**For Task 2**, the existing configuration for e0/0 in SW10 is as follows (you should check it using e.g.

```
"sh run int e0/0")
interface Ethernet0/0
  switchport access vlan 400
  switchport mode access
```

However, since task 2 requires you to setup trunk between SW10 and SW20, this interface should be re-configured as a trunk port as follows:

```
int e0/0
  switchport trunk encapsulation dot1q
  switchport mode trunk
```

PC2 should be able to ping PC1 after the above configuration and VLAN 400 of the port e0/0 reaches forwarding state.

**For Task 3**, the existing configuration in SW10 does not have any port channel configured (you should check this using e.g. "sh run int e0/2", "sh run int e0/3" ... etc.)

Since the question requires that SW10 should connect to SW20 through port channel using e0/2 and e0/3, you need to configure those two interfaces using the interface configuration mode command "channel-group" as follows (since no port channel has been configured, you can use any channel-group number instead of "10" in the suggested answer).

```
int range e0/2-3
  channel-group 10 mode active
```

PC2 should be able to ping PC3 after the above configuration and VLAN 400 of the port Po10 reaches forwarding state.

Remarks :

If ping is not successful and the interface Po10 is down (e.g.: using "sh etherchannel summary")  
10 Po10(SD) LACP Ethernet0/2(s) Ethernet0/3(s)

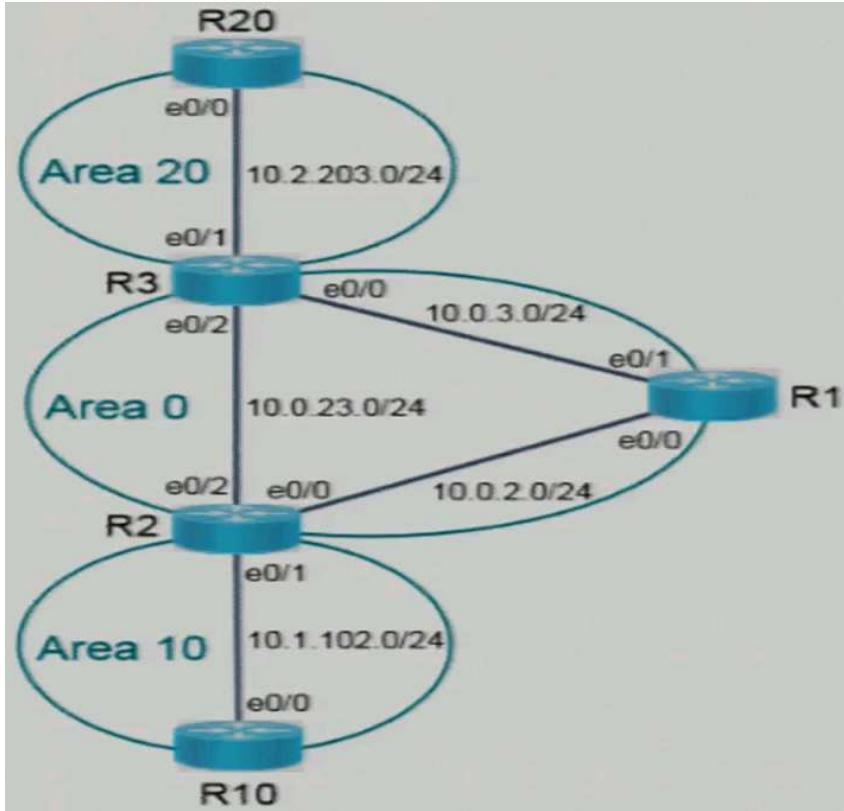
Then may be the question has changed and SW20 is configured to use PAgP for negotiation instead. In this case, you should try changing the configuration as follows and test the connection again.

```
SW10
en
config t
int range e0/2-3
  no channel-group 10 mode active
  channel-group 10 mode desirable
end
```

If ping is now successful after changing to PAgP, you should remember to save the configuration using "copy run start".

**QUESTION 17**

**Topology:**



**Tasks:**

OSPF is partially configured. Complete the OSPF configurations to achieve these goals:

1. Configure OSPF on router R1 according to the topology so that all networks are advertised. Do not use the network statement under the "router ospf" configuration section to accomplish this task.
2. Configure a single command on the ABR routers to ensure only one summary route is advertised to area 0.

**Correct Answer:**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**Ans:**

**Task 1:**

```
R1
en
config t
int lo0
 ip ospf 1 area 0
int e0/0
 ip ospf 1 area 0
int e0/1
 ip ospf 1 area 0
end
copy run start
```

**Task 2:**

```
R2
en
config t
router ospf 10
 area 10 range 10.1.0.0 255.255.0.0
end
copy run start
```

```
R3
en
config t
router ospf 10
 area 20 range 10.2.0.0 255.255.0.0
end
copy run start
```

**Explanations:**

**Task 1:**

Since you need to advertise all networks of R1, you can need to check all the networks configured in R1 using e.g. "sh run" or "sh ip int brief". Assume the result is as follows i.e. there are 3 networks due to the IP addresses configured in 3 interfaces.

```

interface Loopback0
  ip address 10.0.1.1 255.255.255.0
!
interface Ethernet0/0
  ip address 10.0.2.1 255.255.255.0
  duplex auto
!
interface Ethernet0/1
  ip address 10.0.3.1 255.255.255.0
  duplex auto
!
interface Ethernet0/2
  no ip address
  duplex auto
!
interface Ethernet0/3
  no ip address
  duplex auto

```

OSPF is NOT configured in R1. In order to advertise all the networks without configuring anything under "router ospf", you can configure the interface mode configuration command "ip ospf 1 area 0" (note that you can use any process ID other than the number "1" here) under each of the interfaces configured with IP addresses as shown in the suggested answer.

After configuring the required commands, neighbors should be formed with R2 and R3 by R1. Moreover, you can find OSPF routes in R1's routing table.

```

R1#sh ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 17 subnets, 2 masks
O    10.0.1.2/32 [110/2] via 10.0.2.2, 00:01:19, Ethernet0/0
O    10.0.1.3/32 [110/2] via 10.0.3.3, 00:01:19, Ethernet0/1
O    10.0.23.0/24 [110/2] via 10.0.3.3, 00:01:19, Ethernet0/1
                  [110/2] via 10.0.2.2, 00:01:19, Ethernet0/0
O IA   10.1.1.1/32 [110/3] via 10.0.2.2, 00:01:19, Ethernet0/0
O IA   10.1.100.10/32 [110/3] via 10.0.2.2, 00:01:19, Ethernet0/0
O IA   10.1.102.0/24 [110/2] via 10.0.2.2, 00:01:19, Ethernet0/0
O IA   10.1.200.10/32 [110/3] via 10.0.2.2, 00:01:19, Ethernet0/0
O IA   10.2.1.1/32 [110/3] via 10.0.3.3, 00:01:19, Ethernet0/1
O IA   10.2.100.20/32 [110/3] via 10.0.3.3, 00:01:19, Ethernet0/1
O IA   10.2.200.20/32 [110/3] via 10.0.3.3, 00:01:19, Ethernet0/1
O IA   10.2.203.0/24 [110/2] via 10.0.3.3, 00:01:19, Ethernet0/1
R1#

```

#### **Task 2:**

After configuring task 1, there are many individual OSPF inter-area routes (those marked with "IA"). Those inter-area routes having the form "10.1.x.x" with next hop "10.0.2.2" are learnt from area 10 and those inter-area routes having the form "10.2.x.x" with next hop "10.0.3.3" are learnt from area 20.

In this task, you need to configure the ABRs so that only one summary route will be advertised into area 0 from the other two areas. The simplest way is to configure the summary route 10.1.0.0/16 with the router configuration mode command "area 10 range 10.1.0.0 255.255.0.0" in R2 and configure the summary route 10.2.0.0/16 with the router configuration mode command "area 20 range 10.2.0.0 255.255.0.0" in R3.

However, in order to configure the command in R2 and R3, you need to find out the existing OSPF process ID being currently used by R2 and R3. Assume the existing OSPF configurations in R2 and R3 are as follows:

```

R2:
R2# sh run | s router
router ospf 10
  router-id 10.0.1.2
  network 10.0.1.0 0.0.0.255 area 0
  network 10.0.2.0 0.0.0.255 area 0
  network 10.0.23.0 0.0.0.255 area 0
  network 10.1.102.0 0.0.0.255 area 10
R2#

```

```

R3:
R3#sh run | s router
router ospf 10
  router-id 10.0.1.3
  network 10.0.1.0 0.0.0.255 area 0
  network 10.0.3.0 0.0.0.255 area 0
  network 10.0.23.0 0.0.0.255 area 0
  network 10.2.203.0 0.0.0.255 area 20
R3#

```

Then:

In R2, you should configure the router configuration mode command "area 10 range 10.1.0.0

255.255.0.0" under "router ospf 10".

In R3, you should configure the router configuration mode command "area 20 range 10.2.0.0 255.255.0.0" under "router ospf 10".

After configuring the above commands, only two OSPF inter-area routes (one from each area) will be shown in R1:

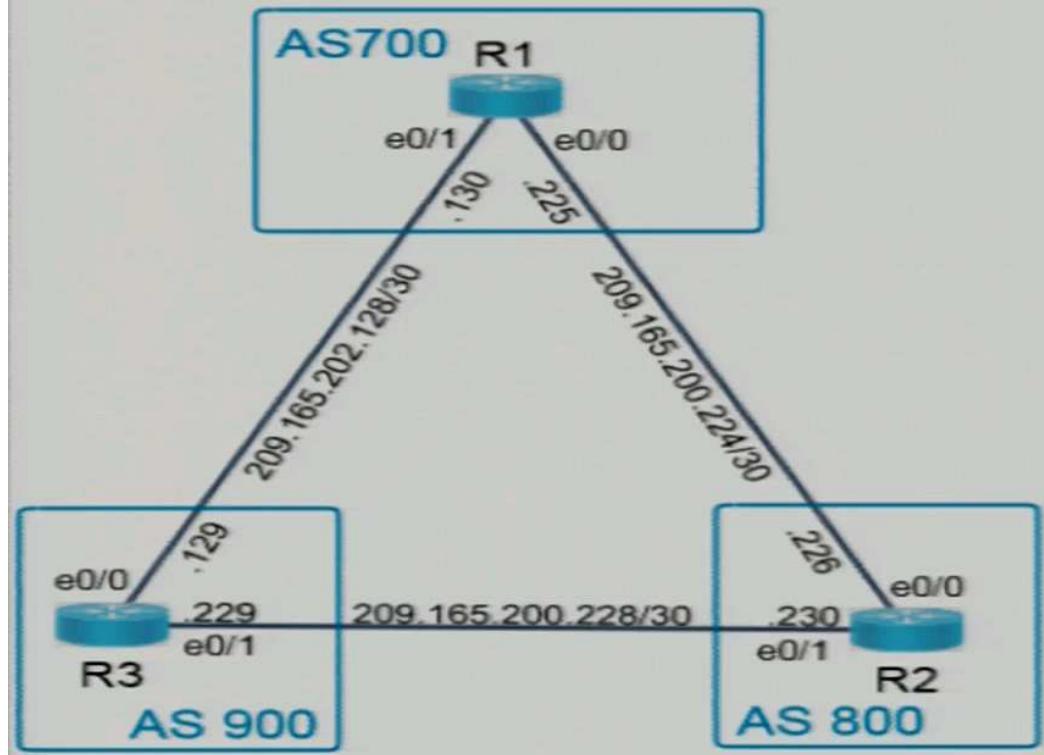
```
R1#sh ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override, p - overrides from PfR
```

Gateway of last resort is not set

```
10.0.0.0/8 is variably subnetted, 11 subnets, 3 masks
O 10.0.1.2/32 [110/2] via 10.0.2.2, 01:58:02, GigabitEthernet0/3
O 10.0.1.3/32 [110/2] via 10.0.3.3, 01:58:02, GigabitEthernet0/4
O 10.0.23.0/24 [110/2] via 10.0.3.3, 01:58:02, GigabitEthernet0/4
          [110/2] via 10.0.2.2, 01:58:02, GigabitEthernet0/3
O IA 10.1.0.0/16 [110/2] via 10.0.2.2, 00:00:12, GigabitEthernet0/3
O IA 10.2.0.0/16 [110/2] via 10.0.3.3, 00:00:04, GigabitEthernet0/4
R1#
```

#### QUESTION 18

Topology:



#### Tasks:

Configure R3 according to the topology to achieve these results:

1. Configure eBGP using Loopback 0 for the router-id. Do not use the address-family command to accomplish this.
2. Advertise R3's Loopback 100 and Loopback 200 networks to AS800 and AS700.

Correct Answer:

Section: (none)

Explanation

#### Explanation/Reference:

Ans:

```
R3
en
config t
router bgp 900
  bgp router-id 10.3.3.3
  network 209.165.201.4 mask 255.255.255.255
  network 209.165.201.5 mask 255.255.255.255
  neighbor 209.165.202.130 remote-as 700
  neighbor 209.165.200.230 remote-as 800
end
copy run start
```

#### Explanations:

With the command "sh run" or "sh run | s router", you should find that BGP is NOT configured in R3. In the network diagram, R3 is in AS 900. Therefore, you should setup BGP using the global configuration mode command "router bgp 900".

In order to use R3's loopback 0 as the Router ID for BGP, you need to find the IP address of this interface e.g.:

```
R3#sh run int lo0
Building configuration...
Current configuration : 80 bytes
!
interface Loopback0
 ip address 10.3.3.3 255.255.255.0
end
R3#
```

Then you can configure the router configuration mode command "bgp router-id 10.3.3.3" within the BGP configuration (i.e. under "router bgp 900").

In order to advertise Loopback 100 and Loopback 200, you need also to find networks of the two interfaces and configure them using the router configuration mode commands "network" under the BGP configuration of R3. Assume:

```
R3#sh run int lo100
Building configuration...
Current configuration : 80 bytes
!
interface Loopback100
 ip address 209.165.201.4 255.255.255.255
end
R3#
R3#sh run int lo200
Building configuration...
Current configuration : 80 bytes
!
interface Loopback200
 ip address 209.165.201.5 255.255.255.255
end
R3#
```

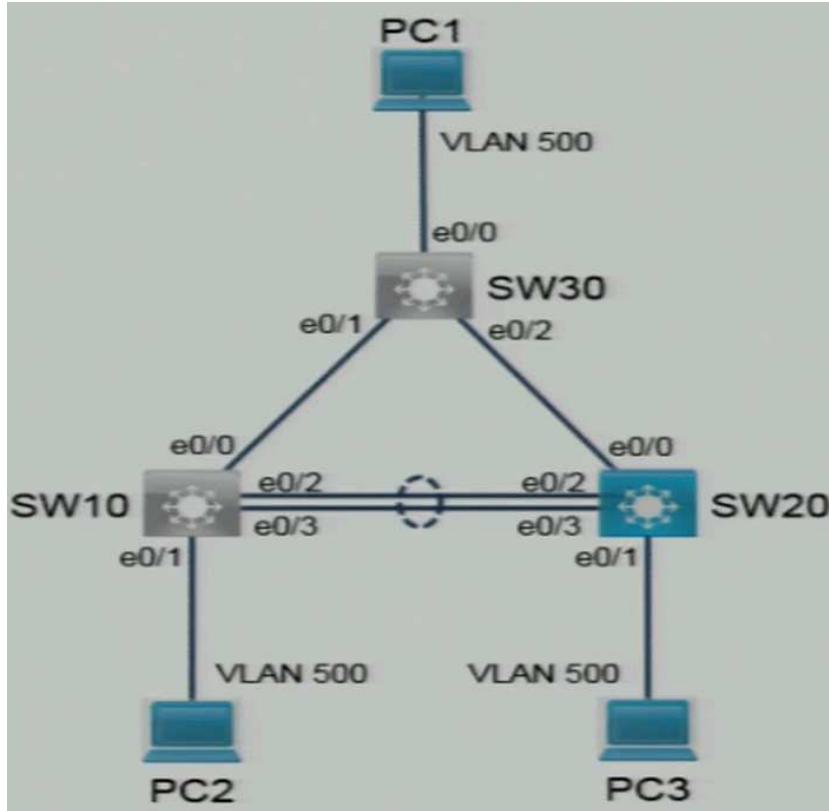
If the IP addresses of the two loopback interfaces are as above, you should configure the router configuration mode commands "network 209.165.201.4 mask 255.255.255.255" and "network 209.165.201.5 mask 255.255.255.255" under the BGP configuration of R3.

Finally, in order to advertise the two networks to other ASes, you need to form neighbors with the remote ASes. Hence, you also need to configure the router configuration mode commands "neighbor" under the BGP configuration of R3. The IP address and the AS number of the neighbor router used in the suggested answer can be found in the diagram.

After configuring the above, you should be able to find two BGP neighbors formed with the command "sh ip bgp" in R3. Moreover, you should be able to find the two BGP routes "209.165.201.4/32" and "209.165.201.5/32" in the output of "sh ip route bgp" from both R1 and R2.

#### QUESTION 19

**Topology:**



**Tasks:**

The operations team started configuring network devices for a new site. Complete the configurations to achieve these goals:

1. Configure Rapid PVST+ on SW20.
2. The trunk between SW20 and SW30 is not operational. Troubleshoot the issue and ensure PC3 can ping PC1 (10.10.100.10) across the link.
3. The LACP port channel between SW10 and SW20 is not operational. Troubleshoot the issue and ensure PC3 can ping PC2 (10.10.100.20) across the port channel.

