

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

Explanation: There are five basic device roles in the fabric overlay:

+ Control plane node: This node contains the settings, protocols, and mapping tables to provide the endpoint-to-location (EID-to-RLOC) mapping system for the fabric overlay.

+ Fabric border node: This fabric device (for example, core layer device) connects external Layer 3 networks to the SDA fabric.

+ Fabric edge node: This fabric device (for example, access or distribution layer device) connects wired endpoints to the SDA fabric.

+ Fabric WLAN controller (WLC): This fabric device connects APs and wireless endpoints to the SDA fabric.

+ Intermediate nodes: These are intermediate routers or extended switches that do not provide any sort of SD-Access fabric role other than underlay services.

2. Refer to the exhibit. Which privilege level is assigned to VTY users?

```
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
```

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

Correct Answer: A

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

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 minor 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

Explanation: CEF uses a Forwarding Information Base (FIB) to make IP destination prefix-based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and those changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table. Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for route cache maintenance that is associated with earlier switching paths such as fast switching and optimum switching.

Note: In order to view the Routing information base (RIB) table, use the “show ip route” command. To view the Forwarding Information Base (FIB), use the “show ip cef” command. RIB is in Control plane while FIB is in Data plane.

4. What is a 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

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

6. Which two descriptions of Flex Connect mode for Cisco APs are true? (Choose two.)

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

Correct Answer: DE

Explanation: FlexConnect is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office.

The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller. In the connected mode, the FlexConnect access point can also perform local authentication.

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

Explanation:

The following different OSPF types are compatible with each other:

+ Broadcast and Non-Broadcast (adjust hello/dead timers)

+ Point-to-Point and Point-to-Multipoint (adjust hello/dead timers)

Broadcast and Non-Broadcast networks elect DR/BDR so they are compatible. Point-to-point/multipoint do not elect DR/BDR so they are compatible.

8. Which NGFW mode blocks flows crossing the firewall?

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

Correct Answer: B

Explanation: Firepower Threat Defense (FTD) provides six interface modes which are: Routed, Switched, Inline Pair, Inline Pair with Tap, Passive, Passive (ERSPAN).

When Inline Pair Mode is in use, packets can be blocked since they are processed inline. When you use Inline Pair mode, the packet goes mainly through the FTD Snort engine. When Tap Mode is enabled, a copy of the packet is inspected and dropped internally while the actual traffic goes through FTD unmodified.

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

Explanation: Answer 'Route targets allow customers to be assigned overlapping addresses' and answer 'Route targets uniquely identify the customer routing table' are not correct as only route distinguisher (RD) identifies the customer routing table and "allows customers to be assigned overlapping addresses". Answer 'When BGP is configured, route targets are transmitted as BGP standard communities' is not correct as "When BGP is configured, route targets are transmitted as BGP extended communities".

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

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

1. Refer to the exhibit. Which statement about the OPSF debug output is true?

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

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

Explanation: This combination of commands is known as “Conditional debug” and will filter the debug output based on your conditions. Each condition added, will behave like an ‘And’ operator in Boolean logic.

Some examples of the “debug ip ospf hello” are shown below:

```
*Oct 12 14:03:32.595: OSPF: Send hello to 224.0.0.5 area 0 on FastEthernet1/0 from
192.168.12.2
*Oct 12 14:03:33.227: OSPF: Rcv hello from 1.1.1.1 area 0 on FastEthernet1/0 from
192.168.12.1
*Oct 12 14:03:33.227: OSPF: Mismatched hello parameters from 192.168.12.1
```

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

Explanation: Proxy ingress tunnel router (PITR): answer 'PETR' PITR is an infrastructure LISP network entity that receives packets from non-LISP sites and encapsulates the packets to LISP sites or natively forwards them to non-LISP sites.

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

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

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

Explanation: A 401 error response indicates that the client tried to operate on a protected resource without providing the proper authorization. It may have provided the wrong credentials or none at all. Note: answer 'HTTP Status Code 200' 4xx code indicates a "client error" while a 5xx code indicates a "server error".

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 VTY group tacacs+ none
aaa session-id common
R1#sh run | section vty
line vty 0 4
password 7 0202039485748
R1#sh run | include username
R1#
```

B.

```
R1#sh run | include aaa
aaa new-model
aaa authentication login telnet group tacacs+ none
aaa session-id common
R1#sh run | section vty
line vty 0 4
R1#sh run | include username
R1#
```

C.

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

D.

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

Correct Answer: C

Explanation: According to the requirements (first use TACACS+, then allow login with no authentication), we have to use “aaa authentication login ... group tacacs+ none” for AAA command. The next thing to check is the if the “aaa authentication login default” or “aaa authentication login list-name” is used. The ‘default’ keyword means we want to apply for all login connections (such as tty, vty, console and aux). If we use this keyword, we don’t need to configure anything else under tty, vty and aux lines. If we don’t use this keyword then we have to specify which line(s) we want to apply the authentication feature.

From above information, we can find out answer ‘R1#sh run | include aaa aaa new-model aaa authentication login default group tacacs+ none aaa session-id common R1#sh run | section vty line vty 0 4 password 7 0202039485748 If you want to learn more about AAA configuration, please read our AAA TACACS+ and RADIUS Tutorial – Part 2.

For your information, answer ‘R1#sh run | include aaa
aaa new-model

aaa authentication login telnet group tacacs+ none
aaa session-id common

R1#sh run | section vty
line vty 0 4

R1#sh run | include username

R1#’ would be correct if we add the following command under vty line (“line vty 0 4”): “login authentication telnet” (“telnet” is the name of the AAA list above

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

Explanation: A rendezvous point (RP) is required only in networks running Protocol Independent Multicast sparse mode (PIM-SM).

By default, the RP is needed only to start new sessions with sources and receivers.

Reference: [here](#)

For your information, in PIM-SM, only network segments with active receivers that have explicitly requested multicast data will be forwarded the traffic. This method of delivering multicast data is in contrast to the PIM dense mode (PIM-DM) model. In PIM-DM, multicast traffic is initially flooded to all segments of the network. Routers that have no downstream neighbors or directly connected receivers prune back the unwanted traffic.

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

Explanation: Link aggregation (LAG) is a partial implementation of the 802.3ad port aggregation standard. It bundles all of the controller's distribution system ports into a single 802.3ad port channel.

Restriction for Link aggregation:

+ LAG requires the EtherChannel to be configured for 'mode on' on both the controller and the Catalyst switch.

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: C

Explanation: Cisco TrustSec uses tags to represent logical group privilege. This tag, called a Security Group Tag (SGT), is used in access policies. The SGT is understood and is used to enforce traffic by Cisco switches, routers and firewalls. Cisco TrustSec is defined in three phases: classification, propagation and enforcement.

When users and devices connect to a network, the network assigns a specific security group. This process is called classification. Classification can be based on the results of the authentication or by associating the SGT with an IP, VLAN, or port-profile (-> Answer 'security group tag ACL assigned to each port on a switch' and answer 'security group tag number assigned to each user on a switch' are not correct as they say "assigned ... on a switch" only. Answer 'security group tag ACL assigned to each router on a network' is not correct either as it says "assigned to each router").

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

Explanation: 802.11r Fast Transition (FT) Roaming is an amendment to the 802.11 IEEE standards. It is a new concept for roaming. The initial handshake with the new AP occurs before client roams to the target AP. Therefore it is called Fast Transition. 802.11r provides two methods of roaming:

- + Over-the-air: With this type of roaming, the client communicates directly with the target AP using IEEE 802.11 authentication with the Fast Transition (FT) authentication algorithm.

- + Over-the-DS (distribution system): With this type of roaming, the client communicates with the target AP through the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP and is then sent through the controller.

But both of these methods do not deal with legacy clients.

The 802.11k allows 11k capable clients to request a neighbor report containing information about known neighbor APs that are candidates for roaming.

Reference: [Click here](#)

IEEE 802.11v is an amendment to the IEEE 802.11 standard which describes numerous enhancements to wireless network management. One such enhancement is Network assisted Power Savings which helps clients to improve the battery life by enabling them to sleep longer. Another enhancement is Network assisted Roaming which enables the WLAN to send requests to associated clients, advising the clients as to better APs to associate to. This is useful for both load balancing and in directing poorly connected clients.

Reference: [Click here](#)

Cisco 802.11r supports three modes:

- + Pure mode: only allows 802.11r client to connect

- + Mixed mode: allows both clients that do and do not support FT to connect + Adaptive mode: does not advertise the FT AKM at all, but will use FT when supported clients connect Therefore “Adaptive mode” is the best answer here.

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

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

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

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

Correct Answer: BD

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

Explanation: The words “try” and “except” are Python keywords and are used to catch exceptions. For example:

```
try:  
    print 1/0  
except ZeroDivisionError:  
    print 'Error! We cannot divide by zero!!!'
```

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

Explanation: Server virtualization and the use of virtual machines is profoundly changing data center dynamics.

Most organizations are struggling with the cost and complexity of hosting multiple physical servers in their data centers. The expansion of the data center, a result of both scale-out server architectures and traditional “one application, one server” sprawl, has created problems in housing, powering, and cooling large numbers of underutilized servers. In addition, IT organizations continue to deal with the traditional cost and operational challenges of matching server resources to organizational needs that seem fickle and ever changing.

Virtual machines can significantly mitigate many of these challenges by enabling multiple application and operating system environments to be hosted on a single physical server while maintaining complete isolation between the guest operating systems and their respective applications. Hence, server virtualization facilitates server consolidation by enabling organizations to exchange a number of underutilized servers for a single highly utilized server running multiple virtual machines.

By consolidating multiple physical servers, organizations can gain several benefits:

- + Underutilized servers can be retired or redeployed.
- + Rack space can be reclaimed.
- + Power and cooling loads can be reduced.
- + New virtual servers can be rapidly deployed.
- + CapEx (higher utilization means fewer servers need to be purchased) and OpEx (few servers means a simpler environment and lower maintenance costs) can be reduced.

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

Explanation: A complete Cisco DNA Center upgrade includes “System Update” and “Application Updates”

System Update

System 1.3.0.109

🕒 Your system package is up to date. Proceed with Application updates.

Application Updates

Update All

Cisco DNA Center Core

	Size	Version	
Automation - Base	493.25 MB	2.1.78.60109	Update failed 🚩
NCP - Base	167.84 MB	2.1.78.60109	Update failed 🚩
NCP - Services	326.84 MB	2.1.78.60109	Update failed 🚩
Network Controller Platform	3.65 GB	2.1.78.60109	Update failed 🚩

Automation

	Size	Version	
Command Runner	55.20 MB	2.1.78.60109	Update failed 🚩
Device Onboarding	162.41 MB	2.1.78.60109	Update failed 🚩
Image Management	362.85 MB	2.1.78.60109	Update failed 🚩

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

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

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

Explanation:

JSON data is written as name/value pairs.

A name/value pair consists of a field name (in double quotes), followed by a colon, followed by a value:

"name": "Mark"

JSON can use arrays. Array values must be of type string, number, object, array, boolean or null. For example:

```
{  
  "name": "John",  
  "age": 30,  
  "alive": true,  
  "cars": [ "Ford", "BMW", "Fiat" ]  
}
```

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
```

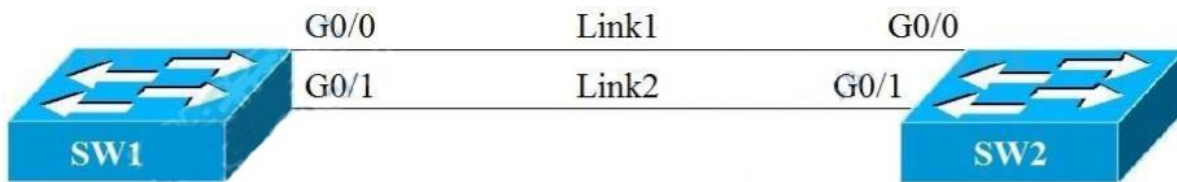
- A. 2WAY/DROTHER on both routers

- B. not established
- C. FULL on both routers
- D. FULL/BDR on R1 and FULL/BDR on R2

Correct Answer: B

Explanation: On Ethernet interfaces the OSPF hello interval is 10 second by default so in this case there would be a Hello interval mismatch -> the OSPF adjacency would not be established.

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 32769 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.lib	Type
-----	----	---	----	-----	-----
Gi0/0	Root	FWD	4	128.1	P2p
Gi0/1	Alto	BLW	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

Explanation: SW1 needs to block one of its ports to SW2 to avoid a bridging loop between the two switches.

Unfortunately, it blocked the fiber port Link2. But how does SW2 select its blocked port? Well, the answer is based on the BPDUs it receives from SW1. answer 'Enter spanning-tree port-priority 32 on

SW1' BPDUs are superior than another if it has:

1. answer 'Enter spanning-tree port-priority 32 on SW1' lower Root Bridge ID
 2. answer 'Enter spanning-tree port-priority 32 on SW1' lower path cost to the Root
 3. answer 'Enter spanning-tree port-priority 32 on SW1' lower Sending Bridge ID
 4. answer 'Enter spanning-tree port-priority 32 on SW1' lower Sending Port ID
- These four parameters are examined in order. In this specific case, all the BPDUs sent by SW1 have the same Root Bridge ID, the same path cost to the Root and the same Sending Bridge ID.

The only parameter left to select the best one is the Sending Port ID (Port ID = port priority + port index). And the port index of Gi0/0 is lower than the port index of Gi0/1 so Link 1 has been chosen as the primary link.

Therefore we must change the port priority to change the primary link. The lower numerical value of port priority, the higher priority that port has. In other words, we must change the port-priority on Gi0/1 of SW1 (not on Gi0/1 of SW2) to a lower value than that of Gi0/0.

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

Explanation: This JSON can be written as follows:

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

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

Explanation: According to the Meraki webpage, radar and rogue AP are two sources of Wireless Interference. Interference between different WLANs occurs when the access points within range of each other are set to the same RFchannel.

Note: Microwave ovens (not conventional oven) emit damaging interfering signals at up to 25 feet or so from an operatingoven. Some microwave ovens emit radio signals that occupy only a third of the 2.4-GHz band, whereas others occupy theentire band.

Reference: [Click here](#)

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

Explanation: The TCP port 6514 has been allocated as the default port for syslog over Transport Layer Security (TLS).