**Note:** No access is provided to SW10 or SW30. Resolve these issues by making changes only to SW20. Traffic on all trunks should be restricted to only active VLANs.

**Correct Answer:**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**Ans:**

```
SW20
en
config t
spanning-tree mode rapid-pvst
int e0/0
switchport trunk encapsulation dot1q
switchport mode trunk
int po10
switchport trunk encapsulation dot1q
switchport mode trunk
end
copy run start
```

**Explanations:**

Using the command "sh run" in SW20, you should find the configuration of the interfaces as follows (only interfaces with settings / used in the question are shown below):

```
interface Port-channel10
switchport mode access
!
interface Ethernet0/0
switchport mode access
!
interface Ethernet0/1
switchport access vlan 500
switchport mode access
spanning-tree portfast edge
!
interface Ethernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 10 mode active
!
interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 10 mode active
```

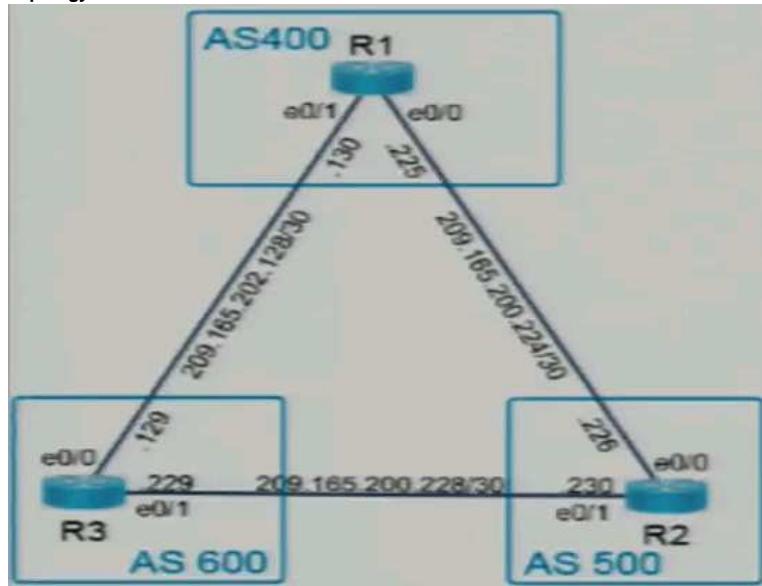
For task 1, you need to configure the global configuration mode command "spanning-tree mode rapid-pvst".

For task 2, since the interface e0/0 is configured as access port, it cannot form trunk with SW30. You should configure the interface as a trunk port. (Although you do not know the setup of the trunk port in SW30, the trunk settings in SW20's e0/2 can be used as a reference). After configuring e0/0 with the commands shown in the suggested answer and wait a while, PC3 should be able to use the command "ping 10.10.100.10" to ping PC1.

For task 3, LACP port channel has been setup in the interfaces e0/2 and e0/3 of SW10. However, the corresponding Port-channel interface Po10 contains settings that are not matching to those of the two individual interfaces e0/2 and e0/3. Therefore the Etherchannel cannot be up properly. Hence, you need to modify the settings in Po10 so that they match those in e0/2 and e0/3 in order to fix the problem. After configuring Po10 with the commands as shown in the suggested answer and wait a while, PC3 should now be able to use the command "ping 10.10.100.20" to ping PC2.

#### QUESTION 20

##### Topology:



##### Tasks:

Configure R2 according to the topology to achieve these results:

1. Configure eBGP using Loopback 0 for the router-id. Do not use the address-family command to accomplish this.
2. Advertise R2's Loopback 100 and Loopback 200 networks to AS400 and AS600.

##### Correct Answer:

Section: (none)

Explanation

##### Explanation/Reference:

Ans:

```
R2
en
config t
router bgp 500
  bgp router-id 10.2.2.2
  network 209.165.201.9 mask 255.255.255.255
  network 209.165.201.10 mask 255.255.255.255
  neighbor 209.165.200.225 remote-as 400
  neighbor 209.165.200.229 remote-as 600
end
copy run start
```

##### Explanations:

With the command "sh run" or "sh run | s router", you should find that BGP is NOT configured in R2. In the network diagram, R2 is in AS 500. Therefore, you should setup BGP using the global configuration mode command "router bgp 500".

In order to use R2's loopback 0 as the Router ID for BGP, you need to find the IP address of this interface e.g.:

```
R2#sh run int lo0
Building configuration...
Current configuration : 80 bytes
!
interface Loopback0
  ip address 10.2.2.2 255.255.255.0
end

R2#
```

Then you can configure the router configuration mode command "bgp router-id 10.2.2.2" within the BGP configuration (i.e. under "router bgp 500").

In order to advertise Loopback 100 and Loopback 200, you also need to find networks of these two interfaces and configure them using the router configuration mode commands "network" under the BGP configuration of R2. Assume:

```
R2#sh run int lo100
Building configuration...
Current configuration : 80 bytes
!
interface Loopback100
 ip address 209.165.201.9 255.255.255.255
end

R2#
R2#sh run int lo200
Building configuration...
Current configuration : 80 bytes
!
interface Loopback200
 ip address 209.165.201.10 255.255.255.255
end

R2#
```

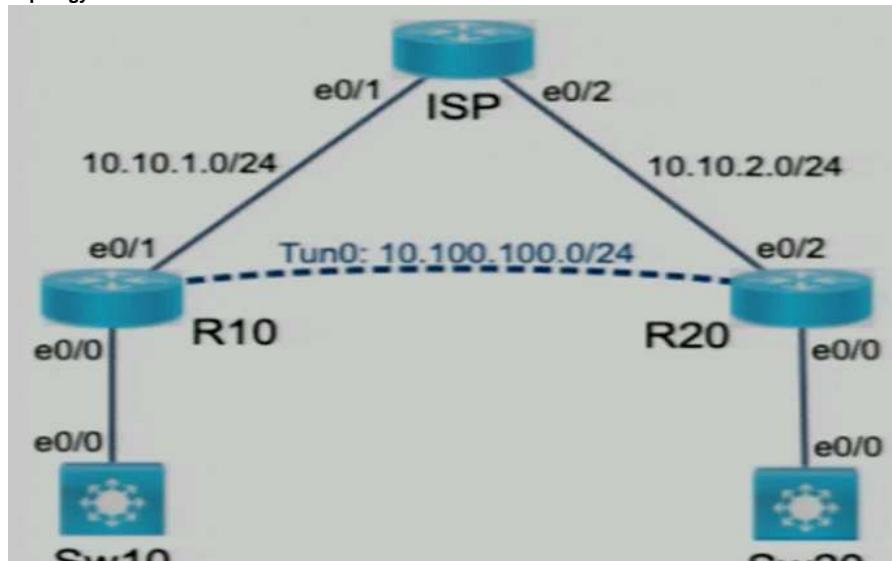
If the IP addresses of the two loopback interfaces are those shown in the above, you should configure the router configuration mode commands "network 209.165.201.9 mask 255.255.255.255" and "network 209.165.201.10 mask 255.255.255.255" under the BGP configuration of R2.

Finally, in order to advertise the two networks to other 2 ASes, you need to form BGP neighbors with those remote ASes. Hence, you also need to configure the router configuration mode commands "neighbor" under the BGP configuration of R2. The IP address and the AS number of the neighbor router used in the suggested answer can be found in the diagram.

After configuring the above, you should be able to find two BGP neighbors with the command "sh ip bgp" in R2. Moreover, you should be able to find the two BGP routes "209.165.201.9/32" and "209.165.201.10/32" in the output of "sh ip route bgp" from both R1 and R3.

#### QUESTION 21

**Topology:**



SITE	VRF	VLAN	SUBNET	GATEWAY
R10	CORP	100	10.100.1.0/24	10.100.1.1
R20	CORP	101	10.101.2.0/24	10.101.2.1

**Tasks:**

The operations team started configuring network devices for a new site. R10 and R20 are preconfigured with the CORP VRF. R10 has network connectivity to R20. Complete the configurations to achieve these goals:

1. Extend the CORP VRF between R10 and R20 using Tunnel0.
2. Configure static routing on R10 and R20 so that users in VLAN 100 and VLAN 101 that belong to the CORP VRF are able to communicate with each other. Tunnel0 should be the only interface used to route traffic for the CORP VRF.

**Correct Answer:**  
Section: Selected  
Explanation

**Explanation/Reference:****Ans:**

```
R10
en
config t
int tu0
  vrf forwarding CORP
  ip addr 10.100.100.1 255.255.255.0
  tunnel source 10.10.1.1
  tunnel destination 10.10.2.1
  exit
ip route vrf CORP 10.101.2.0 255.255.255.0 tu0 10.100.100.2
end
copy run start
```

```
R20
en
config t
int tu0
  vrf forwarding CORP
  ip addr 10.100.100.2 255.255.255.0
  tunnel source 10.10.2.1
  tunnel destination 10.10.1.1
  exit
ip route vrf CORP 10.100.1.0 255.255.255.0 tu0 10.100.100.1
end
copy run start
```

**For verification:**

You can find the IP addresses of Sw10 and Sw20 and then try to ping each other. Or you can just use the following for verification.

```
R10
ping 10.101.2.1 source 10.100.1.1
```

```
R20
ping 10.100.1.1 source 10.101.2.1
```

**Explanations:**

You should use "sh run" or "sh run int tu0" in R10 and R20 to check if their Tunnel 0 configuration settings are as follows:

```
R10
int tu0
  ip addr 10.100.100.1 255.255.255.0
```

```
R20
int tu0
  ip addr 10.100.100.2 255.255.255.0
```

If no VRF is configured in the tunnel interface as shown above, you need to assign the VRF and then set the IP address again as shown in the suggested answer. However, if VRF "CORP" has been configured in the loopback interface, you can skip the interface configuration mode commands for assigning VRF and IP address for the loopback interface.

In order to form the tunnel between R10 and R20 through the ISP, you need to use R10's e0/1 (i.e. 10.10.1.1) and R20's e0/2 (i.e. 10.10.2.1) as tunnel source and destination. Hence, the followings have to be configured.

```
R10
int tu0
  tunnel source 10.10.1.1
  tunnel destination 10.10.2.1
```

```
R20
int tu0
  tunnel source 10.10.2.1
  tunnel destination 10.10.1.1
```

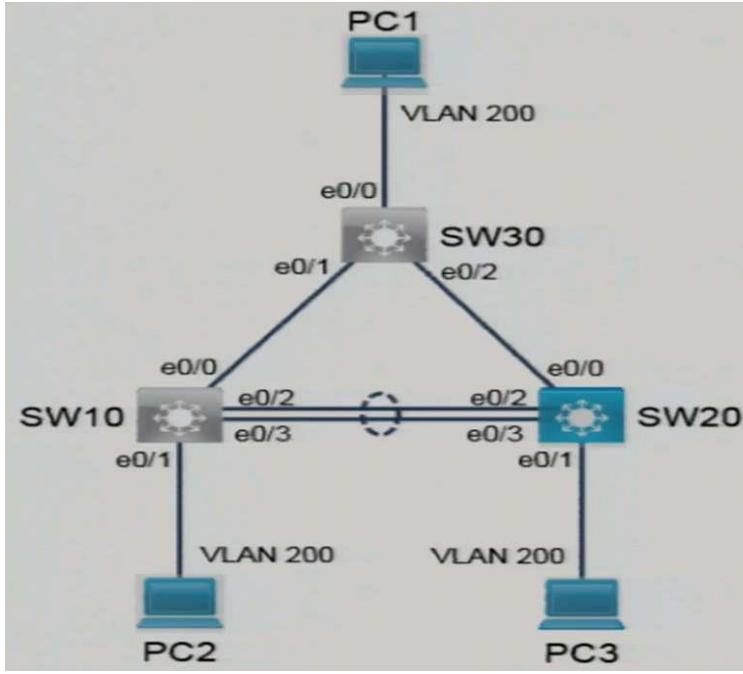
In order for R10 to send vrf CORP traffic for R20's subnet (i.e. 10.101.2.0/24) to R20 through the tunnel, you need the following static route in R10 using R20's tunnel IP (i.e. 10.100.100.2) as next hop. Interface is specified in the static route since the task 2 required that Tunnel 0 should be the only interface used to route traffic.

```
R10
ip route vrf CORP 10.101.2.0 255.255.255.0 tu0 10.100.100.2
```

In order for R20 to send vrf CORP traffic for R10's subnet (i.e. 10.100.1.0/24) to R10 through the tunnel, you need the following static route in R20 using R10's tunnel IP (i.e. 10.100.100.1) as next hop. Interface is specified in the static route since the task 2 required that Tunnel 0 should be the only interface used to route traffic.

```
R20
ip route vrf CORP 10.100.1.0 255.255.255.0 tu0 10.100.100.1
```

**QUESTION 22****Topology:**



**Tasks:**

The operations team started configuring network devices for a new site. Complete the configurations to achieve these goals:

1. Configure SW20 to utilize 32-bit values when calculating spanning-tree port cost.
2. The trunk between SW20 and SW30 is not operational. Troubleshoot the issue and ensure PC3 can ping PC1 (10.10.100.10) across the link.
3. The LACP port channel between SW10 and SW20 is not operational. Troubleshoot the issue and ensure PC3 can ping PC2 (10.10.100.20) across the port channel.

Note: No access is provided to SW10 or SW30. Resolve these issues by making changes only to SW20. Traffic on all trunks should be restricted to only active VLANs.

**Correct Answer:**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**Ans:**

```

SW20
en
config t
spanning-tree pathcost method long
int e0/0
  switchport trunk allowed vlan add 200
  switchport trunk encapsulation dot1q
  switchport mode trunk
int range e0/2-3
  channel-group 10 mode active
end
copy run start

verification:
You can enter the following ping commands in PC3 and their results should be successful.
- ping 10.10.100.10
- ping 10.10.100.20

```

**Explanations:**

Using the command "sh run" in SW20, you should find the following settings pre-configured:

```

interface Port-channel10
  switchport trunk allowed vlan 1,200
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Ethernet0/0
  switchport trunk allowed vlan 1
  switchport trunk encapsulation isl
!
interface Ethernet0/1
  switchport access vlan 200
  switchport mode access
!
interface Ethernet0/2
  switchport trunk allowed vlan 1,200
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Ethernet0/3
  switchport trunk allowed vlan 1,200
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Vlan1

```

ip address 10.10.1.20 255.255.255.0

#### Task 1

You need to configure the global configuration mode command "spanning-tree pathcost method long".

#### Task 2

The interface e0/0 is configured with ISL encapsulation but no trunk is formed (you can use "sh int trunk" to prove e0/0 is not a trunk). This may occur due to:

- no negotiation of trunk port in the other switch (Sw30). This can be solved by "switchport mode trunk"
- the trunk encapsulation is different in the other switch (Sw30). This can be solved by "switchport trunk encapsulation dot1q".

The suggested answer assume that both are required.

Since PC1 and PC3 are both in VLAN 200, in order for them to communicate with each other, the trunk in SW20's e0/0 must allow VLAN 200. However, only VLAN 1 is allowed in the pre-configured setting in e0/0. Hence you need to add VLAN 200 to the allowed list using "switchport trunk allowed vlan add 200".

The following shows the configuration needed for the above two:

```
int e0/0
switchport trunk allowed vlan add 200
switchport trunk encapsulation dot1q
switchport mode trunk
```

After the above configuration, you need to wait a while (due to spanning tree). Then, you can go to PC3 and enter the command "ping 10.10.100.10" for pinging PC1. The result should be successful.

#### Task 3

Although the Port-channel interface Po10 can be found, the individual interfaces i.e. e0/2 and e0/3 are not configured with LACP.

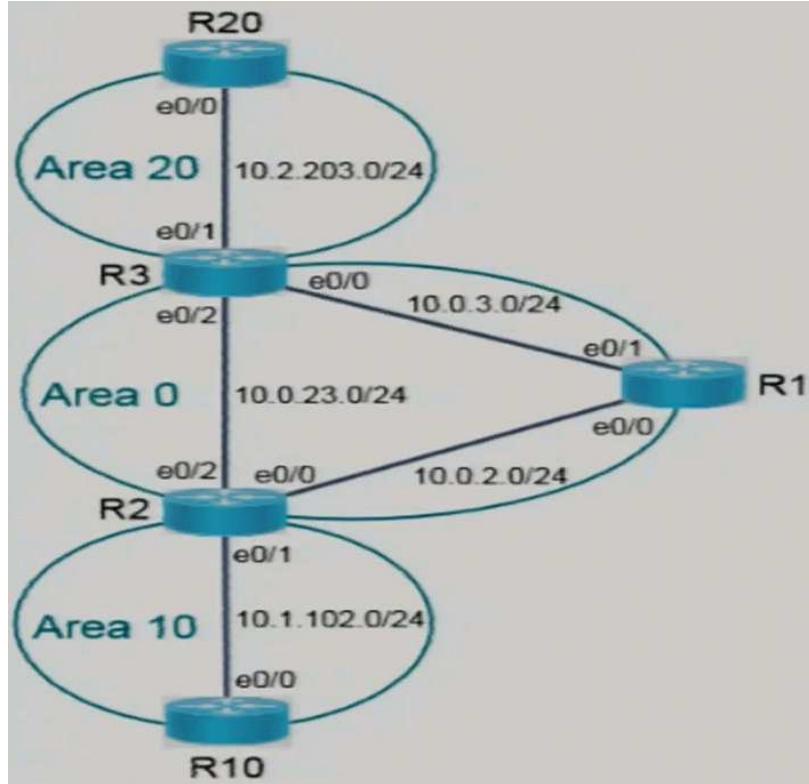
You can use the following command to assign those two interfaces to channel-group 10 so that the pre-configured port-channel interface Po10 can be used.

```
int range e0/2-3
channel-group 10 mode active
```

After the above configuration, you need to wait a while (due to spanning tree). Then, you can go to PC3 and enter the command "ping 10.10.100.20" for pinging PC2. The result should be successful.

#### QUESTION 23

Topology:



#### Tasks:

OSPF is partially configured on all devices. Complete the configurations to achieve these results:

1. Configure R3 so that R20 is always designated as the BDR.
2. Configure R10 so that it does not participate in the DR/BDR election. Do not use the ip ospf network point-to-point command under the interface configuration to accomplish this task.

#### Correct Answer:

Section: (none)

Explanation

#### Explanation/Reference:

Ans:

```
R3
en
config t
int e0/1
  ip ospf priority 255
end
copy run start
```

```
R20
en
clear ip ospf process
```

```
R10
en
config t
int e0/0
  ip ospf priority 0
end
copy run start
```

#### Verification:

##### For Task 1:

Verification can be performed in R3 by the command "sh ip ospf int e0/1" (or "sh ip ospf nei" in R20)

- Before configuring the above answer, the following can be found in the output of "sh ip ospf int e0/1" in R3:

Transmit Delay is 1 sec, State BDR, Priority 1

- After configuring the above answer and clear the OSPF process in R20, the following can be found in the output of "sh ip ospf int e0/1" in R3:

Transmit Delay is 1 sec, State DR, Priority 255

##### For Task 2:

Verification can be performed in R10 by the command "sh ip ospf int e0/0" (or "sh ip ospf nei" in R2)

- Before configuring the above answer, the following can be found in the output of "sh ip ospf int e0/0" in R10:

Transmit Delay is 1 sec, State DR, Priority 1

- After configuring the above answer, the following can be found in the output of "sh ip ospf int e0/0" in R10:

Transmit Delay is 1 sec, State DROTHER, Priority 0

#### Explanations:

##### Task 1

Since the only OSPF neighbor of R20 is R3, in order to make R20 to be BDR, you need to configure R3 as the DR. This can be done by setting R3's interface connecting to R20 i.e. e0/1 to have the highest OSPF priority i.e. 255

```
int e0/1
  ip ospf priority 255
```

In order to verify the result, you need to bring down the OSPF of the existing DR i.e. R20 first. You can achieve this by running the privileged mode command "clear ip ospf process" (answer "yes").

##### Task 2

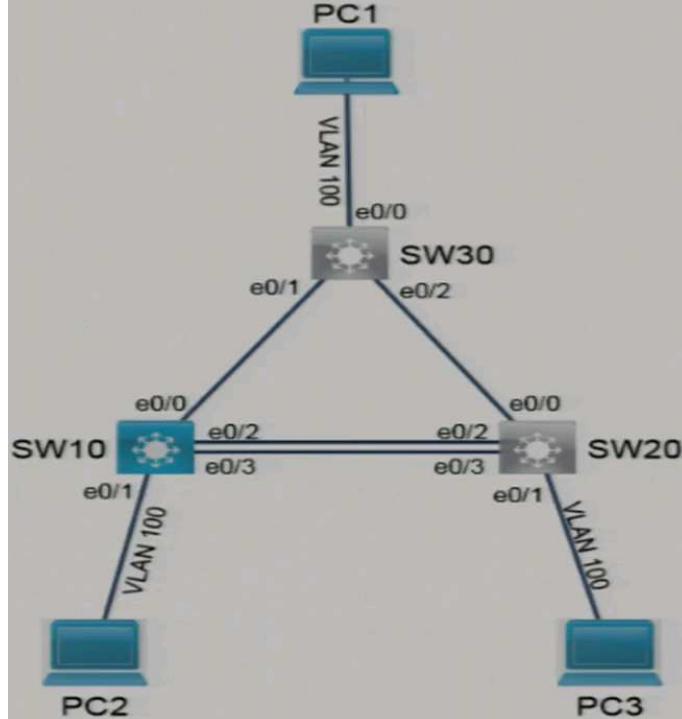
Since the only OSPF neighbor of R10 is R2, in order to prevent R10 from participating in DR/BDR election, you can set R10's interface connecting to R2 i.e. e0/0 to have 0 as the OSPF priority.

```
int e0/0
  ip ospf priority 0
```

Note that this setting is effective immediately and therefore you do not need to run the privileged mode command "clear ip ospf process" in any router.

#### QUESTION 24

##### Topology:



##### Tasks:

The operations team started configuring network devices for a new site. Complete the configurations to achieve these goals:

- Configure interface e0/1 on SW10 so that packet forwarding begins immediately after the link-state moves to UP.
- The trunk between SW10 and SW30 is not operational. It should actively attempt to convert to a trunk but it does not. Troubleshoot the issues and ensure PC2 can ping PC1 (10.10.100.10) across the link.
- The LACP port channel between SW10 and SW20 is not operational. Troubleshoot the issues and ensure PC2 can ping PC3 (10.10.100.30) across the port-channel.

Note: No access is provided to SW20 or SW30. Resolve these issues by making changes only to SW10. Traffic on all trunks should be restricted to only active VLANs.

**Correct Answer:**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**Ans:**

```
SW10
en
config t
int e0/0
  switchport trunk allowed vlan 1,100
  switchport trunk dynamic desirable
int e0/1
  spanning-tree portfast edge
int range e0/2-3
  channel-group 10 mode active
end
copy run start
```

**Verification:**

You can enter the following ping commands in PC2 and their results should be successful.

```
- ping 10.10.100.10
- ping 10.10.100.30
```

**Explanations:**

Using the command "sh run" in SW10, you should find the following settings pre-configured:

```
interface Port-channel10
  switchport trunk allowed vlan 1,100
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Ethernet0/0
  switchport trunk allowed vlan 1,10
  switchport trunk encapsulation dot1q
!
interface Ethernet0/1
  switchport access vlan 100
  switchport mode access
!
interface Ethernet0/2
  switchport trunk allowed vlan 1,100
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Ethernet0/3
  switchport trunk allowed vlan 1,100
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Vlan1
  ip address 10.10.1.10 255.255.255.0
```

**Task 1**

According to the diagram, SW10's interface e0/1 only needs to pass VLAN 100 traffic. Since the interface is pre-configured as an access port of VLAN 100, there is no need to change this setting. Therefore, you just need to configure "portfast" in the interface e0/1 using the Interface configuration mode command "spanning-tree portfast edge" i.e.:

```
int e0/1
  spanning-tree portfast edge
```

**Task 2**

The trunk link between SW10 and SW30 is not operational. Since SW10 is connecting to SW30 through the interface e0/0, you need to configure this interface. The task requires the interface to actively attempt to convert to a trunk, therefore you need to setup "switchport trunk dynamic desirable" in the interface. Moreover, the pre-configured setting for the interface e0/0 only allows VLAN 1 and VLAN 10. However, since PC2 needs to access PC1 and both PCs are in VLAN 100, you need to allow VLAN 100 in the trunk.

Combining the two settings above, the followings are needed in the interface e0/0:

```
int e0/0
  switchport trunk allowed vlan 1,100
  switchport trunk dynamic desirable
```

Remarks : VLAN 10 is not added in the allowed VLAN list since the note mentioned that all trunks should be restricted to only active VLANs.

You can enter "sh int trunk" in SW10 to check if the interface e0/0 forms a trunk.

After the above configuration, you need to wait a while (due to spanning tree). Then, you can go to PC2 and enter the command "ping 10.10.100.10" for pinging PC1. The result should be successful.

**Task 3**

Although the Port-channel interface Po10 can be found, the individual interfaces i.e. e0/2 and e0/3 are not configured with LACP.

You can use the following command to assign those two interfaces to channel-group 10 so that the pre-configured port-channel interface Po10 can be used.

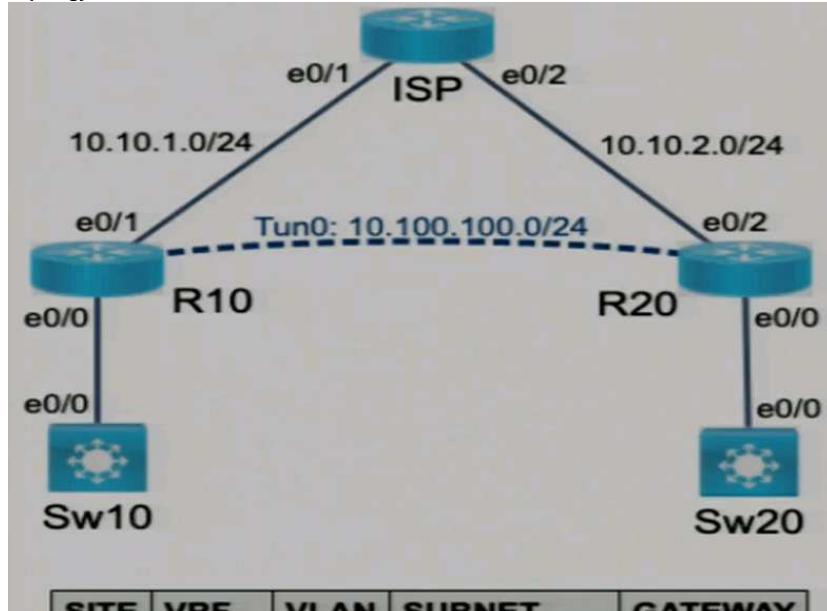
```
int range e0/2-3
  channel-group 10 mode active
```

After the above configuration, you need to wait a while (due to spanning tree). Then, you can go to PC2 and enter the command "ping 10.10.100.30" for pinging

PC3. The result should be successful.

**QUESTION 25**

**Topology:**



**Tasks:**

The operations team started configuring network devices for a new site. R10 and R20 are preconfigured with the CORP VRF. R10 has network connectivity to R20. Complete the configurations to achieve these goals:

1. Extend the CORP VRF between R10 and R20 using Tunnel0.
2. Protect Tunnel0 using the preconfigured profile.
3. Configure static routing on R10 and R20 so that users in VLANs 100 and 101 that belong to the CORP VRF are able to communicate with each other. Tunnel0 should be the only interface used to route traffic for the CORP VRF.

**Correct Answer:**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

**Ans:**

```
R10
en
config t
int tu0
  tunnel source 10.10.1.1
  tunnel protection ipsec profile MyProfile
!
ip route vrf CORP 10.101.2.0 255.255.255.0 tu0 10.100.100.2
end
copy run start
```

```
R20
en
config t
int tu0
  tunnel source 10.10.2.1
  tunnel protection ipsec profile MyProfile
!
ip route vrf CORP 10.100.1.0 255.255.255.0 tu0 10.100.100.1
end
copy run start
```

**For verification:**

You can use the following for verification.

```
R10
ping vrf CORP 10.101.2.1 source 10.100.1.1
```

```
R20
ping vrf CORP 10.100.1.1 source 10.101.2.1
```

**Explanations:**

You should use "sh run" in R10 and R20 to check if their configuration settings are as follows:

```
R10
vrf definition CORP
  address-family ipv4
  exit-address-family
!
```

```

crypto isakmp policy 10
  encr aes
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco address 10.10.2.1
!
crypto ipsec transform-set MYSET esp-aes esp-md5-hmac
  mode tunnel
!
crypto ipsec profile MyProfile
  set transform-set MYSET
!
int Tunnel0
  vrf forwarding CORP
  ip addr 10.100.100.1 255.255.255.0
  tunnel destination 10.10.2.1
!
int Ethernet0/0
  no ip addr

int Ethernet0/0.100
  encapsulation dot1Q 100
  vrf forwarding CORP
  ip addr 10.100.1.1 255.255.255.0
!
int Ethernet0/1
  ip addr 10.10.1.1 255.255.255.0
  ip ospf network point-to-point
  ip ospf 100 area 0.0.0.0

```

**R20**

```

vrf definition CORP
  address-family ipv4
  exit-address-family
!
crypto isakmp policy 10
  encr aes
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco address 10.10.1.1
!
crypto ipsec transform-set MYSET esp-aes esp-md5-hmac
  mode tunnel
!
crypto ipsec profile MyProfile
  set transform-set MYSET
!
int Tunnel0
  vrf forwarding CORP
  ip addr 10.100.100.2 255.255.255.0
  tunnel destination 10.10.1.1
!
int Ethernet0/0
  no ip addr
!
int Ethernet0/0.101
  encapsulation dot1Q 101
  vrf forwarding CORP
  ip addr 10.101.2.1 255.255.255.0
!
int Ethernet0/2
  ip addr 10.10.2.1 255.255.255.0
  ip ospf network point-to-point
  ip ospf 100 area 0.0.0.0

```

#### Task 1:

The interfaces tu0 in R10 and R20 are setup with VRF and other settings. However, tunnel source is missing. You just need to setup the tunnel source using the IP address of their interfaces connecting to the ISP router (i.e. the IP address of R1's e0/1 and R2's e0/2).

**R10**

```

int tu0
  tunnel source 10.10.1.1

```

**R20**

```

int tu0
  tunnel source 10.10.2.1

```

Remarks : You can also use the interface name e0/1 (in R1) or e0/2 (in R2) as the tunnel source.

#### Task 2:

You just need to apply the existing IPSec profile "MyProfile" to the tunnel 0 interfaces in the two routers.

**R10**

```

int tu0
  tunnel protection ipsec profile MyProfile

```

**R20**

```

int tu0
  tunnel protection ipsec profile MyProfile

```

#### Task 3:

In order to add a static route in a specific VRF, you need to use the command "ip route vrf CORP ...". Moreover, since tunnel 0 must be used, you can specify the interface in the static route.

For R10, you need to configure a static route to route traffic for VLAN 101 of network 10.101.2.0/24 through tunnel 0 to R20's tunnel's IP, therefore the static route

required is:

R10

```
ip route vrf CORP 10.101.2.0 255.255.255.0 tu0 10.100.100.2
```

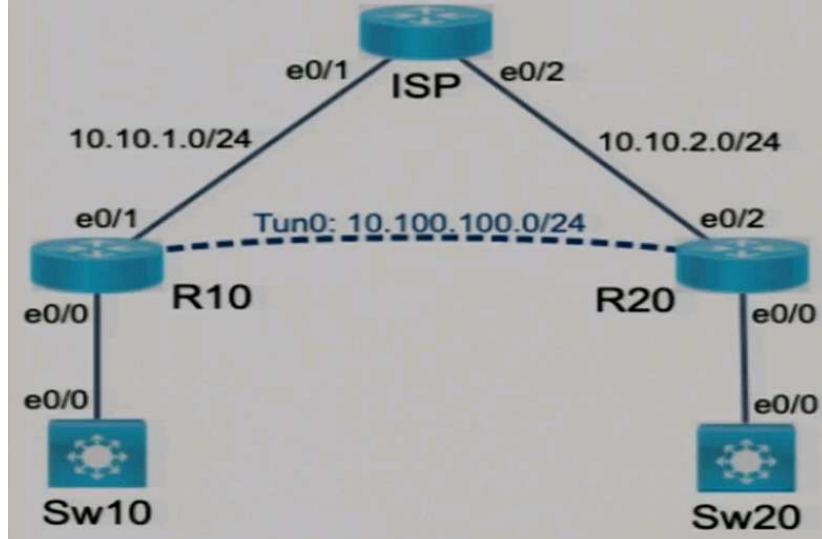
For R20, you need to configure a static route to route traffic for VLAN 100 of network 10.100.1.0/24 through tunnel 0 to R10's tunnel's IP, therefore the static route required is:

R20

```
ip route vrf CORP 10.100.1.0 255.255.255.0 tu0 10.100.100.1
```

**QUESTION 26**

Topology:



SITE	VRF	VLAN	SUBNET	GATEWAY
R10	CORP	100	10.100.1.0/24	10.100.1.1
R20	CORP	101	10.101.2.0/24	10.101.2.1

**Tasks:**

The operations team started configuring network devices for a new site. R10 and R20 are preconfigured with the CORP VRF. R10 has network connectivity to R20. Complete the configurations to achieve these goals:

1. Extend the CORP VRF between R10 and R20 using Tunnel0.
2. Protect Tunnel0 using the preconfigured profile.
3. Configure static routing on R10 and R20 so that users in VLANs 100 and 101 that belong to the CORP VRF are able to communicate with each other. Tunnel0 should be the only interface used to route traffic for the CORP VRF.

**Correct Answer:**

Section: Selected

Explanation

**Explanation/Reference:**

Ans:

```
R10
en
config t
int tu0
  vrf forwarding CORP
  ip addr 10.100.100.1 255.255.255.0
  tunnel protection ipsec profile MyProfile
!
int e0/0.100
  vrf forwarding CORP
  ip addr 10.100.1.1 255.255.255.0
end
copy run start
```

```
R20
en
config t
int tu0
  vrf forwarding CORP
  ip addr 10.100.100.2 255.255.255.0
  tunnel protection ipsec profile MyProfile
!
int e0/0.101
  vrf forwarding CORP
  ip addr 10.101.2.1 255.255.255.0
end
copy run start
```

**Explanations:**

This question has the same diagram and same tasks as another question. However, the pre-configured settings are different. Hence, the configuration settings required for this question are also different. Therefore, you must check the pre-configured settings before answering any simulation question!!