Reference: <https://tools.ietf.org/html/rfc5425>

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

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

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

Correct Answer: C

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

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

36. Refer to the exhibit. Which IP address becomes the active next hop for 192.168.102.0/24 when 192.168.101.2 fails?

```
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

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

Correct Answer: D

Explanation: The '>' shown in the output above indicates that the path with a next hop of 192.168.101.2 is the current best path.

Path Selection Attributes: Weight > Local Preference > Originate > AS Path > Origin > MED >

External > IGP Cost > eBGP Peering > Router ID BGP prefers the path with highest weight but the weights here are all 0 (which indicate all routes that are not originated by the local router) so we need to check the Local Preference. Answer '192.168.101.18' path without LOCAL_PREF (LocPrf column) means it has the default value of 100.

Therefore we can find the two next best paths with the next hop of 192.168.101.18 and 192.168.101.10.

We have to move to the next path selection attribute: Originate. BGP prefers the path that the local router originated (which is indicated with the "next hop 0.0.0.0"). But none of the two best paths is self-originated.

The AS Path of the next hop 192.168.101.18 is shorter than the AS Path of the next hop 192.168.101.10 then the next hop 192.168.101.18 will be chosen as the next best path.

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

Explanation: There are two PAgP modes:

	Responds to PAGP messages but does not aggressively negotiate a PAGP
Auto	EtherChannel. Answer 'auto/auto' channel is formed only if the port on the other end is set to Desirable. This is the default mode.
Desirable	Port actively negotiates channeling status with the interface on the other end of the link. Answer 'auto/auto' channel is formed if the other side is Auto or Desirable.

The table below lists if an EtherChannel will be formed or not for PAgP:

PAgP	Desirable	Auto
Desirable	Yes	Yes
Auto	Yes	No

Reference: <https://www.omniseccu.com/cisco-certified-network-associate-ccna/etherchannel-pagp-and-lacp-modes.php>

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

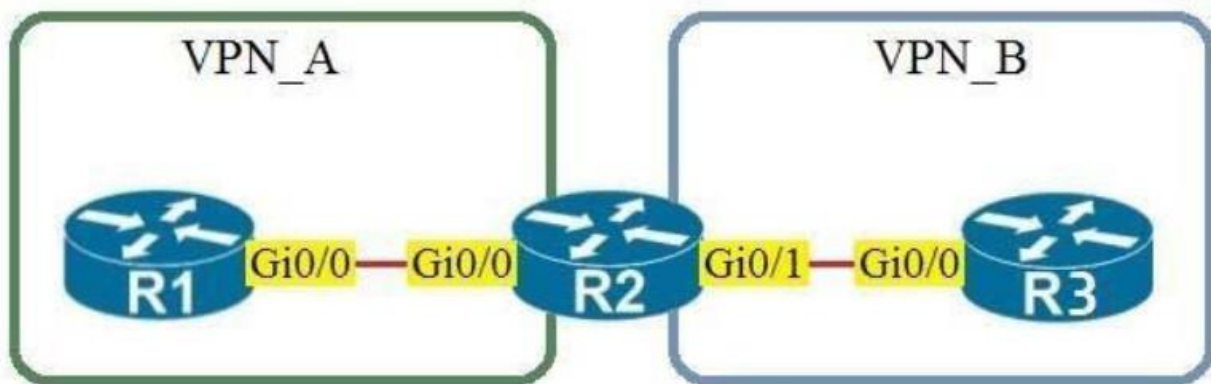
39. Which QoS component alters a packet to change the way that traffic is treated in the network?

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

Correct Answer: C

Explanation: QoS Packet Marking refers to changing a field within a packet either at Layer 2 (802.1Q/p CoS, MPLS EXP) or Layer 3 (IP Precedence, DSCP and/or IP ECN).

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

Explanation: There is nothing special with the configuration of Gi0/0 on R1. Only Gi0/0 interface on R2 is assigned to VRF VPN_A. The default VRF here is similar to the global routing table concept in Cisco IOS

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

General Security QoS Advanced Policy Mapping

Layer 2 Layer 3 AAA Servers

Fast Transition

Fast Transition ☐

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy-AES ☒

Authentication Key Management

802.1X	☐	Enable
CCKM	☐	Enable
PSK	☒	Enable
FT 802.1X	☐	Enable
FT PSK	☐	Enable
PSK Format		ASCII

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

Correct Answer: A

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

Explanation: The time kept on a machine is a critical resource and it is strongly recommend that you use the security features of NTP to avoid the accidental or malicious setting of incorrect time. The two security features available are an access list-based restriction scheme and an encrypted authentication mechanism.

Reference: <https://www.cisco.com/c/dam/en/us/td/docs/ios-xml/ios/bsm/configuration/xen-3se/3650/bsm-xe-3se-3650-book.html>

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

Explanation: MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using outofband methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1x Extensible Authentication Protocol (EAP-TLS) or Pre Shared Key (PSK) framework.

A switch using MACsec accepts either MACsec or non-MACsec frames, depending on the policy associated with the MKA peer. MACsec frames are encrypted and protected with an integrity check value (ICV). When the switch receives frames from the MKA peer, it decrypts them and calculates the correct ICV by using session keys provided by MKA. The switch compares that ICV to the ICV within the frame. If they are not identical, the frame is dropped. The switch also encrypts and adds an ICV to any frames sent over the secured port (the access point used to provide the secure MAC service to a MKA peer) using the current session key.

Reference: [Click here](#)

Note: Cisco Trustsec is the solution which includes MACsec.

44. Refer to the exhibit.

```

Extended IP access list EGRESS
10 permit ip 10.0.0.0.0.0.255 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

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

Explanation: A Cisco lightweight wireless AP needs to be paired with a WLC to function.

An AP must be very diligent to discover any controllers that it can join-all without any preconfiguration on your part. To accomplish this feat, several methods of discovery are used.

The goal of discovery is just to build a list of live candidate controllers that are available, using the following methods:

- + Prior knowledge of WLCs
- + DHCP and DNS information to suggest some controllers (DHCP Option 43)
- + Broadcast on the local subnet to solicit controllers

Reference: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide If you do not tell the LAP where the controller is via DHCP option 43, DNS resolution of “Cisco-capwap-controller.local_domain”, or statically configure it, the LAP does not know where in the network to find the management interface of the controller.

In addition to these methods, the LAP does automatically look on the local subnet for controllers with a 255.255.255.255 local broadcast.

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

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

Explanation:

Cisco IOS IP SLA Responder is a Cisco IOS Software component whose functionality is to respond to Cisco IOS IP SLA request packets. The IP SLA source sends control packets before the operation starts to establish a connection to the responder. Once the control packet is acknowledged, test packets are sent to the responder. The responder inserts a time-stamp when it receives a packet and factors out the destination processing time and adds time-stamps to the sent packets. This feature allows the calculation of unidirectional packet loss, latency, and jitter measurements with the kind of accuracy that is not possible with ping or other dedicated probe testing.

Reference: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/46sg/configuration/guide/Wrapper-46SG/swipsla.pdf>

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

Explanation: There are two types of hypervisors: type 1 and type 2 hypervisor.

In type 1 hypervisor (or native hypervisor), the hypervisor is installed directly on the physical server.

Then instances of an operating system (OS) are installed on the hypervisor. Type 1 hypervisor has direct access to the hardware resources. Therefore they are more efficient than hosted architectures.

Some examples of type 1 hypervisor are VMware vSphere/ESXi, Oracle VM Server, KVM and Microsoft Hyper-V.

In contrast to type 1 hypervisor, a type 2 hypervisor (or hosted hypervisor) runs on top of an operating system and not the physical hardware directly. answer 'Type 1 hypervisor runs directly on the physical hardware of the host machine without relying on the underlying OS' big advantage of Type 2 hypervisors is that management console software is not required. Examples of type 2 hypervisor are VMware Workstation (which can run on Windows, Mac and Linux) or Microsoft Virtual PC (only runs on Windows).



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 servers. 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

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

Explanation: Summary ASBR LSA (Type 4) – Generated by the ABR to describe an ASBR to routers in other areas so that routers in other areas know how to get to external routes through that ASBR. For example, suppose R8 is redistributing external route (EIGRP, RIP...) to R3. This makes R3 an Autonomous System Boundary Router (ASBR). When R2 (which is an ABR) receives this LSA Type 1 update, R2 will create LSA Type 4 and flood into Area 0 to inform them how to reach R3. When R5 receives this LSA it also floods into Area 2. In the above example, the only ASBR belongs to area 1 so the two ABRs (R2 & R5) send LSA Type 4 to area 0 & area 2 (not vice versa). This is an indication of the existence of the ASBR in area 1.

Note:

+ Type 4 LSAs contain the router ID of the ASBR.

+ There are no LSA Type 4 injected into Area 1 because every router inside area 1 knows how to reach R3. R3 only uses LSA Type 1 to inform R2 about R8 and inform R2 that R3 is an ASBR.

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

Explanation: SW3 does not have VLAN 60 so it should not receive traffic for this VLAN (sent from SW2).

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

Reference: <https://www.orbit-computer-solutions.com/vtp-pruning/>

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

Explanation: Fabric mode APs continue to support the same wireless media services that traditional APs support; apply AVC, quality of service (QoS), and other wireless policies; and establish the CAPWAP control plane to the fabric WLC. Fabric APs join as local-mode APs and must be directly connected to the fabric edge node switch to enable fabric registration events, including RLOC assignment via the fabric WLC. The fabric edge nodes use CDP to recognize APs as special wired hosts, applying special port configurations and assigning the APs to a unique overlay network within a common EID space across a fabric. The assignment allows management simplification by using a single subnet to cover the AP infrastructure at a fabric site.