You should use "sh run" in R10 and R20 to check if their configuration settings are as follows:

**R10**

```
vrf definition CORP
  address-family ipv4
  exit-address-family
!
crypto isakmp policy 10
  encr aes
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco address 10.10.2.1
!
crypto ipsec transform-set MYSET esp-aes esp-md5-hmac
  mode tunnel
!
crypto ipsec profile MyProfile
  set transform-set MYSET
!
int Tunnel0
  ip addr 10.100.100.1 255.255.255.0
  tunnel source Ethernet0/1
  tunnel destination 10.10.2.1
!
int Ethernet0/0
  no ip addr
!
int Ethernet0/0.100
  encapsulation dot1Q 100
  ip addr 10.100.1.1 255.255.255.0
!
int Ethernet0/1
  ip addr 10.10.1.1 255.255.255.0
  ip ospf network point-to-point
  ip ospf 100 area 0.0.0.0
!
ip route vrf CORP 10.101.2.0 255.255.255.0 tu0 10.100.100.2
```

**R20**

```
vrf definition CORP
  address-family ipv4
  exit-address-family
!
crypto isakmp policy 10
  encr aes
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco address 10.10.1.1
!
crypto ipsec transform-set MYSET esp-aes esp-md5-hmac
  mode tunnel
!
crypto ipsec profile MyProfile
  set transform-set MYSET
!
int Tunnel0
  ip addr 10.100.100.2 255.255.255.0
  tunnel source Ethernet0/2
  tunnel destination 10.10.1.1
!
int Ethernet0/0
  no ip addr
!
int Ethernet0/0.101
  encapsulation dot1Q 101
  ip addr 10.101.2.1 255.255.255.0
!
int Ethernet0/2
  ip addr 10.10.2.1 255.255.255.0
  ip ospf network point-to-point
  ip ospf 100 area 0.0.0.0
!
ip route vrf CORP 10.100.1.0 255.255.255.0 tu0 10.100.100.1
```

In the existing configuration, the vrf CORP has been defined but has NOT been applied to any interface.

**Task 1:**

Since the interface tu0 in R10 and R20 has been setup. You just need to assign them to the vrf CORP. However, since the assigning of VRF will remove the IP address configured, you need to reconfigure the IP address.

**R10**

```
int tu0
  vrf forwarding CORP
  ip addr 10.100.100.1 255.255.255.0
```

**R20**

```
int tu0
  vrf forwarding CORP
  ip addr 10.100.100.2 255.255.255.0
```

**Remarks :** Before configuration, you need to check the pre-configured IP addresses of the tunnel interfaces to make sure that the IP addresses that should be re-configured in those interfaces.

**Task 2:**

You just need to apply the existing IPSec profile to the tunnel 0 interfaces in the two routers.

```
R10
int tu0
tunnel protection ipsec profile MyProfile
```

```
R20
int tu0
tunnel protection ipsec profile MyProfile
```

**Task 3:**

Because there is a correct command of "ip route vrf CORP ..." already existed in the configuration, you should only configure the following settings:

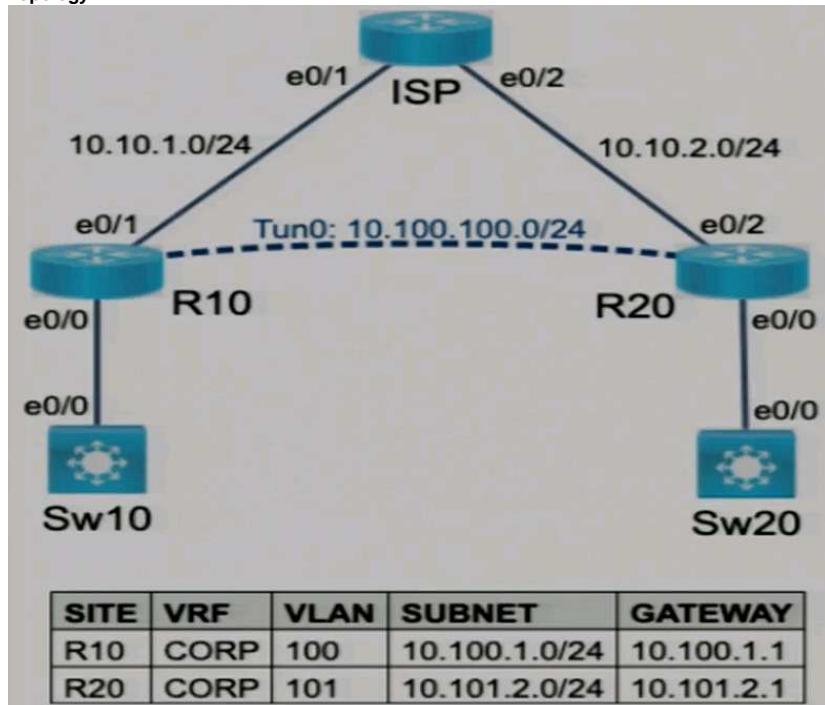
```
R10
int e0/0.100
vrf forwarding CORP
ip addr 10.100.1.1 255.255.255.0
```

```
R20
int e0/0.101
vrf forwarding CORP
ip addr 10.101.2.1 255.255.255.0
```

Remarks : Before configuration, you need to check the subinterface names and their pre-configured IP addresses of the tunnel interfaces to make sure the proper sub-interface names and IP addresses are re-configured.

**QUESTION 27**

**Topology:**

**Tasks:**

The operations team started configuring network devices for a new site. R10 and R20 are preconfigured with the CORP VRF. R10 has network connectivity to R20. Complete the configurations to achieve these goals:

1. Extend the CORP VRF between R10 and R20 using Tunnel0.
2. Protect Tunnel0 using the preconfigured profile.

**Correct Answer:**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

**Ans:**

```
R10
en
config t
int tu0
tunnel destination 10.10.2.1
tunnel protection ipsec profile MyProfile
!
ip route vrf CORP 10.101.2.0 255.255.255.0 tu0 10.100.100.2
end
copy run start
```

```
R20
en
config t
int tu0
```

```

tunnel destination 10.10.1.1
tunnel protection ipsec profile MyProfile
!
ip route vrf CORP 10.100.1.0 255.255.255.0 tu0 10.100.100.1
end
copy run start

```

For verification:  
 You can use the following for verification.

R10  
 ping vrf CORP 10.101.2.1 source 10.100.1.1

R20  
 ping vrf CORP 10.100.1.1 source 10.101.2.1

**Explanations:**

You must use "sh run" in R10 and R20 to check if their configuration settings are as follows since there is another question with the same diagram and tasks but with different pre-configured settings !!!!

```

R10
vrf definition CORP
  address-family ipv4
  exit-address-family
!
crypto isakmp policy 10
  encr aes
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco address 10.10.2.1
!
crypto ipsec transform-set MYSET esp-aes esp-md5-hmac
  mode tunnel
!
crypto ipsec profile MyProfile
  set transform-set MYSET
!
int Tunnel0
  vrf forwarding CORP
  ip addr 10.100.100.1 255.255.255.0
  tunnel source Ethernet0/1
!
int Ethernet0/0
  no ip addr

int Ethernet0/0.100
  encapsulation dot1Q 100
  vrf forwarding CORP
  ip addr 10.100.1.1 255.255.255.0
!
int Ethernet0/1
  ip addr 10.10.1.1 255.255.255.0
  ip ospf network point-to-point
  ip ospf 100 area 0.0.0.0

```

```

R20
vrf definition CORP
  address-family ipv4
  exit-address-family
!
crypto isakmp policy 10
  encr aes
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco address 10.10.1.1
!
crypto ipsec transform-set MYSET esp-aes esp-md5-hmac
  mode tunnel
!
crypto ipsec profile MyProfile
  set transform-set MYSET
!
int Tunnel0
  vrf forwarding CORP
  ip addr 10.100.100.2 255.255.255.0
  tunnel source Ethernet0/2
!
int Ethernet0/0
  no ip addr
!
int Ethernet0/0.101
  encapsulation dot1Q 101
  vrf forwarding CORP
  ip addr 10.101.2.1 255.255.255.0
!
int Ethernet0/2
  ip addr 10.10.2.1 255.255.255.0
  ip ospf network point-to-point
  ip ospf 100 area 0.0.0.0

```

Task 1:

The interfaces tu0 in R10 and R20 are setup with VRF and other settings. However, tunnel destination is missing. You need to setup the tunnel destination using the IP address of the other routers' interfaces connecting to the ISP router.

- For R10, you need to configure the IP address of R20's e0/2 i.e. 10.10.2.1 as tunnel destination.
- For R20, you need to configure the IP address of R10's e0/1 i.e. 10.10.1.1 as tunnel destination.

```
R10
int tu0
  tunnel destination 10.10.2.1

R20
int tu0
  tunnel destination 10.10.1.1
```

#### Task 2:

You just need to apply the existing IPSec profile "MyProfile" to the tunnel 0 interfaces in the two routers.

```
R10
int tu0
  tunnel protection ipsec profile MyProfile

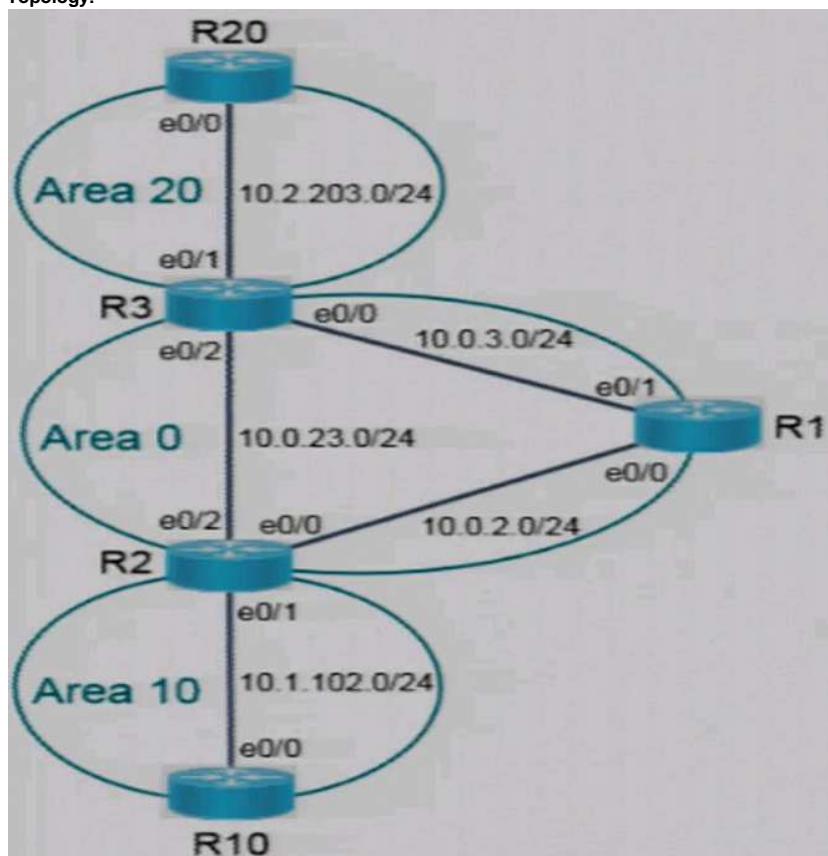
R20
int tu0
  tunnel protection ipsec profile MyProfile
```

Remarks : You should double check the profile name. For example in "sh run", you should check the name in the command "crypto ipsec profile <profile name>". You can view the pre-configured settings shown above to familiarize the location where you can find this command.

Remarks:: Although the task of "Configure static routing on R10 and R20 so that users in VLANs100 and 101 that belong to the CORP VRF are able to communicate with each other." is not stated in this question, we still configure for it by typing the correct command "ip route vrf CORP ..." in order to make the verification functional. In addition, it is more safe in case it is required implicitly by the examination.

#### QUESTION 28

**Topology:**



#### Tasks:

OSPF is partially configured on all devices. Complete the configurations to achieve these goals:

1. Configure R2 to always be the DR in Area 10. Do not change the router ID.
2. Configure a single command on R2 to summarize area 10 routes into a single route.

**Correct Answer:**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Ans:**

```
R2
en
config t
int e0/1
  ip ospf priority 255
!
router ospf 10
  area 10 range 10.1.0.0 255.255.0.0
```

```
end  
copy run start
```

```
R10  
en  
clear ip ospf process
```

Verification:

For Task 1:

Verification can be performed in R2 by the command "sh ip ospf int e0/1" (or "sh ip ospf nei" in R10)

- Before configuring the above answer, the following can be found in the output of "sh ip ospf int e0/1" in R2:

Transmit Delay is 1 sec, State BDR, Priority 1

- After configuring the above answer and clear the OSPF process in R10, the following can be found in the output of "sh ip ospf int e0/1" in R2:

Transmit Delay is 1 sec, State DR, Priority 255

For Task 2:

Verification can be performed in R1 using the command "sh ip route ospf"

- Before configuring the above answer, the "IA" routes having 10.0.2.2 (i.e. R2) as next hop in the output by "sh ip route ospf" from R1 are:

```
10.1.1.1/32  
10.1.100.10/32  
10.1.102.0/24  
10.1.200.10/32
```

- Before configuring the above answer, the "IA" routes having 10.0.2.2 (i.e. R2) as next hop in the output by "sh ip route ospf" from R1 are:

```
10.1.0.0/16
```

#### Explanations:

##### Task 1

In order to make R2 to be DR in area 10, you need to configure the R2's interface connecting to area 10 i.e. e0/1 to have the highest OSPF priority i.e. 255

```
int e0/1  
  ip ospf priority 255
```

In order to verify the result, you need to bring down the OSPF of the existing DR i.e. R10 first. You can achieve this by running the privileged mode command "clear ip ospf process" (answer "yes") in R10.

##### Task 2

In order to perform summarization, you need to check the existing OSPF routes from area 10 learnt by other area 0 router e.g. R1 first.

In R1, the "IA" OSPF routes having R2 (i.e. 10.0.2.2) as next hop in the output by "sh ip route ospf" are:

```
10.1.1.1/32  
10.1.100.10/32  
10.1.102.0/24  
10.1.200.10/32
```

These are inter-area routes learnt by R1 from R2. Since, other than area 0, the only other area connected by R2 is area 10 only. The above are all OSPF Inter-Area routes from area 10.

Since all routes are having the pattern "10.1.X.X", you can configure a summary route using "10.1.0.0/16".

Before configuration, use "sh run | s router ospf" to find out the process number of the pre-configured OSPF in R2 first e.g.

#### Output from "sh run | s router ospf" in R2:

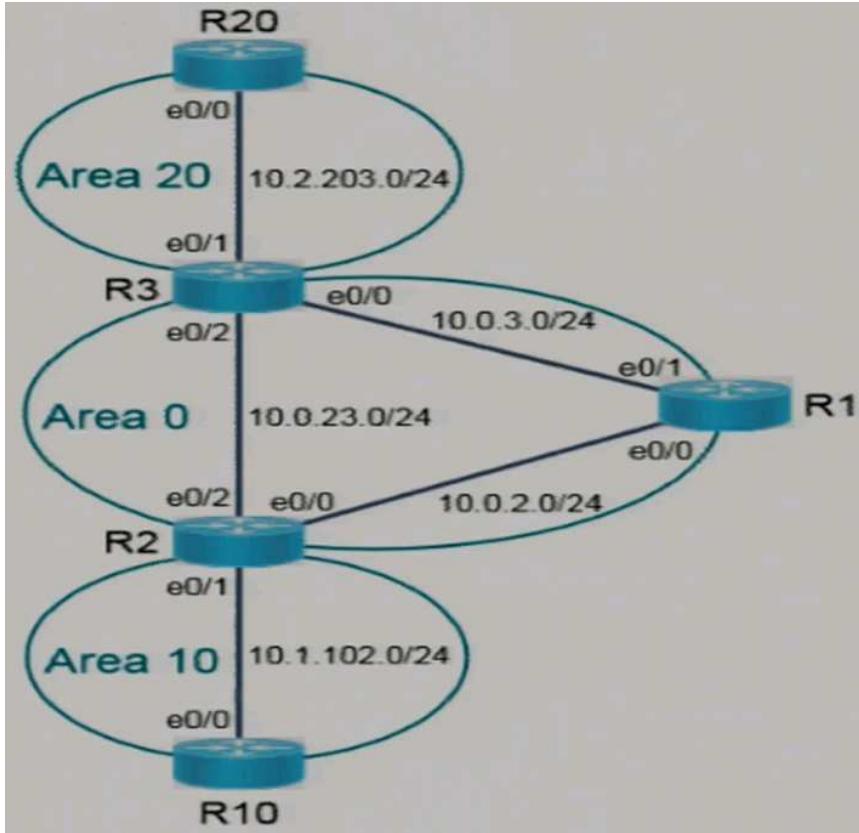
```
router ospf 10 <----  
  router-id 10.0.1.2  
  network 10.0.1.0 0.0.0.255 area 0  
  network 10.0.2.0 0.0.0.255 area 0  
  network 10.0.23.0 0.0.0.255 area 0  
  network 10.1.102.0 0.0.0.255 area 10
```

Then you can use the process number to enter the existing OSPF configuration to configure the summarized route as follows:

```
R2  
router ospf 10  
  area 10 range 10.1.0.0 255.255.0.0
```

#### QUESTION 29

Topology:



**Tasks:**

OSPF is partially configured. Complete the OSPF configurations to achieve these goals:

1. Configure R3 and R20 so they do not participate in a DR/BDR election process in Area 20.
2. Configure R10 so it is always the DR for Area 10. Do not change the router ID.

**Correct Answer:**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**Ans:**

```
R3
en
config t
int e0/1
  ip ospf network point-to-point
end
copy run start
```

```
R20
en
config t
int e0/0
  ip ospf network point-to-point
end
copy run start
```

```
R10
en
config t
int e0/0
  ip ospf priority 255
end
copy run start
```

```
R2
en
clear ip ospf process
```

**Verification:**

**For Task 1:**

- After configuring the above answer, the following entry can be found in the output of "sh ip ospf nei" in R20 proving that neighbor is formed without DR/BDR.

10.0.1.3 0 FULL/ -

**For Task 2:**

Verification can be performed in R10 by the command "sh ip ospf int e0/0" (or "sh ip ospf nei" in R2)

- Before configuring the above answer, the following can be found in the output of "sh ip ospf int e0/0" in R10:

Transmit Delay is 1 sec, State BDR, Priority 1

- After configuring the above answer and clear the OSPF process in R2, the following can be found in the output of "sh ip ospf int e0/0" in R10:

Transmit Delay is 1 sec, State DR, Priority 255

**Explanations:**

### Task 1

Normally, in order to prevent a router from participating in DR/BDR election, you can configure OSPF priority 0 in the concerned interface. However, since R3 and R20 are the only two routers in the broadcast network, you cannot disable DR/BDR election in both routers or otherwise there will be no DR in the broadcast network.

The only way to achieve this task is to change the network type of both routers so that DR is not required. The most common way is to change the network type to "point-to-point" since only two routers are involved in the network.

Since R3's e0/1 and R20's e0/0 are connecting to that concerned network:

R3

```
int e0/1
  ip ospf network point-to-point
```

R20

```
int e0/0
  ip ospf network point-to-point
```

### Task 2

Since the only OSPF neighbor of R10 is R2, in order to make R10 to be the DR, you need to set R10's interface connecting to R2 i.e. e0/0 to have the highest OSPF priority i.e. 255.

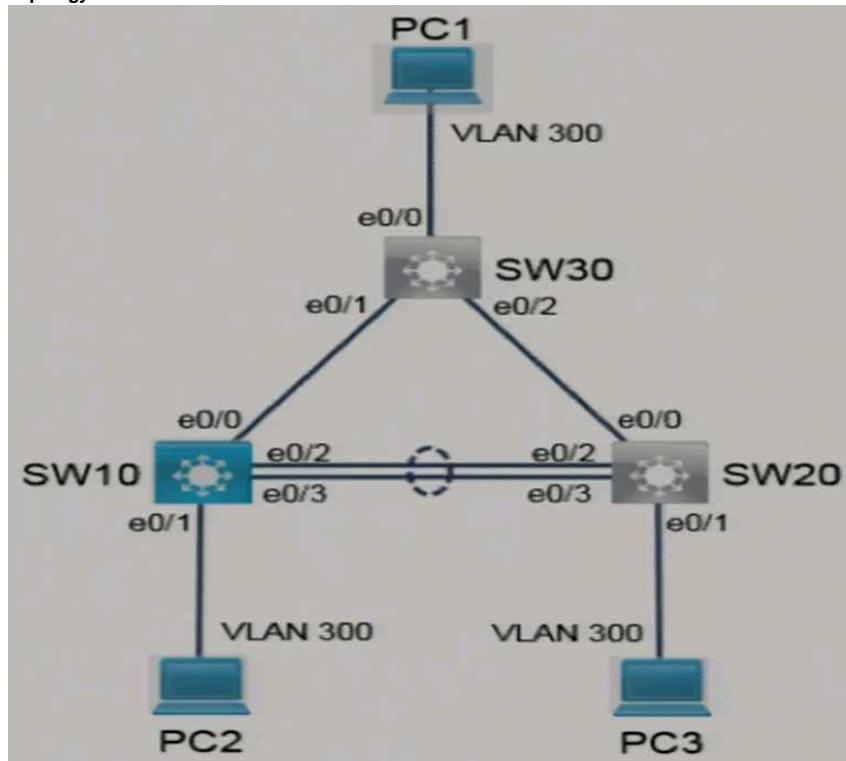
```
int e0/0
  ip ospf priority 255
```

In order to verify the setting immediately, you need to run the privileged mode command "clear ip ospf process" (answer "yes") in R2.

Remarks : Since the task does NOT ask you to prevent R2 from participating in DR/BDR election, therefore do NOT configure priority 0 in R2.

### QUESTION 30

**Topology:**



#### **Tasks:**

The operations team started configuring network devices for a new site. Complete the configurations to achieve these goals:

1. The trunk between SW10 and SW30 is not operational. Troubleshoot the issue and ensure PC2 can ping PC1 (10.10.100.10) across the link.
2. Configure SW10 interface E0/0 for aggressive unidirectional link detection.
3. The LACP port-channel between SW10 and SW20 is not operational. Troubleshoot the issue and ensure that PC2 can ping PC3 (10.10.100.30) across the port-channel.

Note: No access is provided to SW20 or SW30. Resolve these issues by making changes only to SW10. Traffic on all trunks should be restricted to only active VLANs.

#### **Correct Answer:**

**Section: (none)**

**Explanation**

#### **Explanation/Reference:**

**Ans:**

```
SW20
en
config t
spanning-tree mode rapid-pvst
int e0/0
  switchport trunk encapsulation dot1q
```

```

switchport mode trunk
udld port aggressive
int range e0/2-3
switchport trunk allowed vlan 1,300
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 10 mode active
end
copy run start

```

**verification:**

You can enter the following ping commands in PC2 and their results should be successful.

```
-ping 10.10.100.10
-ping 10.10.100.30
```

**Explanations:**

Using the command "sh run" in SW10, you should find the following settings pre-configured:

```

interface Port-channel10
switchport trunk allowed vlan 1,300
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/0
switchport mode access
!
interface Ethernet0/1
switchport access vlan 300
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Vlan1
ip address 10.10.1.10 255.255.255.0

```

**Task 1**

SW10's is connecting to SW30 through its interface e0/0. However, the interface is configured as an access port. In order to form a trunk, you can configure the trunk encapsulation and then configure it as a trunk port manually.

```

int e0/0
switchport trunk encapsulation dot1q
switchport mode trunk

```

After the above configuration, wait a while (due to spanning tree), PC2 should now be able to use the command "ping 10.10.100.10" to ping PC1.

**Task 2**

In order to configure SW10's interface e0/0 for aggressive unidirectional link detection, you can use the Interface configuration mode command "udld port aggressive".

```

int e0/0
udld port aggressive

```

**Task 3**

Although the Port-channel interface Po10 is configured, no individual interface has been assigned to this channel group. Since SW10 is connecting to SW20 through the interfaces e0/2 and e0/3, you should assign them to the channel group 10.

After checking the configuration settings in Po10, you should configure the same settings in those two interfaces and then assign them to channel group 10.

For example:

Output of "sh run int po10" in SW10:

```

interface Port-channel10
switchport trunk allowed vlan 1,300
switchport trunk encapsulation dot1q
switchport mode trunk

```

The configuration commands required are then:

```

int range e0/2-3
switchport trunk allowed vlan 1,300
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 10 mode active

```

You can use "sh etherchannel" in SW10 to check if the Port Channel group is up (i.e. with status "SU").

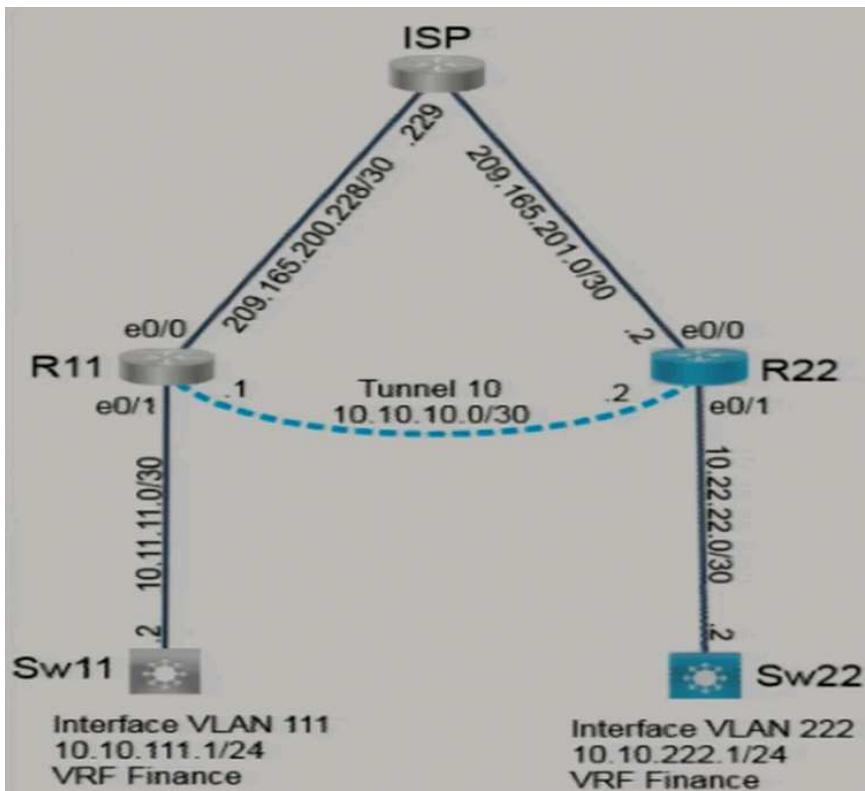
Remarks : If it is not in Up status, you need to check if the configuration settings in the Port Channel interface matches those of the individual interfaces. If one or more settings are missing, you need to re-configure the missed settings in the individual interfaces. After re-configuring, you may need to shut and no shut the Port Channel interface to verify if it becomes Up.

After the above configuration, wait a while (due to spanning tree), PC2 should now be able to use the command "ping 10.10.100.30" to ping PC3.

Remarks : PC2 may still ping PC3 even if the port channel is down since the two individual interfaces may run as standalone data port. Therefore, you should remember to check the status of the Port Channel to find out if it is properly configured and up.

**QUESTION 31**

**Topology:**



#### Tasks:

A colleague started configuring a new network. All configurations on R11 are complete and communication between R11 and R22 is functional. Complete the configurations on R22 for the tasks below.

#### Task 1

Extend the Finance VRF between R11 and R22 using Tunnel 10.

#### Task 2

Complete the Finance VRF configuration on R22 and configure static routing so that traffic between VLAN 111 and VLAN 222 uses Tunnel 10 exclusively.

Note: Sw22 can be used to validate traffic flow.

#### Correct Answer:

Section: Selected

Explanation

#### Explanation/Reference:

Ans:

```

R22
en
config t
int tu10
vrf forwarding Finance
ip address 10.10.10.2 255.255.255.252
tunnel source e0/0
tunnel destination 209.165.200.230
!
int e0/1
vrf forwarding Finance
ip address 10.22.22.1 255.255.255.252
!
ip route vrf Finance 10.10.111.0 255.255.255.0 tu10 10.10.10.1
end
copy run start

```

#### Verification:

You can enter the following ping command in Sw22 (not in R22) and the results should be successful.

ping 10.10.111.1

#### Explanations:

Using the command "sh run" in R22, you should find the following settings pre-configured:

```

R22
vrf definition Finance
address-family ipv4
exit-address-family
!
interface Loopback0
ip address 10.2.2.2 255.255.255.255
!
interface Ethernet0/0
ip address 209.165.201.2 255.255.255.252
!
interface Ethernet0/1
ip address 10.22.22.1 255.255.255.252
!
router bgp 65502

```

```
bgp router-id 10.2.2.2
network 209.165.201.0 mask 255.255.255.252
neighbor 209.165.201.1 remote-as 65500
```

#### Task 1

From the pre-configured settings in R22, the tunnel 10 interface has not been created yet. You need to create the tunnel interface with the following settings:  
- Use 10 as the tunnel interface number (as mentioned by the task and diagram)  
- Assign the tunnel interface to vrf Finance (as mentioned by the task).  
- Assign 10.10.10.2/30 as the tunnel IP address (as mentioned by the diagram)  
- Use R22's e0/0 as the tunnel source.  
- Use the IP address of R1's e0/0 (i.e. 209.165.200.230) as the tunnel destination. (R22 can reach this IP address through the route learnt from BGP)

```
R22
int tu10
vrf forwarding Finance
ip address 10.10.10.2 255.255.255.252
tunnel source e0/0
tunnel destination 209.165.200.230
```

After the configuration, you can verify the tunnel setup by the following command:  
ping vrf Finance 10.10.10.1

#### Task 2

R22's e0/1 is connecting to Sw22 and the vrf Finance network 10.10.222.0/24. However, the interface e0/1 has NOT been assigned to the vrf Finance yet. Hence, the following configuration settings are required.

```
R22
int e0/1
vrf forwarding Finance
ip address 10.22.22.1 255.255.255.252
```

Finally, in order for R22 to route traffic to the vrf Finance network 10.10.111.0/24 (connected by Sw11) through tunnel 10, the following static route is required.

```
R22
ip route vrf Finance 10.10.111.0 255.255.255.0 tu10 10.10.10.1
```

#### Remarks:

If your question asks you to configure R11 instead of R22, the answer will be:

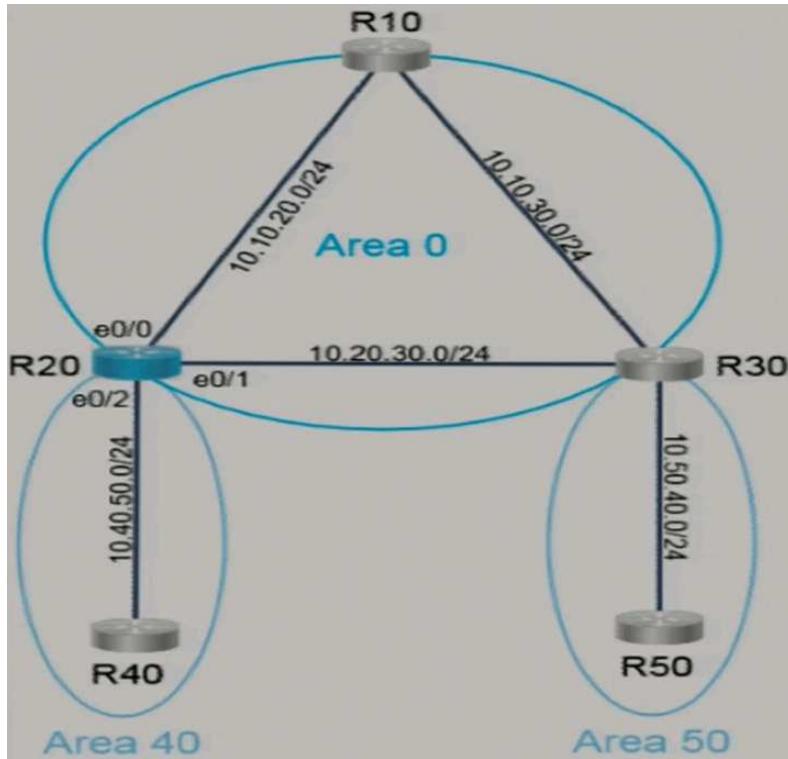
```
R11
en
config t
int tu10
vrf forwarding Finance
ip address 10.10.10.1 255.255.255.252
tunnel source e0/0
tunnel destination 209.165.201.2
!
int e0/1
vrf forwarding Finance
ip address 10.11.11.1 255.255.255.252
!
ip route vrf Finance 10.10.222.0 255.255.255.0 tu10 10.10.10.2
end
copy run start
```

#### \*\*\*\* Important \*\*\*\*

The IP addresses / networks and/or interface names in your question may be different from those shown above. You should make the required changes in your answer accordingly.

#### QUESTION 32

**Topology:**



#### Tasks:

OSPF is preconfigured on all devices except R20. Configure R20 to complete these tasks.

#### Task 1:

Configure OSPF according to the topology using these requirements:

- Use Process ID 10.
- Use Loopback1 for the Router ID.
- Advertise all networks into OSPF.
- Use network statements under the OSPF process to accomplish this task.

#### Task 2:

Configure a /20 summary route for Area 40.

- Advertise only Type 3 LSAs into the Area 0.

#### Correct Answer:

**Section: Selected**

**Explanation**

#### Explanation/Reference:

**Ans:**

```
R20
en
config t
router ospf 10
  router-id 10.20.20.20
  network 10.0.1.20 0.0.0.0 area 0
  network 10.20.20.20 0.0.0.0 area 0
  network 10.10.20.0 0.0.0.255 area 0
  network 10.10.30.0 0.0.0.255 area 0
  network 10.40.50.0 0.0.0.255 area 40
  area 40 range 10.40.0.0 255.255.240.0
end
copy run start
```

#### Explanations:

Using the command "sh run" in R20, you should find the following settings pre-configured:

```
R20
interface Loopback0
  ip address 10.0.1.20 255.255.255.255
!
interface Loopback1
  ip address 10.20.20.20 255.255.255.255
!
interface Ethernet0/0
  ip address 10.10.20.20 255.255.255.0
!
interface Ethernet0/1
  ip address 10.10.30.20 255.255.255.0
!
interface Ethernet0/2
  ip address 10.40.50.20 255.255.255.0
```

#### Task 1

No OSPF has been pre-configured in R20 yet. You need to create the OSPF process according to the requirement specified in task 1 as follows:

- Use process number 10
- Check the IP address of interface lo1 and configure it as the router ID.
- Advertise all networks into OSPF using "network" command. Hence, you can NOT use interface configuration command to advertise the networks. Moreover, the

term "all networks" may also require you to advertise the networks of the loopback interfaces.