Reference: <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/sda-sdg-2019oct.html>

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

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

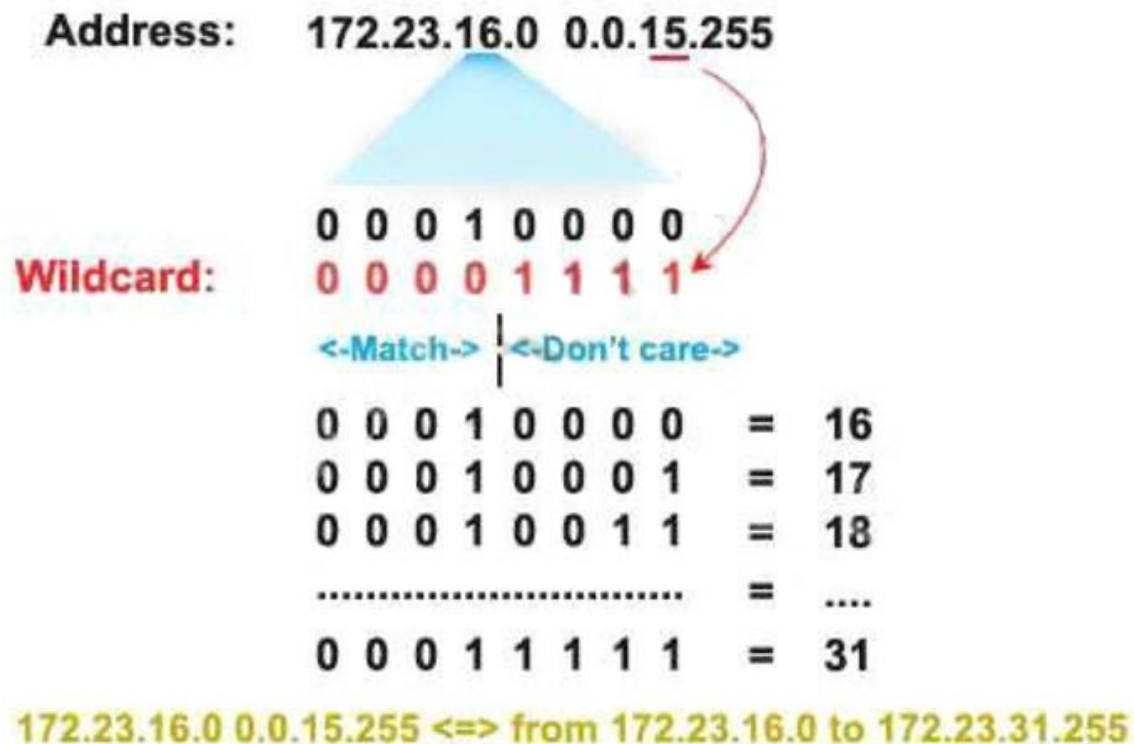
- A. permit 10.0.0.0 0.0.0.1
- **B. permit 10.0.0.1 0.0.0.254**
- C. permit 10.0.0.1 0.0.0.0
- D. permit 10.0.0.0 255.255.255.254

Correct Answer: B

Explanation: Remember, for the wildcard mask, 1s are I DON'T CARE, and 0s are I CARE. So now let's analyze a simple ACL:

access-list 1 permit 172.23.16.0 0.0.15.255

Two first octets are all 0's meaning that we care about the network .x.x. The third octet of the wildcard mask, 15 (0000 1111 in binary), means that we care about first 4 bits but don't care about last 4 bits so we allow the third octet in the form of 0001xxxx (minimum:00010000 = 16; maximum: 00011111 = 31).



The fourth octet is 255 (all 1 bits) that means I don't care.

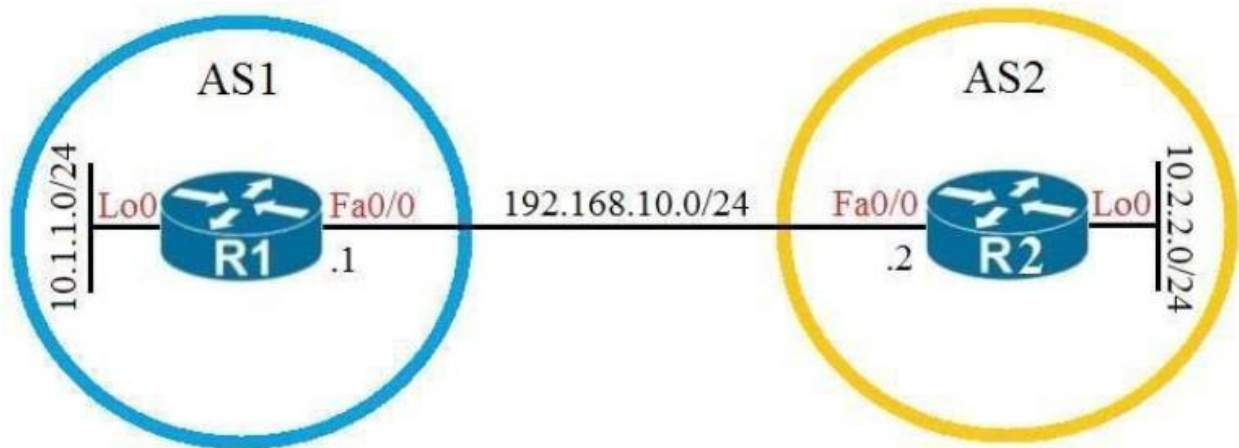
Therefore network 172.23.16.0 0.0.15.255 ranges from 172.23.16.0 to 172.23.31.255.

Now let's consider the wildcard mask of 0.0.0.254 (four octet: 254 = 1111 1110) which means we only care the last bit. Therefore if the last bit of the IP address is a "1" (0000 0001) then only odd numbers are allowed. If the last bit of the IP address is a "0" (0000 0000) then only even numbers are allowed.

Note: In binary, odd numbers are always end with a "1" while even numbers are always end with a "0".

Therefore in this question, only the statement "permit 10.0.0.1 0.0.0.254" will allow all oddnumbered hosts in the 10.0.0.0/24 subnet.

54. Refer to the exhibit.Which configuration establishes EBGp connected 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

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

It is easy to establish eBGP neighborship via the direct link. But let’s see what are required when we want to establish eBGP neighborship via their loopback interfaces. We will need two commands:

- + the command “neighbor 10.1.1.1 ebgp-multihop 2” on R1 and “neighbor 10.2.2.2 ebgpmultihop 2” on R1. This command increases the TTL value to 2 so that BGP updates can reach the BGP neighbor which is two hops away.

- + Answer ‘R1 (config) #router bgp 1

```
R1 (config-router) #neighbor 192.168.10.2 remote-as 2
```

```
R1 (config-router) #network 10.1.1.0 mask 255.255.255.0
```

```
R2 (config) #router bgp 2
```

```
R2 (config-router) #neighbor 192.168.10.1 remote-as 1
```

```
R2 (config-router) #network 10.2.2.0 mask 255.255.255.0
```

Quick Wireless Summary

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

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

- + Lightweight: A Cisco lightweight AP (LAP) has to join a Wireless LAN Controller (WLC) to function.

LAP and WLC communicate with each other via a logical pair of CAPWAP tunnels.

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

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

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

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

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

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

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

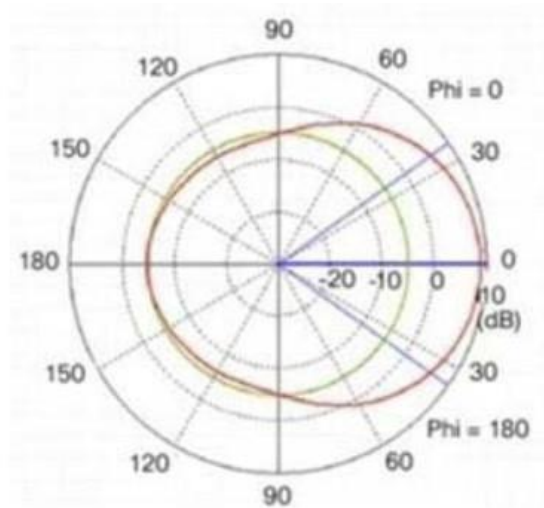
- + Rogue detector mode: monitor for rogue APs. It does not handle data at all.