#### R20

```
router ospf 10
  router-id 10.20.20.20
  network 10.0.1.20 0.0.0.0 area 0
  network 10.20.20.20 0.0.0.0 area 0
  network 10.10.20.0 0.0.0.255 area 0
  network 10.10.30.0 0.0.0.255 area 0
  network 10.40.50.0 0.0.0.255 area 40
```

Remarks : The networks of the loopback interfaces are assigned to area 0. This usually simplifies summarization required for other areas.

#### Task 2

In R20, there is a network 10.40.50.0/24 belonging to area 40. In order to find more, you need to use "sh ip route ospf" to find any route with R40 as next hop. You should find the following OSPF route:  
10.40.1.40/32 [110/11] via 10.40.50.40

Therefore, for a summarized route with /20, you can configure:

#### R20

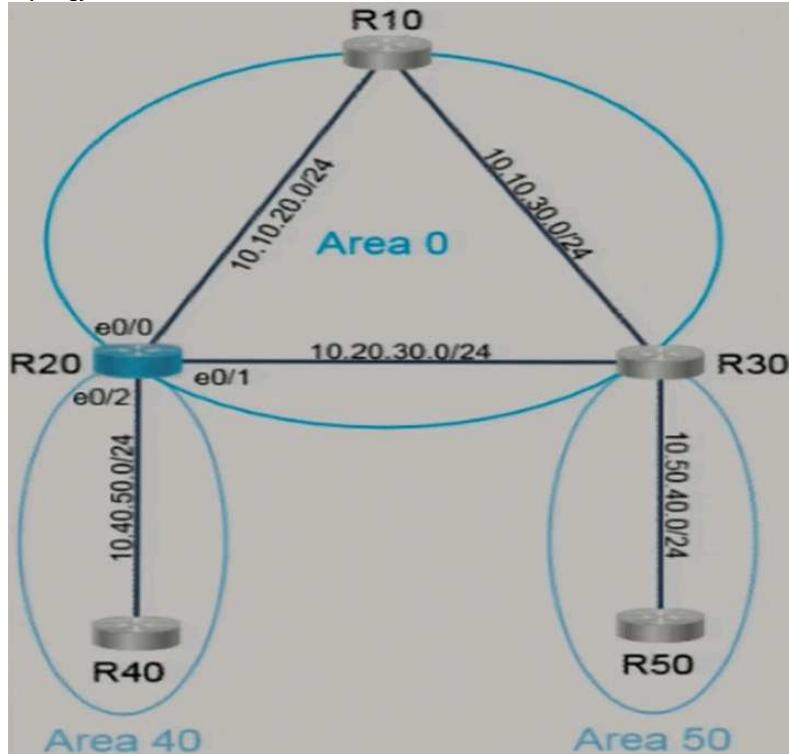
```
router ospf 10
  area 40 range 10.40.0.0 255.255.240.0
```

Remarks : 10.40.0.0 255.255.240.0 is 10.40.0.0/20 which includes 10.40.0.0 up to 10.40.15.255. Although it includes the route from R40, it does not include the network of R20's e0/2. Since the task ask you to configure a single summarize route, we shall not include the network of R20's e0/2 in the summarized route (since there is no way to include both in a /20 summarized route)

Remarks : The word "only Type 3 LSAs" is included in the task to prevent you from using other ways to advertise the summarize route (e.g. redistribution).

#### QUESTION 33

Topology:



#### Tasks:

OSPF is preconfigured on all devices except R20. Configure R20 to complete these tasks.

##### Task 1:

Configure OSPF according to the topology using these requirements:

- Use Process ID 200.
- Use Loopback0 for the Router ID.
- Advertise all networks into OSPF.
- Use network statements under the OSPF process to accomplish this task.

##### Task 2:

Configure a /17 summary route for Area 40.

- Advertise only Type 3 LSAs into the Area 0.

#### Correct Answer:

Section: Selected

Explanation

#### Explanation/Reference:

Ans:

#### R20

```
en
config t
router ospf 200
  router-id 10.0.1.20
```

```

network 10.0.1.20 0.0.0.0 area 0
network 10.20.20.20 0.0.0.0 area 0
network 10.10.20.0 0.0.0.255 area 0
network 10.10.30.0 0.0.0.255 area 0
network 10.40.50.0 0.0.0.255 area 40
area 40 range 10.40.0.0 255.255.128.0
end
copy run start

```

#### **Explanations:**

Using the command "sh run" in R20, you should find the following settings pre-configured:

```

R20
interface Loopback0
 ip address 10.0.1.20 255.255.255.255
!
interface Loopback1
 ip address 10.20.20.20 255.255.255.255
!
interface Ethernet0/0
 ip address 10.10.20.20 255.255.255.0
!
interface Ethernet0/1
 ip address 10.10.30.20 255.255.255.0
!
interface Ethernet0/2
 ip address 10.40.50.20 255.255.255.0

```

#### Task 1

No OSPF has been pre-configured in R20 yet. You need to create the OSPF process according to the requirement specified in task 1 as follows:

- Use process number 200 (this may be different in your question)
- Check the IP address of interface lo0 (this may be different in your question) and configure it as the router ID.
- Advertise all networks into OSPF using "network" command. Hence you can NOT use interface configuration command to advertise the networks. Moreover, the term "all networks" may also require you to advertise the networks of the loopback interfaces.

#### R20

```

router ospf 200
 router-id 10.0.1.20
 network 10.0.1.20 0.0.0.0 area 0
 network 10.20.20.20 0.0.0.0 area 0
 network 10.10.20.0 0.0.0.255 area 0
 network 10.10.30.0 0.0.0.255 area 0
 network 10.40.50.0 0.0.0.255 area 40

```

Remarks : The networks of the loopback interfaces are assigned to area 0. This usually simplifies summarization required for other areas.

#### Task 2

In R20, there is a network 10.40.50.0/24 belonging to area 40. In order to find more, you need to use "sh ip route ospf" to find any route with R40 as next hop.

You should find the following OSPF route:

```
10.40.1.40/32 [110/11] via 10.40.50.40
```

Therefore, for a summarized route with /17 (this may be different in your question), you can configure:

#### R20

```

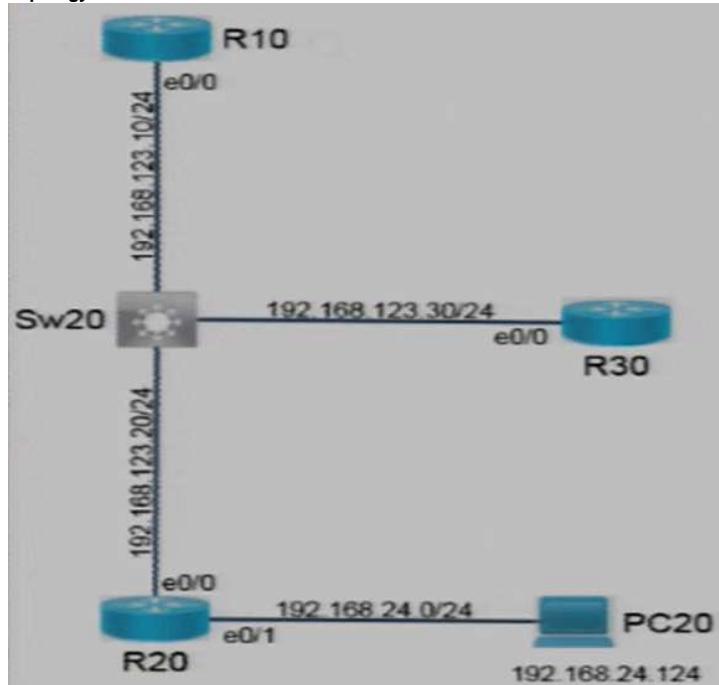
router ospf 200
 area 40 range 10.40.0.0 255.255.128.0

```

Remarks : 10.40.0.0 255.255.128.0 is 10.40.0.0/17 which includes 10.40.0.0 up to 10.40.127.255. Hence, this summarized route can properly include all area 40's networks i.e. both the network from R40 as well as the network from R20's e0/2.

#### **QUESTION 34**

**Topology:**



**Tasks:**

OSPF is preconfigured on all routers. Configure R10 and R30 to complete these tasks.

Task 1: Modify the existing ACL on R10 so that OSPF routes are received from R20 and R30.

- The modification should only allow OSPF routes to pass.
- Do not remove any configuration from R10 to achieve this task.

Task 2: Configure CoPP on R30 to achieve these results:

- Permit Telnet traffic from 192.168.24.0/24.
- Limit traffic to 8,000 bps.
- Discard additional packets.

**Correct Answer:**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

**Ans:**

```
R10
en
config t
ip access-list extended 120
  5 permit ospf any any
end
copy run start
```

```
R30
en
config t
access-list 100 permit tcp 192.168.24.0 0.0.0.255 any eq 23
class-map telnet24
  match access-group 100
policy-map copp
  class telnet24
    police cir 8000 conform-action transmit exceed-action drop
control-plane
  service-policy input copp
end
copy run start
```

**Explanations:**

Task 1

Using the command "sh run" in R10, you should find the following settings pre-configured:

```
R10
interface Loopback0
  ip address 192.168.1.10 255.255.255.255
!
interface Ethernet0/0
  ip address 192.168.123.10 255.255.255.0
  ip access-group 120 in
!
router ospf 10
  router-id 192.168.1.10
  network 192.168.1.10 0.0.0.0 area 0
  network 192.168.123.0 0.0.0.255 area 0
!
access-list 120 permit tcp any any
access-list 120 permit udp any any
access-list 120 permit icmp any any
access-list 120 deny ip any any
```

Due to the access list configured in R10's e0/0, all OSPF packets are blocked and neighbor cannot be formed with R20 and R30.

In order to allow OSPF packets, the packets of the OSPF protocol have to be allowed. However, the task does not allow you to remove any configuration in R10. Hence, you need to insert a rule for allowing OSPF protocol in the existing access list 120.

You can use the following command to check the sequence of the existing rules first:

```
R10#sh access-list 120
Extended IP access list 120
  10 permit tcp any any
  20 permit udp any any
  30 permit icmp any any
  40 deny ip any any
R10#
```

Then you need to insert the rule allowing OSPF protocol with a sequence number before the "deny" rule e.g. 5.

```
R10
ip access-list extended 120
  5 permit ospf any any
```

After the above configuration, logging messages about forming OSPF neighbors with R20 and R30 will be shown. Moreover, you can check the access list 120 to confirm that the rule has been inserted in the appropriate location:

```
R10#sh access-list 120
Extended IP access list 120
```

```

5 permit ospf any any
10 permit tcp any any
20 permit udp any any
30 permit icmp any any
40 deny ip any any
R10#

```

### Task 2

Using the command "sh run" in R30, you should find the following settings pre-configured:

```

R30
interface Loopback0
    ip address 192.168.1.30 255.255.255.255
!
interface Ethernet0/0
    ip address 192.168.123.30 255.255.255.0
!
router ospf 10
    router-id 192.168.1.30
    network 192.168.1.30 0.0.0.0 area 0
    network 192.168.123.0 0.0.0.255 area 0

```

No access list, class map or policy map has been pre-configured in R30.

In order to configure CoPP to allow telnet from 192.168.24.0/24 and limit the traffic to 8000 bps with additional packets discarded, you can configure the following access list, class map and policy map. Then you can apply the policy map in CoPP.

```

R30
access-list 100 permit tcp 192.168.24.0 0.0.0.255 any eq 23
!
class-map telnet24
    match access-group 100
!
policy-map copp
    class telnet24
        police cir 8000 conform-action transmit exceed-action drop
!
control-plane
    service-policy input copp

```

Remarks : You can use any access list number (provided that it is within 100-199), class map name, policy map name that you like in the configuration.

After the above configuration, you can use the following command to check your settings.

```

R30#sh access-list 100
Extended IP access list 100
    10 permit tcp 192.168.24.0 0.0.0.255 any eq telnet
R30#

```

```

R30#sh policy-map control-plane
Control Plane

Service-policy input: copp

Class-map: telnet24 (match-all)
    0 packets, 0 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: access-group 100
    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

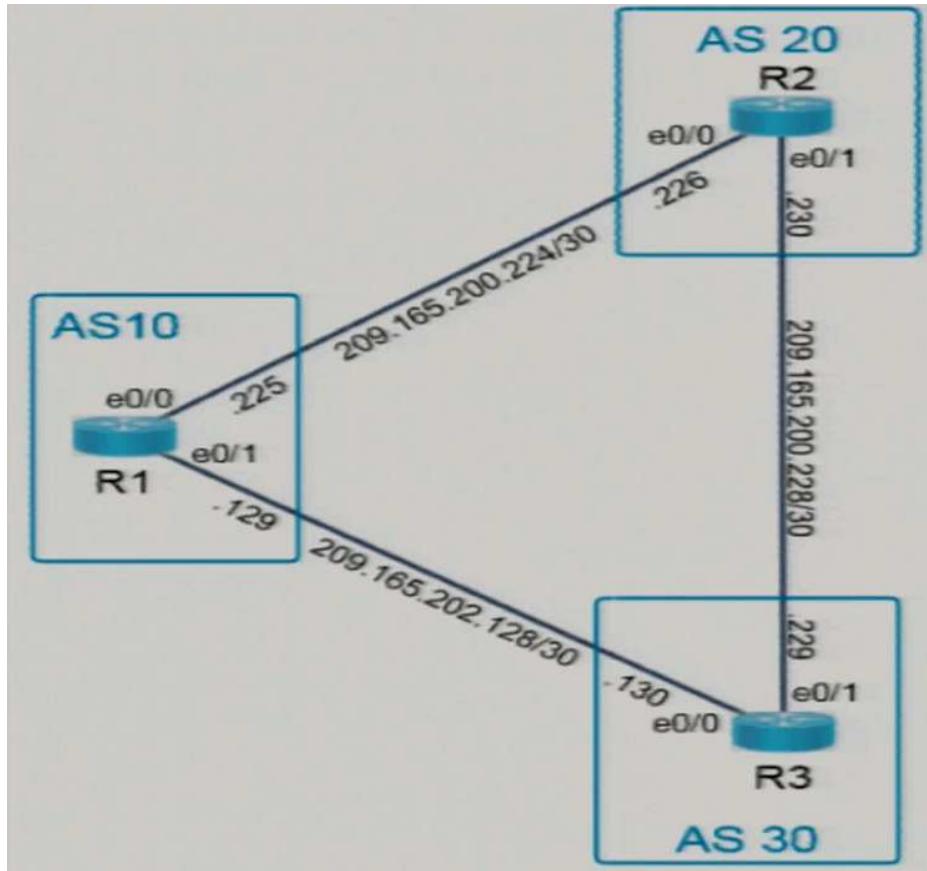
Class-map: class-default (match-any)
    22 packets, 2832 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: any
R30#

```

Remarks : The above configuration is based on the wordings specified by the task. However, there may be some other implied requirements that we have not taken care of e.g.:
i. whether telnet traffic from networks other than 192.168.24.0/24 should be discarded.
ii. whether non-telnet traffic (except OSPF, ARP ... etc) from any network should be discarded.
Normally, the question will not require you to configure a lot of settings. Hence, the above settings are not included in the suggested answer.

### **QUESTION 35**

**Topology:**



**Tasks:**

eBGP is configured on R2 and R3. Configure R1 to complete these tasks.

1. Using the address-family command, configure eBGP according to the topology. Use Loopback 0 for the router-id.
2. Advertise R1's Loopback 0, 10, and 20 networks to AS 20 and AS 30.

**Correct Answer:**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

**Ans:**

```
R1
en
config t
router bgp 10
bgp router-id 10.1.1.10
neighbor 209.165.200.226 remote-as 20
neighbor 209.165.202.130 remote-as 30
address-family ipv4
  network 209.165.200.224 mask 255.255.255.252
  network 209.165.202.128 mask 255.255.255.252
  network 10.1.1.10 mask 255.255.255.255
  network 209.165.201.10 mask 255.255.255.255
  network 209.165.201.20 mask 255.255.255.255
end
copy run start

verification:
You can enter the command "sh ip route bgp" in R2 and R3 and the following routes should be found:
10.1.1.10/32
209.165.201.10/32
209.165.201.20/32
```

**Explanations:**

**Task 1**

Using the command "sh run" in R1, you should find the following settings pre-configured:

```
R1
interface Loopback0
  ip address 10.1.1.10 255.255.255.255
!
interface Loopback10
  ip address 209.165.201.10 255.255.255.255
!
interface Loopback20
  ip address 209.165.201.20 255.255.255.255
!
interface Etherne0/0
  ip address 209.165.200.225 255.255.255.252
!
```

```
interface Etherne0/1
 ip address 209.165.202.129 255.255.255.252
```

The following shows the BGP configuration settings in R1 using "address-family" as required by the task.

```
R1
router bgp 10
bgp router-id 10.1.1.10
neighbor 209.165.200.226 remote-as 20
neighbor 209.165.202.130 remote-as 30
address-family ipv4
 network 209.165.200.224 mask 255.255.255.252
 network 209.165.202.128 mask 255.255.255.252
```

#### Task 2

Find the pre-configured IP addresses / networks of the interface lo0, lo10 and lo20 of R1. Then advertise them in BGP through the "network" command under "address-family".

```
R1
router bgp 10
address-family ipv4
 network 10.1.1.10 mask 255.255.255.255
 network 209.165.201.10 mask 255.255.255.255
 network 209.165.201.20 mask 255.255.255.255
```

After configuring both task 1 and task 2, the BGP configuration in R1 will be as follows:

```
R1#sh run | s router bgp
router bgp 10
bgp router-id 10.1.1.10
neighbor 209.165.202.130 remote-as 30
neighbor 209.165.200.226 remote-as 20
!
address-family ipv4
 network 10.1.1.10 mask 255.255.255.255
 network 209.165.200.224 mask 255.255.255.252
 network 209.165.201.10 mask 255.255.255.255
 network 209.165.201.20 mask 255.255.255.255
 network 209.165.202.128 mask 255.255.255.252
 neighbor 209.165.202.130 activate
 neighbor 209.165.200.226 activate
exit-address-family
R1#
```

#### Remarks :

- The AS numbers may be different e.g. AS100, AS200 and AS300
- The loopback interface numbers may be different e.g. lo0, lo1 and lo2

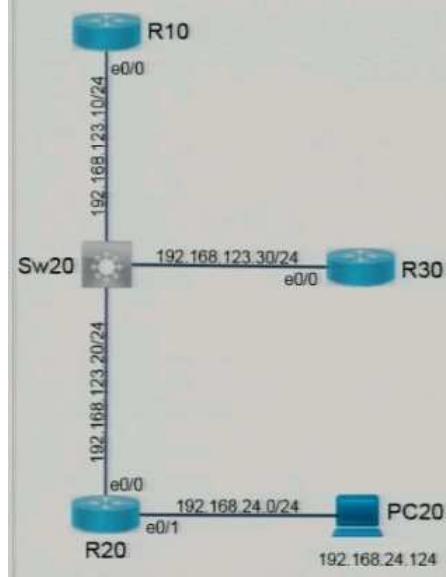
- The IP address and network mask of the loopback interfaces may be different.

For example, if you are required to advertise lo1 and lo2 which are pre-configured with "ip addr 209.165.201.1 255.255.255.248" and "ip addr 209.165.201.9 255.255.255.248" respectively. Then the following commands are needed instead:

```
network 209.165.201.0 mask 255.255.255.248
network 209.165.201.8 mask 255.255.255.248
```

#### QUESTION 36

**Topology:**



#### Tasks:

EIGRP is preconfigured on all routers. Configure R20 and R30 to complete these tasks.

##### Task 1:

Modify the existing ACL on R30 so that EIGRP routes are received from R10 and R20.

- The modification should only allow EIGRP routes to pass.
- Do not remove any configuration from R30 to achieve this task.

**Task 2:**

Configure CoPP on R20 to achieve these results:

- Permit Telnet traffic from 192.168.24.124.
- Limit traffic to 10,000 bps.
- Discard additional packets.

**Correct Answer:**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

**Ans:**

```
R20
en
config t
access-list 100 permit tcp host 192.168.24.124 any eq 23
class-map match-all pc20-telnet
  match access-group 100
policy-map copp-policy
  class pc20-telnet
    police 10000 conform-action transmit exceed-action drop
control-plane
  service-policy input copp-policy
end
copy run start
```

```
R30
en
config t
ip access-list extended 120
  5 permit eigrp any any
end
copy run start
```

**Explanations:**

Using the command "sh run" in each router, you should find the following pre-configured settings:

```
R10
interface Loopback0
  ip address 192.168.1.10 255.255.255.255
!
interface Ethernet0/0
  ip address 192.168.123.10 255.255.255.0
!
router eigrp 10
  network 192.168.1.10 0.0.0.0
  network 192.168.123.0
```

```
R20
interface Loopback0
  ip address 192.168.1.20 255.255.255.255
!
interface Ethernet0/0
  ip address 192.168.123.20 255.255.255.0
!
interface Ethernet0/1
  ip address 192.168.24.20 255.255.255.0
!
router eigrp 10
  network 192.168.1.20 0.0.0.0
  network 192.168.24.0
  network 192.168.123.0
```

```
R30
interface Loopback0
  ip address 192.168.1.30 255.255.255.255
!
interface Ethernet0/0
  ip address 192.168.123.30 255.255.255.0
  ip access-group 120 in
!
router eigrp 10
  network 192.168.1.30 0.0.0.0
  network 192.168.123.0
!
access-list 120 permit tcp any any
access-list 120 permit udp any any
access-list 120 permit icmp any any
access-list 120 deny ip any any
```

**Task 1**

Since you are not allowed to remove any configuration, you need to add a rule to the ACL 120 in R30 to allow EIGRP.

The ACL 120 in R30 should be as follows:

```
R30#sh access-list
Extended IP access list 120
  10 permit tcp any any
  20 permit udp any any
  30 permit icmp any any
  40 deny ip any any
R30#
```

Therefore, you can add the rule using e.g. sequence 5 as follows:

```
R30
ip access-list extended 120
```

```
5 permit eigrp any any
```

After a while, R30 should form neighbor with R10 and R20. Moreover, EIGRP routes can be learnt.

#### Task 2

In order to limit telnet traffic from PC20 i.e. 192.168.24.124 to 10,000bps, you can configure policing for the traffic in CoPP as follows.

```
R20
access-list 100 permit tcp host 192.168.24.124 any eq 23
!
class-map match-all pc20-telnet
match access-group 100
!
policy-map copp-policy
class pc20-telnet
police 10000 conform-action transmit exceed-action drop
!
control-plane
service-policy input copp-policy
```

#### Remarks:

Your question may be similar as the above but with one or more of the following changes:

- The network topology is the same but the diagram may be horizontally flipped (e.g. PC20 is on the left of the diagram and Sw20 is on the right of the diagram).
- The router names may be different.
- The IP addresses / networks and interface names may be different.
- Limit rate may be different.
- Instead of limiting Telnet traffic from a single IP, the question may ask you to limit SSH or ICMP traffic from a /24 network (this requires a change in the rule in the access list).

For SSH:

```
access-list 100 permit tcp host 192.168.24.124 any eq 22
```

For ICMP:

```
access-list 100 permit icmp host 192.168.24.124 any
```

- The pre-configured ACL may be as follows:

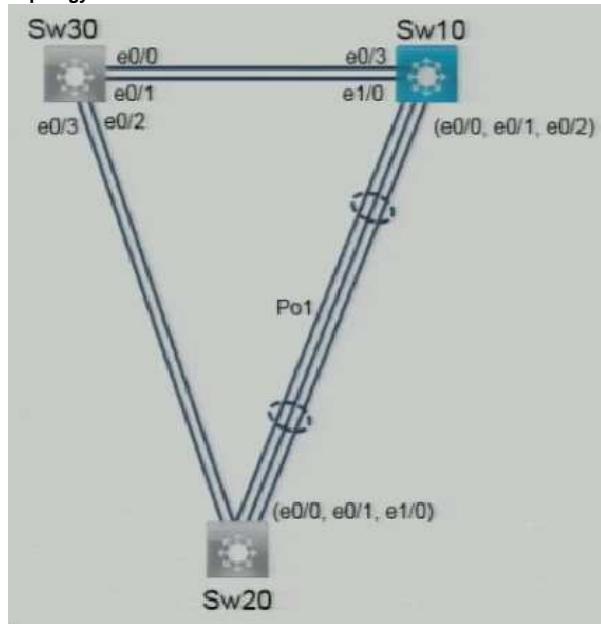
```
access-list 150 deny ip any any
access-list 150 permit tcp any any
access-list 150 permit udp any any
access-list 150 permit icmp any any
access-list 150 permit eigrp any any
```

Since you are not allowed to remove any configuration from the router, you need to insert the required rule at the top of the ACL so that the existing rule can be kept:

```
config t
ip access-list extended 150
  5 permit eigrp any any
end
```

#### QUESTION 37

Topology:



#### Tasks:

Complete the tasks below by making changes to SW10 only. No access is provided to Sw20 or Sw30.

##### Task 1:

Sw20 is actively attempting to negotiate an 802.1 trunking EtherChannel with Sw10 using LACP, but the channel is not functional. Resolve the issues on Sw10.

##### Task 2:

Modify the spanning tree configuration to ensure that Sw10 is always the root for VLAN 10 and VLAN 30.

**Correct Answer:**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

**Ans:**

```
Sw10
en
config t
spanning-tree vlan 10,30 root primary
int range e0/0-2
    switchport mode dynamic desirable
    channel-group 1 mode active
int pol
    switchport mode dynamic desirable
    shut
    no shut
end
copy run start
```

**Explanations:**

Using the command "sh run" in Sw10, you should find the following pre-configured settings:

```
Sw10
interface Port-channel1
    switchport access vlan 10
    switchport mode access
!
interface Ethernet0/0
    switchport access vlan 10
    switchport mode access
!
interface Ethernet0/1
    switchport access vlan 10
    switchport mode access
!
interface Ethernet0/2
    switchport access vlan 10
    switchport mode access
!
interface Ethernet0/3
    switchport access vlan 30
    switchport mode access
!
interface Ethernet1/0
    switchport access vlan 30
    switchport mode access
!
interface vlan 10
    ip address 10.100.10.10 255.255.255.0
!
interface vlan 30
    ip address 10.100.20.10 255.255.255.0
```

**Task 1**

The pre-configured settings for the interfaces e0/0, e0/1 and e0/2 in Sw10 do not setup any 802.1q trunking or EtherChannel.

Since the question does not mention whether negotiation is needed for LACP only or negotiation is needed for both 802.1q and LACP, we assume that both should be negotiated.

Note that when setting up Port Channel 1 (this interface is mentioned in the diagram), since it is pre-configured without trunking, after adding the interfaces to this Port Channel, you also need to setup trunking in this Port Channel.

```
Sw10
int range e0/0-2
    switchport mode dynamic desirable
    channel-group 1 mode active
int pol
    switchport mode dynamic desirable
    shut
    no shut
```

The shut and no shut for the Port Channel allows the configuration changes to be effective immediately for checking.

After the above, the EtherChannel should be up as follows:

```
Sw10#sh etherchannel 1 summary
Flags: D - down P - bundled in port-channel
      I - stand-alone S - suspended
      H - Hot-Standby (LACP only)
      R - Layer3     S - Layer2
      U - in use     N - not in use, no aggregation
      f - failed to allocate aggregator

      M - not in use, minimum links not met
      m - not in use, port not aggregated due to minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

      A - formed by Auto LAG
```

Number of channel-groups in use: 1  
Number of aggregators: 1

Group	Port-channel	Protocol	Ports		
1	Po1(SU)	LACP	E0/0(P)	E0/1(P)	E0/2(P)

Sw10#

**Remarks :**

Since the task does not mention which VLAN should be the native VLAN, the default VLAN 1 will be used.

## Task 2

In order to set Sw10 as the root bridge for VLAN 10 and 30, you can configure the followings:

Sw10  
spanning-tree vlan 10,30 root primary

### Remarks:

No space is allowed between "10," and "30"

```
Sw10(config)#spanning-tree vlan 10, 30 root primary  
% Invalid input detected at '^' marker.  
Sw10(config)#spanning-tree vlan 10,30 root primary  
Sw10(config)#
```

You can use "sh spanning-tree vlan 10" and "sh spanning-tree vlan 30" to confirm that Sw10 becomes the root bridge for both VLANs. "This bridge is the root" should be found in the "Root ID" section.

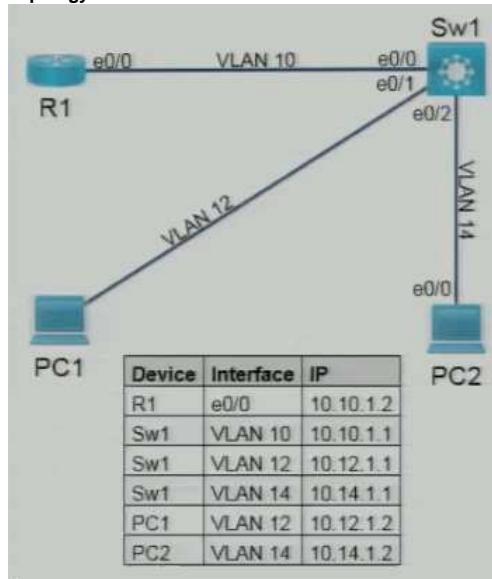
### Remarks:

Your question may be similar as the above but with one or more of the following changes:

- The interface names may be different. For example, if Po1 becomes Po10, then you need to use commands such as "int Po10" and "channel-group 10 mode active" instead.
- The VLANs that Sw10 should be the root bridge may be different e.g. VLAN 10 and VLAN 20

## QUESTION 38

### Topology:



### Tasks:

The Operations team started configuring several monitoring activities. Complete the configurations for the tasks below.

1. Complete the Flexible NetFlow Flow Exporter configuration on R1 to send data to the collector located at 10.10.1.110.
2. Configure a basic IP SLA HTTP GET operation on R1 to monitor the server at 10.10.1.100 every 300 seconds.
3. Configure the switch port analyzer on Sw1 using these settings:
  - Session number 7
  - Mirror all traffic on E0/0
  - Direct the output to interface E1/1

### Correct Answer:

Section: Selected

Explanation

### Explanation/Reference:

Ans:

```
R1  
en  
config t  
flow exporter Export-NetFlowENCOR  
destination 10.10.1.110  
ip sla 1  
http get http://10.10.1.100  
frequency 300  
ip sla schedule 1 life forever start-time now  
end  
copy run start
```

```
Sw1  
en  
config t  
monitor session 7 source int e0/0 both  
monitor session 7 destination int e1/1  
end  
copy run start
```

**Explanations:**

Using the command "sh run" in R1 and Sw1, you should find the following pre-configured settings:

```
R1
flow exporter Export-NetFlowENCOR
source Loopback0
transport udp 2055
!
flow monitor Monitor-NetFlowENCOR
exporter Export-NetFlowENCOR
cache timeout inactive 60
cache timeout active 600
record netflow ipv4 original-input
!
interface Loopback0
ip address 1.1.1.1 255.255.255.255
!
interface Ethernet0/0
ip address 10.10.1.2 255.255.255.0
ip flow monitor Monitor-NetFlowENCOR input
ip flow monitor Monitor-NetFlowENCOR output
ip ospf network point-to-point
!
router ospf 10
router-id 1.1.1.1
network 1.1.1.1 0.0.0.0 area 0
network 10.10.1.0 0.0.255 area 0
```

```
Sw1
interface Loopback0
ip address 10.2.2.2 255.255.255.255
!
interface Ethernet0/0
switchport access vlan 10
ip flow ingress
ip flow egress
!
interface Ethernet0/1
switchport access vlan 12
ip flow ingress
ip flow egress
!
interface Ethernet0/2
switchport access vlan 14
ip flow ingress
ip flow egress
!
interface Vlan10
ip address 10.10.1.1 255.255.255.0
ip ospf network point-to-point
!
interface Vlan12
ip address 10.12.1.1 255.255.255.0
!
interface Vlan14
ip address 10.12.1.1 255.255.255.0
!
router ospf 10
router-id 10.2.2.2
network 10.2.2.2 0.0.0.0 area 0
network 10.10.1.0 0.0.255 area 0
network 10.12.1.0 0.0.255 area 0
network 10.14.1.0 0.0.255 area 0
```

**Task 1**

In pre-configured settings in R1, the exporter is missing the destination. Therefore, you just need to add the "destination" command under the existing exporter configuration "Export-NetFlowENCOR" as follows:

```
R1
flow exporter Export-NetFlowENCOR
destination 10.10.1.110
```

**Remarks:**

You can use "sh flow exporter" to check your settings.

**Task 2**

The IP SLA can be configured as follows. Note that you should also schedule it to start.

```
R1
ip sla 1
http get http://10.10.1.100
frequency 300
!
ip sla schedule 1 life forever start-time now
```

**Remarks:**

You can use "sh ip sla configuration" to check your settings and use "sh ip sla summary" to display the summary statistics.

**Task 3**

In Sw1, the SPAN settings for session 7 are as follows:

```
Sw1
monitor session 7 source int e0/0 both
monitor session 7 destination int e1/1
```

**Remarks:**

You can use "sh monitor session 7" to check your settings.

**Remarks:**

Your question may be similar as the above but with one or more of the following changes:

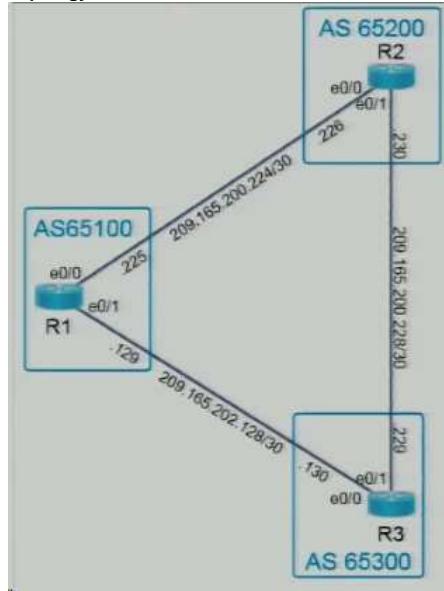
- The name of the exporter "Export-NetFlowENCOR" may be different and the collector's IP address (for configuration the "destination" command) may be different.
- The session number for configuring SPAN may be different, the traffic that needs to be monitored may be different and the output interface may be different. For example: if the SPAN session number is 2, all communications to and from both PC1 and PC2 have to be monitored and the mirrored traffic should be sent to e1/0, then the answer will be:

```
monitor session 2 source int e0/1,e0/2 both
monitor session 2 destination int e1/0
```

- The IP address of the web server and the frequency interval for setting up IP SLA may be different.