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

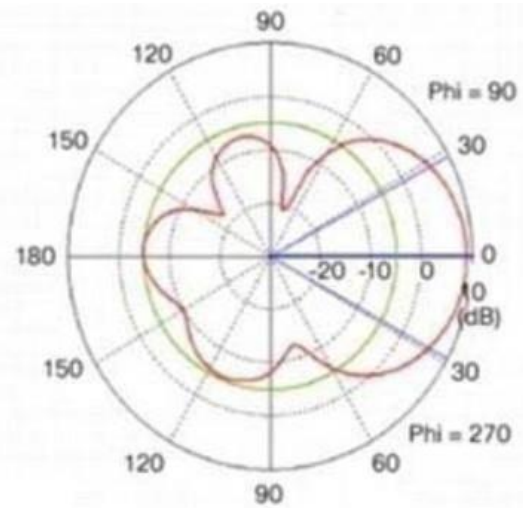
- + Bridge mode: bridge together the WLAN and the wired infrastructure together. Mobility

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

55. Refer to the exhibit. Which type of antenna do the radiation patterns present?



**Antenna Azimuth
Plane Pattern**



**Antenna Elevation
Plane Pattern**

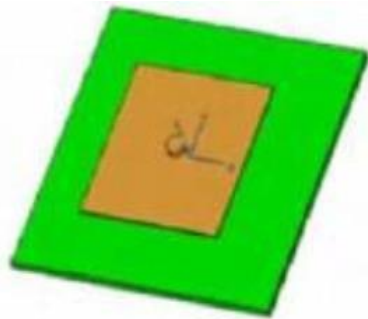
- A. Yagi
- **B. patch**
- C. omnidirectional
- D. dipole

Correct Answer: B

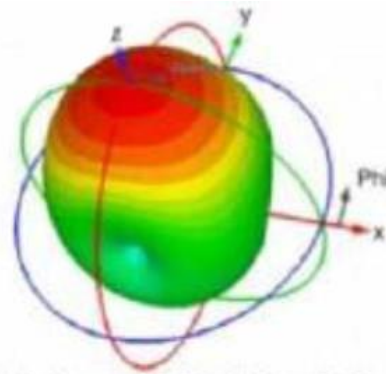
Explanation:

A patch antenna, in its simplest form, is just a single rectangular (or circular) conductive plate that is spaced above a ground plane. Patch antennas are attractive due to their low profile and ease of fabrication.

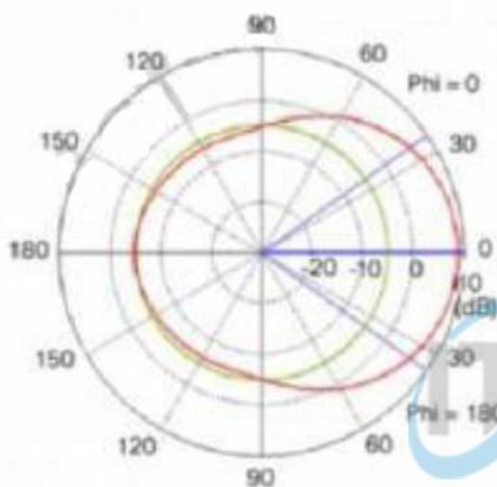
The azimuth and elevation plane patterns are derived by simply slicing through the 3D radiation pattern. In this case, the azimuth plane pattern is obtained by slicing through the x-z plane, and the elevation plane pattern is formed by slicing through the y-z plane. Note that there is one main lobe that is radiated out from the front of the antenna. There are three back lobes in the elevation plane (in this case), the strongest of which happens to be 180 degrees behind the peak of the main lobe, establishing the front-to-back ratio at about 14 dB. That is, the gain of the antenna 180 degrees behind the peak is 14 dB lower than the peak gain.



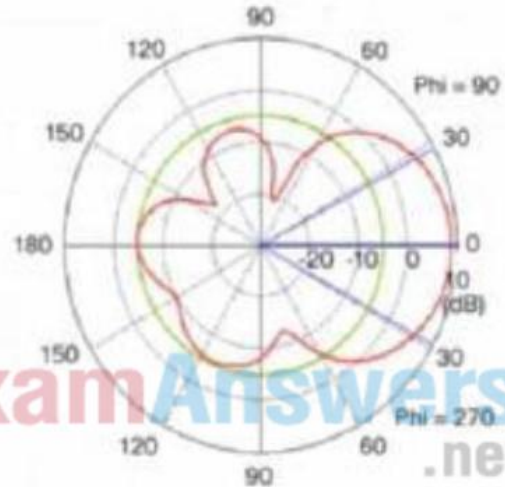
(a) Patch Antenna Model



(b) Patch Antenna 3D Radiation Pattern



(c) Patch Antenna Azimuth Plane Pattern



(d) Patch Antenna Elevation Plane Pattern

Again, it doesn't matter if these patterns are shown pointing up, down, to the left or to the right. That is usually an artifact of the measurement system. answer 'Patch' patch antenna radiates its energy out from the front of the antenna. That will establish the true direction of the patterns.

Reference: https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/prod_white_paper0900aecd806a1a3e.html

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

Explanation: An EEM policy is an entity that defines an event and the actions to be taken when that event occurs. There are two types of EEM policies: an applet or a script. An applet is a simple form of policy that is defined within the CLI configuration. answer 'event manager applet ondemand event register action 1.0 syslog priority critical msg 'This is a message from ondemand'

<="" p="" style="box-sizing: border-box;">

There are two ways to manually run an EEM policy. EEM usually schedules and runs policies on the basis of an event specification that is contained within the policy itself. The event none command allows EEM to identify an EEM policy that can be manually triggered. To run the policy, use either the action policy command in applet configuration mode or the event manager run command in privileged EXEC mode.

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

Explanation: "The next step is to configure the WLC for the Internal web authentication. Internal web authentication is the default web authentication type on WLCs." In step 4 of the link above, we will configure Security as described in this question. Therefore we can deduce this configuration is for Internal web authentication.

This paragraph was taken from the link

[Click here](#)

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

- A. vBond

- B. vSmart
- **C. vManage**
- D. vEdge

Correct Answer: C

Explanation: The primary components for the Cisco SD-WAN solution consist of the vManage network management system (management plane), the vSmart controller (control plane), the vBond orchestrator (orchestration plane), and the vEdge router (data plane).

+ vManage – This centralized network management system provides a GUI interface to easily monitor, configure, and maintain all Cisco SD-WAN devices and links in the underlay and overlay network.

+ vSmart controller – This software-based component is responsible for the centralized control plane of the SD-WAN network. It establishes a secure connection to each vEdge 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 vEdge routers by distributing crypto key information, allowing for a very scalable, IKE-less architecture.

+ vBond orchestrator – This software-based component performs the initial authentication of vEdge devices and orchestrates vSmart and vEdge connectivity. It also has an important role in enabling the communication of devices that sit behind Network Address Translation (NAT).

+ vEdge 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.

Reference: <https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/CVD-SD-WAN-Design-2018OCT.pdf>

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

60. 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

Explanation: When a device boots up with the startup configuration, the nginx process will be running. NGINX is an internal webserver that acts as a proxy webserver. It provides Transport Layer Security (TLS)-based HTTPS. RESTCONF request sent via HTTPS is first received by the NGINX proxy web server, and the request is transferred to the confd web server for further syntax/semantics check.

61. Which reason could cause an OSPF neighborship 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

Explanation:

When OSPF adjacency is formed, a router goes through several state changes before it becomes fully adjacent with its neighbor. The states are Down -> Attempt (optional) -> Init -> 2-Way -> Exstart -> Exchange -> Loading -> Full. Short descriptions about these states are listed below:
Down: no information (hellos) has been received from this neighbor.

Attempt: only valid for manually configured neighbors in an NBMA environment. In Attempt state, the router sends unicast hello packets every poll interval to the neighbor, from which hellos have not been received within the dead interval.

Init: specifies that the router has received a hello packet from its neighbor, but the receiving router's ID was not included in the hello packet

2-Way: indicates bi-directional communication has been established between two routers.

Exstart: Once the DR and BDR are elected, the actual process of exchanging link state information can start between the routers and their DR and BDR.

Exchange: OSPF routers exchange database descriptor (DBD) packets

Loading: In this state, the actual exchange of link state information occurs Full: routers are fully adjacent with each other (Reference:

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0e.s.html)

Neighbors Stuck in Exstart/Exchange State the problem occurs most frequently when attempting to run OSPF between a Cisco router and another vendor's router. The problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces don't match. If the router with the higher MTU sends a packet larger than the MTU set on the neighboring router, the neighboring router ignores the packet.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/166/b_166_programmability_cg/b_166_programmability_cg_chapter_01011.html

62. 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

Explanation:

An Egress Tunnel Router (ETR) connects a site to the LISP-capable part of a core network (such as the Internet), publishes EID-to-RLOC mappings for the site, responds to Map-Request messages, and decapsulates and delivers LISP-encapsulated user data to end systems at the site.

Reference: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/locator-id-separation-protocol-lisp/white_paper_c11-652502.html

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

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

Correct Answer: A

Explanation:

Reference: <https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/107614-64.html>

64. 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

Explanation: Agentless tool means that no software or agent needs to be installed on the client machines that are to be managed. Ansible is such an agentless tool. In contrast to agentless tool, agent-based tool requires software or agent to be installed on the client. Therefore the master and slave nodes can communicate directly without the need of high-level language interpreter. An agentless tool uses standard protocols, such as SSH, to push configurations down to a device (and it can be considered a “messaging system”).

65. 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

Explanation: Cisco Express Forwarding (CEF) provides the ability to switch packets through a device in a very quick and efficient way while also keeping the load on the router’s processor low. CEF is made up of two different main components: the Forwarding Information Base (FIB) and the Adjacency Table. These are automatically updated at the same time as the routing table. The Forwarding Information Base (FIB) contains destination reachability information as well as next hop information. This information is then used by the router to make forwarding decisions. The FIB allows for very efficient and easy lookups. Below is an example of the FIB table:

```
R2#show ip cef
```

Prefix	Next Hop	Interface
0.0.0.0/0	192.168.201.1	FastEthernet0/0
0.0.0.0/32	receive	
192.168.201.0/27	attached	FastEthernet0/0
192.168.201.0/32	receive	
192.168.201.1/32	192.168.201.1	FastEthernet0/0
192.168.201.2/32	receive	
192.168.201.31/32	receive	
224.0.0.0/4	drop	
224.0.0.0/24	receive	
255.255.255.255/32	receive	

The adjacency table is tasked with maintaining the layer 2 next-hop information for the FIB. An example of the adjacency table is shown below:

Router#show adjacency		
Protocol	Interface	Address

IP	Serial0	192.168.209.130 (2) (incomplete)
IP	Serial0	192.168.209.131 (7)
IP	Ethernet0	192.168.201.1 (7)

It uses a fast cache that is maintained in a router data plane' fast cache is only used when fast switching is enabled while CEF is disabled.

66. Refer to the exhibit. What are two effects of this configuration? (Choose two.)

```
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
```

- 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: CD

67. 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

Explanation: Deploying WPA2-Enterprise requires a RADIUS server, which handles the task of authenticating network users access. The actual authentication process is based on the 802.1X policy and comes in several different systems labelled EAP. Because each device is authenticated before it connects, a personal, encrypted tunnel is effectively created between the device and the network.

Reference: [Click here](#)

Reference: [Click here](#)

68. 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

Explanation: JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA or ECDSA. JSON Web Tokens are composed of three parts, separated by a dot (.): Header, Payload, Signature.

Therefore, a JWT typically looks like the following:

xxxxx.yyyyy.zzzzz

The header typically consists of two parts: the type of the token, which is JWT, and the signing algorithm being used, such as HMAC SHA256 or RSA.

The second part of the token is the payload, which contains the claims. Claims are statements about an entity (typically, the user) and additional data.

To create the signature part you have to take the encoded header, the encoded payload, a secret, the algorithm specified in the header, and sign that.

Reference: <https://auth0.com/docs/tokens/references/jwt-structure>

69. 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

Explanation: The 404 (Not Found) error status code indicates that the REST API can't map the client's URI to a resource but may be available in the future. Subsequent requests by the client are permissible.

70. 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 coding 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

Explanation: The difference between on-premise and cloud is essentially where this hardware and software resides. On-premise means that a company keeps all of this IT environment onsite either managed by themselves or a third-party. Cloud means that it is housed offsite with someone else responsible for monitoring and maintaining it.

71. 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

Explanation: Mobility Express is the ability to use an access point (AP) as a controller instead of a real WLAN controller.

But this solution is only suitable for small to midsize, or multi-site branch locations where you might not want to invest in a dedicated WLC. answer 'Autonomous' Mobility Express WLC can support up to 100 APs.

Mobility Express WLC also uses CAPWAP to communicate to other APs.

Note: Local mode is the most common mode that an AP operates in. This is also the default mode. In local mode, the LAP maintains a CAPWAP (or LWAPP) tunnel to its associated controller.

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

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

Correct Answer: CF

Explanation: RESTCONF operations include OPTIONS, HEAD, GET, POST, PATCH, DELETE.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/166/b_166_programmability_cg/b_166_programmability_cg_chapter_01011.html

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

Clients > Detail

< Back

Apply

Link Test

Remove

Client Properties		AP Properties	
MAC Address	00:09:ef:95:07: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	1602	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	LUN	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	5.5,11.0,6.6,9.0,12.0,19.0,24.0,26.6,40.0,51.6		

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

Correct Answer: B

Explanation: If the clients roam between APs registered to different controllers and the client WLAN on the two controllers is on different subnet, then it is called inter-controller L3 roam.

In this situation as well controllers exchange mobility messages. Client database entry change is completely different that to L2 roam (instead of move, it will copy). In this situation the original controller marks the client entry as “Anchor” where as new controller marks the client entry as “Foreign”. The two controllers now referred to as “Anchor controller” & “Foreign Controller” respectively. Client will keep the original IP address & that is the real advantage.

Note: Inter-Controller (normally layer 2) roaming occurs when a client roam between two APs registered to two different controllers, where each controller has an interface in the client subnet.

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

- A. HTTP method
- B. body
- **C. header**
- D. URI

Correct Answer: C

Explanation:

Reference: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Type>

75. 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

Explanation: 802.1Q VLAN identifier space is only 12 bits. The VXLAN identifier space is 24 bits. This doubling in size allows the VXLAN ID space to support 16 million Layer 2 segments - > Answer 'VXLAN extends the Layer 2 Segment ID field to 24-bits, which allows up to 4094 unique Layer 2 segments over the same network' is not correct.

VXLAN is a MAC-in-UDP encapsulation method that is used in order to extend a Layer 2 or Layer 3 overlay network over a Layer 3 infrastructure that already exists.

76. 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

Explanation: The EAP-FAST protocol is a publicly accessible IEEE 802.1X EAP type that Cisco developed to support customers that cannot enforce a strong password policy and want to deploy an 802.1X EAP type that does not require digital certificates.

EAP-FAST is also designed for simplicity of deployment since it does not require a certificate on the wireless LAN client or on the RADIUS infrastructure yet incorporates a built-in provisioning mechanism.

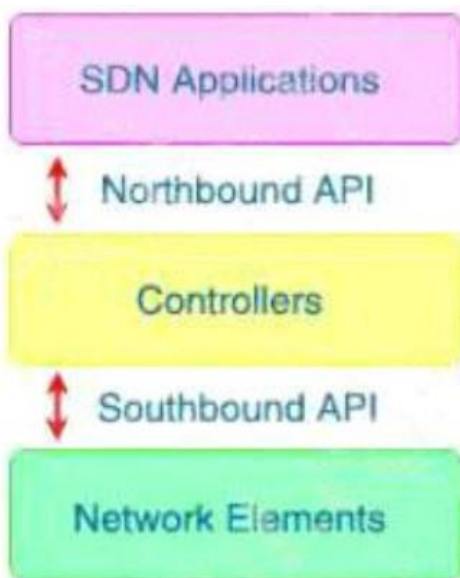
Reference: <https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/99791-eapfast-wlc-rad-config.html>

77. 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

Explanation: The Southbound API is used to communicate with network devices.



78. 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

Explanation: The Lightweight AP (LAP) can discover controllers through your domain name server (DNS). For the access point (AP) to do so, you must configure your DNS to return controller IP addresses in response to CISCO-LWAPP-CONTROLLER.localdomain, where localdomain is the AP domain name. When an AP receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCOCAPWAP-CONTROLLER.localdomain. When the DNS sends a list of controller IP addresses, the AP sends discovery requests to the controllers.

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.

Reference: http://www.revolutionwifi.net/revolutionwifi/2010/11/capwap-controller-discovery-process_23.html

79. 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

Explanation: The TCP Maximum Segment Size (TCP MSS) defines the maximum amount of data that a host is willing to accept in a single TCP/IP datagram. This TCP/IP datagram might be fragmented at the IP layer. The MSS value is sent as a TCP header option only in TCP SYN segments. Each side of a TCP connection reports its MSS value to the other side. Contrary to popular belief, the MSS value is not negotiated between hosts. The sending host is required to limit the size of data in a single TCP segment to a value less than or equal to the MSS reported by the receiving host.

TCP MSS takes care of fragmentation at the two endpoints of a TCP connection, but it does not handle the case where there is a smaller MTU link in the middle between these two endpoints. PMTUD was developed in order to avoid fragmentation in the path between the endpoints. It is used to dynamically determine the lowest MTU along the path from a packet's source to its destination.

80. 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

Explanation: in all participating switches -> This VLAN can be considered a special VLAN type -> Answer 'A special VLAN type must be used as the RSPAN destination' is correct.