**QUESTION 39**

**Topology:**

**Tasks:**

eBGP is configured on R1 and R3. Configure R2 to complete these tasks.

1. Using the address-family command, configure eBGP according to the topology. Use Loopback 0 for the router-id.
2. Advertise R2's Loopback 0, 1, and 2 networks to AS 65100 and AS 65300.

**Correct Answer:**

Section: Selected

Explanation

**Explanation/Reference:**

Ans:

```
R1
en
config t
router bgp 65200
  bgp router-id 192.168.2.2
  neighbor 209.165.200.225 remote-as 65100
  neighbor 209.165.200.229 remote-as 65300
  address-family ipv4
    network 192.168.2.2 mask 255.255.255.255
    network 209.165.201.1 mask 255.255.255.255
    network 209.165.201.2 mask 255.255.255.255
  end
copy run start
```

**Explanations:**

Using the command "sh run" in R1 and Sw1, you should find the following settings pre-configured:

```
R1
interface Loopback0
  ip address 192.168.1.1 255.255.255.255
!
interface Ethernet0/0
  ip address 209.165.200.225 255.255.255.252
!
interface Ethernet0/1
  ip address 209.165.202.129 255.255.255.252
!
router bgp 65100
  bgp router-id 192.168.1.1
  neighbor 209.165.200.226 remote-as 65200
  neighbor 209.165.202.130 remote-as 65300
```

**R2**

```
interface Loopback0
  ip address 192.168.2.2 255.255.255.255
!
interface Loopback1
  ip address 209.165.201.1 255.255.255.255
```

```

!
interface Loopback2
 ip address 209.165.201.2 255.255.255.255
!
interface Ethernet0/0
 ip address 209.165.200.226 255.255.255.252
!
interface Ethernet0/1
 ip address 209.165.200.230 255.255.255.252

```

**R3**

```

interface Loopback0
 ip address 192.168.3.3 255.255.255.255
!
interface Ethernet0/0
 ip address 209.165.202.130 255.255.255.252
!
interface Ethernet0/1
 ip address 209.165.200.229 255.255.255.252
!
router bgp 65300
 bgp router-id 192.168.3.3
 neighbor 209.165.200.230 remote-as 65200
 neighbor 209.165.202.129 remote-as 65100

```

Since R2 does not have any BGP configuration, you need to configure the BGP settings so that R2 can form neighbors with R1 and R3. Moreover, R2 needs to advertise all 3 loopback interfaces through BGP.

Note that the task requires you to use "address-family" in the BGP configuration.

**R2**

```

router bgp 65200
 bgp router-id 192.168.2.2
 neighbor 209.165.200.225 remote-as 65100
 neighbor 209.165.200.229 remote-as 65300
 address-family ipv4
 network 192.168.2.2 mask 255.255.255.255
 network 209.165.201.1 mask 255.255.255.255
 network 209.165.201.2 mask 255.255.255.255

```

After a while:

- You can check if R2 can form neighbor with R1 and R3 using the command "sh ip bgp summary" in R2.

```

R2#sh ip bgp summary
BGP router identifier 192.168.2.2, local AS number 65200
BGP table version is 1, main routing table version 1
1 network entries using 144 bytes of memory
1 path entries using 84 bytes of memory
1/0 BGP path/bestpath attribute entries using 160 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 388 total bytes of memory
BGP activity 1/0 prefixes, 1/0 paths, scan interval 60 secs

Neighbor      V      AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
209.165.200.225 4    65100     2       2        1      0      0 00:00:49      0
209.165.200.229 4    65300     2       2        1      0      0 00:00:40      0
R2#

```

- You can check whether R1 (and R3) receives the BGP routes for the 3 loopback interfaces using the command "sh ip bgp" or "sh ip route bgp" in R1 (and R3):

```

R1#sh ip bgp
BGP table version is 4, local router ID is 192.168.1.1
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,
               t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

      Network          Next Hop            Metric LocPrf Weight Path
*   192.168.2.2/32  209.165.202.130        0      65300  65200  i
* > 209.165.200.226          0      65200  i
*   209.165.201.1/32 209.165.202.130        0      65300  65200  i
* > 209.165.200.226          0      65200  i
*   209.165.201.2/32 209.165.202.130        0      65300  65200  i
* > 209.165.200.226          0      65200  i
R1#

```

```

R1#sh ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

```

```

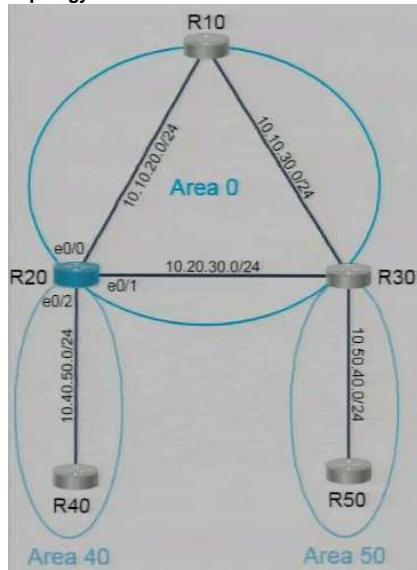
      192.168.2.0/32 is subnetted, 1 subnets
B         192.168.2.2 [20/0] via 209.165.200.226, 00:08:43
      209.165.201.0/32 is subnetted, 2 subnets
B         209.165.201.1 [20/0] via 209.165.200.226, 00:07:20
B         209.165.201.2 [20/0] via 209.165.200.226, 00:06:50

```

R1#

#### QUESTION 40

Topology:



**Tasks:**

OSPF is preconfigured on all devices except R20. Configure R20 to complete these tasks.

**Task 1:**

Configure OSPF according to the topology using these requirements:

- Use Process ID 20.
- Use Loopback0 for the Router ID.
- Advertise all networks into OSPF.
- Do not use network statements under the OSPF process to accomplish this task.

**Task 2:**

Configure a /18 summary route for Area 40.

**Correct Answer:**

**Section: Selected**

**Explanation**

**Explanation/Reference:**

```
R20
en
config t
router ospf 20
  router-id 10.0.1.20
  area 40 range 10.40.0.0 255.255.192.0
int lo0
  ip ospf 20 area 0
int lo1
  ip ospf 20 area 0
int e0/0
  ip ospf 20 area 0
int e0/1
  ip ospf 20 area 0
int e0/2
  ip ospf 20 area 40
end
copy run start
```

**Explanations:**

You should use "sh run" to its configuration settings to see if they are as follows:

```
R20
interface Loopback0
  ip address 10.0.1.20 255.255.255.255
!
interface Loopback1
  ip address 10.20.20.20 255.255.255.255
!
interface Ethernet0/0
  ip address 10.10.20.20 255.255.255.0
!
interface Ethernet0/1
  ip address 10.20.30.20 255.255.255.0
!
interface Ethernet0/2
  ip address 10.40.50.20 255.255.255.0
```

**Task 1:**

Since "network" commands are not allowed, you should use interface configuration mode command "ip ospf ..." instead. Moreover, since the task requires you to advertise all networks, the "ip ospf ..." command should also be configured in all loopback interfaces.

```
R20
router ospf 20
  router-id 10.0.1.20
```

```

!
int lo0
 ip ospf 20 area 0
!
int lo1
 ip ospf 20 area 0
!
int e0/0
 ip ospf 20 area 0
!
int e0/1
 ip ospf 20 area 0
!
int e0/2
 ip ospf 20 area 40

```

After the above is configured, OSPF neighboring with other routers should be formed. You can also find OSPF routes 10.10.30.0/24 and 10.50.40.0/24 in R20's routing table.

#### Remarks :

You may be required to use a process number other than "20" or the diagram may show an area other than area "40" connected by an interface other than "e0/2".

#### Task 2:

You need to configure R20 to send a summary route with mask /18 i.e. 255.255.192.0 for area 40.

Since the network within area 40 is 10.40.50.0/24, you need to configure the summary route "10.40.0.0 255.255.192.0"

#### R20

```

router ospf 20
 area 40 range 10.40.0.0 255.255.192.0

```

#### Remarks:

Since the 3rd octet of the mask is 192, the 3rd octet of the networks are increments of  $256-192 = 64$  i.e. 10.40.0.0/18, 10.40.64.0/18, 10.40.128.0/18 ... etc.  
Since the network 10.40.50.0/24 is included within 10.40.0.0/18, therefore 10.40.0.0/18 should be configured as the summary route.

However, if "Configure a /19 summary route for Area 40." is asked instead for another question, the following commands should be typed instead:

#### R20

```

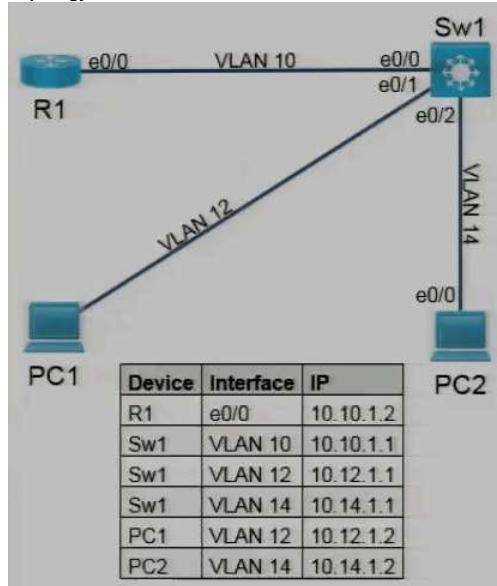
router ospf 20
 area 40 range 10.40.32.0 255.255.224.0

```

Since this time the 3rd octet of the mask is 224, the 3rd octet of the networks are increments of  $256-224 = 32$  i.e. 10.40.0.0/19, 10.40.32.0/19, 10.40.64.0/19 ... etc.  
Since the network 10.40.50.0/24 is included within 10.40.32.0/19, therefore 10.40.32.0/19 should be configured as the summary route.

#### QUESTION 41

##### Topology:



##### Tasks:

The Operations team started configuring several monitoring activities. Complete the configurations for the tasks below.

1. Complete the Flexible NetFlow Flow Exporter configuration on R1 to send data to the collector using UDP port 2055.
2. Configure the switch port analyzer on Sw1 and mirror all communication to and from PC1 to interface E1/1 using session number 11.
3. Schedule the pre-configured IP SLA operation on R1 to start running immediately and to run indefinitely.

##### Correct Answer:

Section: Selected

Explanation

##### Explanation/Reference:

Ans:

```

R1
en
config t
flow exporter Export-NetFlowENCOR
 transport udp 2055

```

```

ip sla schedule 100 life forever start-time now
end
copy run start

```

```

Sw1
en
config t
monitor session 11 source int e0/1 both
monitor session 11 destination int e1/1
end
copy run start

```

**Explanations:**

Using the command "sh run" in R1 and Sw1, you should find the following pre-configured settings:

```

R1
flow exporter Export-NetFlowENCOR
  destination 10.10.1.10
  source Loopback0
!
flow monitor Monitor-NetFlowENCOR
  exporter Export-NetFlowENCOR
  cache timeout inactive 60
  cache timeout active 600
  record netflow ipv4 original-input
!
interface Loopback0
  ip address 1.1.1.1 255.255.255.255
!
interface Ethernet0/0
  ip address 10.10.1.2 255.255.255.0
  ip ospf network point-to-point
!
router ospf 10
  router-id 1.1.1.1
  network 1.1.1.1 0.0.0.0 area 0
  network 10.10.1.0 0.0.255 area 0
!
ip sla 100
  icmp-echo 10.12.1.2
  frequency 300

```

```

Sw1
interface Loopback0
  ip address 10.2.2.2 255.255.255.255
!
interface Ethernet0/0
  switchport access vlan 10
  ip flow ingress
  ip flow egress
!
interface Ethernet0/1
  switchport access vlan 12
  ip flow ingress
  ip flow egress
!
interface Ethernet0/2
  switchport access vlan 14
  ip flow ingress
  ip flow egress
!
interface Vlan10
  ip address 10.10.1.1 255.255.255.0
  ip ospf network point-to-point
!
interface Vlan12
  ip address 10.12.1.1 255.255.255.0
!
interface Vlan14
  ip address 10.12.1.1 255.255.255.0
!
router ospf 10
  router-id 10.2.2.2
  network 10.2.2.2 0.0.0.0 area 0
  network 10.10.1.0 0.0.255 area 0
  network 10.12.1.0 0.0.255 area 0
  network 10.14.1.0 0.0.255 area 0

```

**Task 1**

In pre-configured settings in R1, the exporter is missing the port number required by the task. Therefore, you just need to add the "transport" command under the existing exporter configuration "Export-NetFlowENCOR" as follows:

```

R1
flow exporter Export-NetFlowENCOR
  transport udp 2055

```

**Remarks:**

You can use "sh flow exporter" to check your settings.

**Remarks:**

In pre-configured settings in R1, no interface has been assigned with the flow monitor with the following Interface Configuration mode commands:

```

ip flow monitor Monitor-NetFlowENCOR input
ip flow monitor Monitor-NetFlowENCOR output

```

However, since the task does not ask you to apply the flow monitor and it does not mention about which interface should be applied. The above two commands are not included in the suggested answer.

#### Task 2

Since PC1 is connected to the port e0/1 of Sw1, the SPAN settings for session 11 in Sw1 required by the task are:

#### Sw1

```
monitor session 11 source int e0/1 both  
monitor session 11 destination int e1/0
```

#### Remarks:

You can use "sh monitor session 11" to check your settings.

#### Task 3

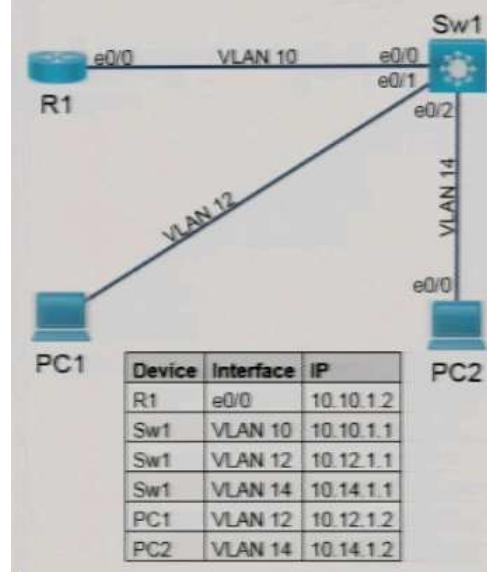
In R1, an IP SLA 100 is already pre-configured but it is not started. You should configure the following start and run it indefinitely.

#### R1

```
ip sla schedule 100 life forever start-time now
```

#### **QUESTION 42**

##### **Topology:**



##### **Tasks:**

The Operations team started configuring several monitoring activities. Complete the configurations for the tasks below.

1. Enable Flexible NetFlow on R1 E0/0 in both directions using the pre-configured flow monitor.
2. Configure a basic IP SLA ICMP echo operation on R1 to ping Sw1's Loopback interface every 60 seconds.
3. Configure the switch port analyzer on Sw1 using these settings:
  - Session number 5
  - Mirror all traffic on E0/2
  - Direct output to interface E1/0

##### **Correct Answer:**

**Section: Selected**

**Explanation**

##### **Explanation/Reference:**

##### **Ans:**

```
R1  
en  
config t  
int e0/0  
  ip flow monitor Monitor-FlowR1 input  
  ip flow monitor Monitor-FlowR1 output  
ip sla 1  
  icmp-echo 5.5.5.5  
  frequency 60  
ip sla schedule 1 life forever start-time now  
end  
copy run start
```

#### Sw1

```
en  
config t  
monitor session 5 source int e0/2 both  
monitor session 5 destination int e1/0  
end  
copy run start
```

**Explanations:**

Using the command "sh run" in R1 and Sw1, you should find the following pre-configured settings:

**R1**

```
flow exporter Export-FlowR1
destination 10.10.1.10
source Loopback0
transport udp 2055

flow monitor Monitor-FlowR1
exporter Export-FlowR1
cache timeout inactive 30
cache timeout active 300
record netflow ipv4 original-input

interface Loopback0
ip address 1.1.1.1 255.255.255.255

interface Ethernet0/0
ip address 10.10.1.2 255.255.255.0
ip ospf network point-to-point
!
```

**Sw1**

```
interface Loopback0
ip address 5.5.5.5 255.255.255.255
!
interface Ethernet0/0
switchport access vlan 10
ip flow ingress
ip flow egress
!
interface Ethernet0/1
switchport access vlan 12
ip flow ingress
ip flow egress
!
interface Ethernet0/2
switchport access vlan 14
ip flow ingress
ip flow egress
!
```

**Task 1**

You should configure the pre-configured NetFlow monitor e.g. "Export-FlowR1" to the interface E0/0 for both input and output direction as follows:

**R1**

```
ip flow monitor Monitor-FlowR1 input
ip flow monitor Monitor-FlowR1 output
```

**Remarks:**

You can use "sh flow interface e0/0" to check your settings.

**Task 2**

The following assumes that:

- IP SLA number "1" is not in use (you can use "sh ip sla summary" in R1 to verify it first).
- The loopback address of Sw1 is "5.5.5.5" (you can use "sh run" in Sw1 to verify it first).

After configuring the IP SLA, you should also start it.

**R1**

```
ip sla 1
icmp-echo 5.5.5.5
frequency 60
ip sla schedule 1 life forever start-time now
```

**Remarks:**

You can use "sh ip sla summary" to check your settings.

**Task 3**

The configuration required is:

**Sw1**

```
monitor session 5 source int e0/2 both
monitor session 5 destination int e1/0
```

**Remarks:**

You can use "sh monitor session 5" to check your settings.