81. Refer to the exhibit. 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?

```
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
```

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

82. What is the role of a fusion router in an SD-Access solution?

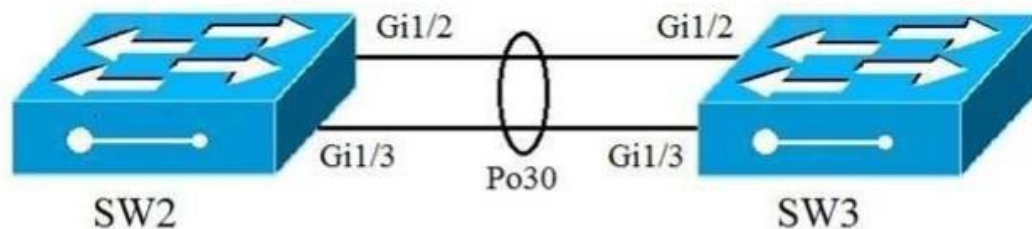
- A. acts as a DNS server
- B. provides additional forwarding capacity to the fabric
- C. performs route leaking between user-defined virtual networks and shared services
- D. provides connectivity to external networks

Correct Answer: C

Explanation: Today the Dynamic Network Architecture Software Defined Access (DNA-SDA) solution requires a fusion router to perform VRF route leaking between user VRFs and Shared-Services, which may be in the Global routing table (GRT) or another VRF. Shared Services may consist of DHCP, Domain Name System (DNS), Network Time Protocol (NTP), Wireless LAN Controller (WLC), Identity Services Engine (ISE), DNAC components which must be made available to other virtual networks (VN's) in the Campus.

Reference: <https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/dna-center/213525-sda-steps-to-configure-fusion-router.html#anc1>

83. 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 except 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

Explanation: The Cisco switch was configured with PAgP, which is a Cisco proprietary protocol so non-Cisco switch could not communicate.

84. What does this EEM applet event accomplish?

“event snmp oid 1.3.6.1.3.7.1.5.1.2.4.2.9 get-type next entry-op g 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

Explanation: EEM offers the ability to monitor events and take informational or corrective action when the monitored events occur or reach a threshold. An EEM policy is an entity that defines an event and the actions to be taken when that event occurs. There are two types of EEM policies: an applet or a script. An applet is a simple form of policy that is defined within the CLI configuration.

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run by sampling Simple Network Management Protocol (SNMP) object identifier values, use the event snmp command in applet configuration mode.

event snmp oid oid-value get-type {exact | next} entry-op operator entry-val entryvalue [exit-comb {or | and}] [exit-op operator] [exit-val exit-value] [exit-time exit-timevalue] poll-interval poll-int-value

+ oid: Specifies the SNMP object identifier (object ID)

+ get-type: Specifies the type of SNMP get operation to be applied to the object ID specified by the oid-value argument.

– next – Retrieves the object ID that is the alphanumeric successor to the object ID specified by the oid-value argument.

+ entry-op: Compares the contents of the current object ID with the entry value using the specified operator. If there is a match, an event is triggered and event monitoring is disabled until the exit criteria are met.

+ entry-val: Specifies the value with which the contents of the current object ID are compared to decide if an SNMP event should be raised.

+ exit-op: Compares the contents of the current object ID with the exit value using the specified operator. If there is a match, an event is triggered and event monitoring is reenabled.

+ poll-interval: Specifies the time interval between consecutive polls (in seconds)

85. 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

86. 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

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

Reference: <https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html>

87. 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

Explanation:

+ Orchestration plane (vBond) assists in securely onboarding the SD-WAN WAN Edge routers into the SD-WAN overlay (-> Therefore answer “onboard vEdge nodes into the SD-WAN fabric” mentioned about vBond). The vBond controller, or orchestrator, authenticates and authorizes the SD-WAN components onto the network. The vBond orchestrator takes an added responsibility to distribute the list of vSmart and vManage controller information to the WAN Edge routers. vBond is the only device in SD-WAN that requires a public IP address as it is the first point of contact and authentication for all SD-WAN components to join the SD-WAN fabric. All other components need to know the vBond IP or DNS information.

+ Management plane (vManage) is responsible for central configuration and monitoring. The vManage controller is the centralized network management system that provides a single pane of glass GUI interface to easily deploy, configure, monitor and troubleshoot all Cisco SD-WAN components in the network. (-> Answer “manage, maintain, and gather configuration and status for nodes within the SD-WAN fabric” and answer “gather telemetry data from vEdge routers” are about vManage)

+ Control plane (vSmart) builds and maintains the network topology and make decisions on the traffic flows. The vSmart controller disseminates control plane information between WAN Edge devices, implements control plane policies and distributes data plane policies to network devices for enforcement (-> Answer “distribute security information for tunnel establishment between vEdge routers” is about vSmart)

88. 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

Explanation: Access Points

+ AP is directly connected to FE (or to an extended node switch)

+ AP is part of Fabric overlay

89. 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

Explanation: EIGRP support unequal-cost load balancing via the “variance ...” while OSPF only supports equalcost load balancing.

90. 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

Explanation: Path Selection Attributes: Weight > Local Preference > Originate > AS Path > Origin > MED > External > IGP Cost > eBGP Peering > Router ID

91. 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

92. Which tunneling technique is used when designing a Cisco SD-Access fabric data plane?

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

Correct Answer: A

Explanation: The tunneling technology used for the fabric data plane is based on Virtual Extensible LAN (VXLAN). VXLAN encapsulation is UDP based, meaning that it can be forwarded by any IP-based network (legacy or third party) and creates the overlay network for the SD-Access fabric. Although LISP is the control plane for the SD-Access fabric, it does not use LISP data encapsulation for the data plane; instead, it uses VXLAN encapsulation because it is capable of encapsulating the original Ethernet header to perform MAC-in-IP encapsulation,

while LISP does not. Using VXLAN allows the SD-Access fabric to support Layer 2 and Layer 3 virtual topologies (overlays) and the ability to operate over any IP-based network with built-in network segmentation (VRF instance/VN) and built-in group-based policy.

93. 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

Explanation: The “enable secret” password is always encrypted (independent of the “service passwordencryption” command) using MD5 hash algorithm. The “enable password” does not encrypt the password and can be view in clear text in the running-config. In order to encrypt the “enable password”, use the “service password-encryption” command. This command will encrypt the passwords by using the Vigenere encryption algorithm. Unfortunately, the Vigenere encryption method is cryptographically weak and trivial to reverse. The MD5 hash is a stronger algorithm than Vigenere so answer ‘The enable secret password is protected via stronger cryptography mechanisms’ is correct.

94. Which access controls 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 it 444

B.
Permit tcp any any ne 80

**C.
Permit tcp any any range 22 443
Deny tcp any any eq 80**

D.
Deny tcp any any ne 80
Permit tcp any any range 22 443

Correct Answer: C (not sure)

95. 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

Explanation: A virtual machine (VM) is a software emulation of a physical server with an operating system.

From an application's point of view, the VM provides the look and feel of a real physical server, including all its components, such as CPU, memory, and network interface cards (NICs).

The virtualization software that creates VMs and performs the hardware abstraction that allows multiple VMs to run concurrently is known as a hypervisor.

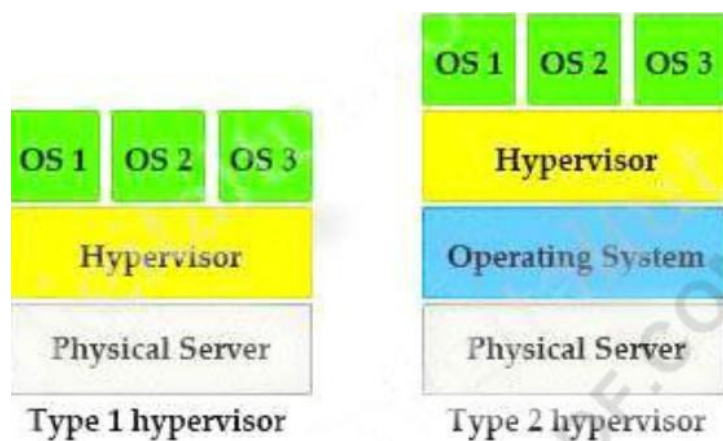
There are two types of hypervisors: type 1 and type 2 hypervisor.

In type 1 hypervisor (or native hypervisor), the hypervisor is installed directly on the physical server.

Then instances of an operating system (OS) are installed on the hypervisor. Type 1 hypervisor has direct access to the hardware resources. Therefore they are more efficient than hosted architectures.

Some examples of type 1 hypervisor are VMware vSphere/ESXi, Oracle VM Server, KVM and Microsoft Hyper-V.

In contrast to type 1 hypervisor, a type 2 hypervisor (or hosted hypervisor) runs on top of an operating system and not the physical hardware directly. answer 'Each virtual machine requires a unique IP and MAC addresses to be able to reach to other nodes' big advantage of Type 2 hypervisors is that management console software is not required. Examples of type 2 hypervisor are VMware Workstation (which can run on Windows, Mac and Linux) or Microsoft Virtual PC (only runs on Windows).



96. 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

Explanation: The BGP session may report in the following states

1 – Idle: the initial state of a BGP connection. In this state, the BGP speaker is waiting for a BGP start event, generally either the establishment of a TCP connection or the re-establishment of a previous connection. Once the connection is established, BGP moves to the next state.

2 – Connect: In this state, BGP is waiting for the TCP connection to be formed. If the TCP connection completes, BGP will move to the Open Sent stage; if the connection cannot complete, BGP goes to Active

3 – Active: In the Active state, the BGP speaker is attempting to initiate a TCP session with the BGP speaker it wants to peer with. If this can be done, the BGP state goes to Open Sent state.

4 – Open Sent: the BGP speaker is waiting to receive an OPEN message from the remote BGP speaker

5 – Open Confirm: Once the BGP speaker receives the OPEN message and no error is detected, the BGP speaker sends a KEEPALIVE message to the remote BGP speaker

6 – Established: All of the neighbor negotiations are complete. You will see a number, which tells us the number of prefixes the router has received from a neighbor or peer group.

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

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

Correct Answer: B

Explanation:

Encapsulated remote SPAN (ERSPAN): encapsulated Remote SPAN (ERSPAN), as the name says, brings generic routing encapsulation (GRE) for all captured traffic and allows it to be extended across Layer 3 domains.

Reference: <https://community.cisco.com/t5/networking-documents/understanding-span-rspan-and-erspan/ta-p/3144951>

98. 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.

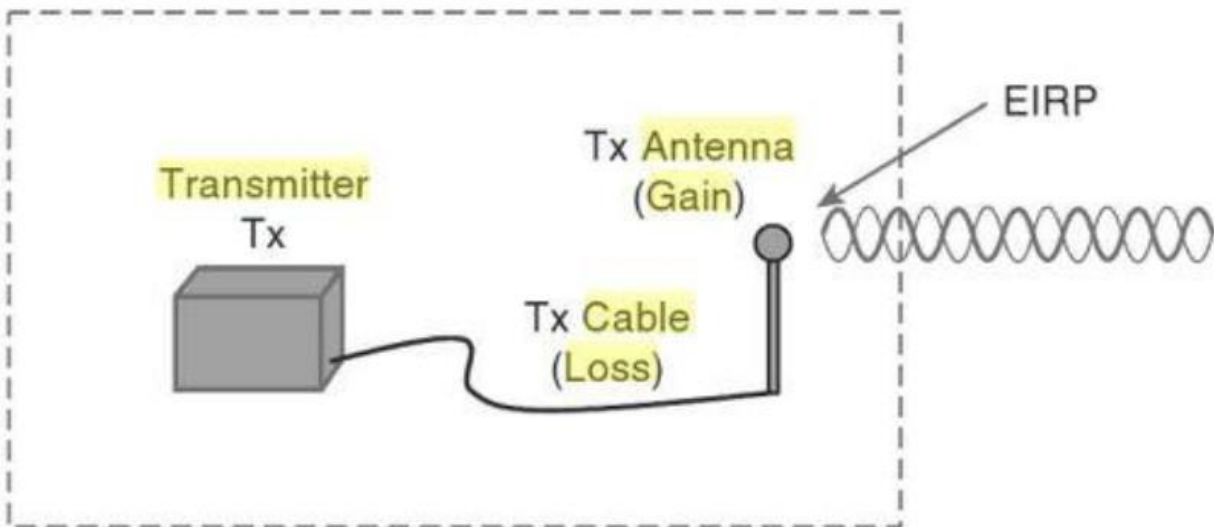
Correct Answer: AB

99. 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

Explanation: Once you know the complete combination of transmitter power level, the length of cable, and the antenna gain, you can figure out the actual power level that will be radiated from the antenna. This is known as the effective isotropic radiated power (EIRP), measured in dBm. EIRP is a very important parameter because it is regulated by governmental agencies in most countries. In those cases, a system cannot radiate signals higher than a maximum allowable EIRP. To find the EIRP of a system, simply add the transmitter power level to the antenna gain and subtract the cable loss.



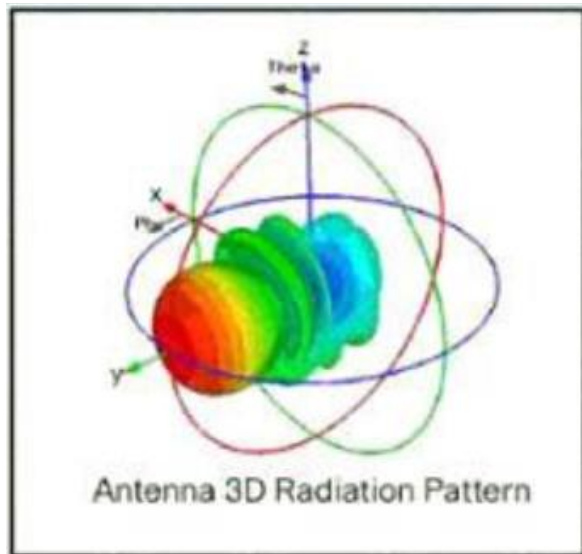
EIRP = Tx Power – Tx Cable + Tx Antenna

Suppose a transmitter is configured for a power level of 10 dBm (10 mW). answer 'SNR' cable with 5-dB loss connects the transmitter to an antenna with an 8-dBi gain. The resulting EIRP of the system is 10 dBm – 5 dB + 8 dBi, or 13 dBm.

You might notice that the EIRP is made up of decibel-milliwatt (dBm), dB relative to an isotropic antenna (dBi), and decibel (dB) values. Even though the units appear to be different, you can safely combine them because they are all in the dB “domain”.

Reference: CCNA Wireless 640-722 Official Cert Guide

100. Which type of antenna does the radiation pattern represent?



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

Correct Answer: A

Explanation:

A Yagi antenna is formed by driving a simple antenna, typically a dipole or dipolelike antenna, and shaping the beam using a well-chosen series of non-driven elements whose length and spacing are tightly controlled.



https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/prod_white_paper0900aecd806a1a3e.html

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
MD5 digest                  : 0xE5 0x28 0x5D 0x3E 0x2F 0xE5 0xAD 0x2B
Configuration last modified by 0.0.0.0 at 1-10-19 09:01:38

SwitchC#show vlan brief

```

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

```

[...output omitted...]

SwitchC#show int trunk

```

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

```

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

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

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

SwitchC#show run interface port-channel 1
interface Port-channel 1

```

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

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

Correct Answer: D

Explanation: From the “show vlan brief” we learn that Finance belongs to VLAN 110 and all VLANs (from 1 to 1005) are allowed to traverse the trunk (port-channel 1). Therefore we have to remove VLAN 110 from the allowed VLAN list with the “switchport trunk allowed vlan remove ” command. The pruning feature cannot do this job as Finance VLAN is active.

102. Refer to the exhibit. Which HTTP JSON response does the python code output give?

```

PYTHON CODE
import requests
import json

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

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

print(response['ins_api']['outputs'][output]['body']['kickstart_ver_str'])
=====
HTTP JSON Response:
{
    "ins_api": {
        "type": "cli_show",
        "version": "1.0",
        "sid": "eoc",
        "outputs": {
            "output": {
                "input": "show version",
                "msg": "Success",
                "code": "200",
                "body": {
                    "bios_ver_str": "07.61",
                    "kickstart_ver_str": "7.0(3)I7(4)",
                    "bios_cmpl_time": "04/08/2017",
                    "kick_file_name": "bootflash:///nxos.7.0.3.I7.4.bin",
                    "kick_cmpl_time": "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_ctime": "Sun Mar 10 15:41:46 2019",
                    "rr_reason": "Reset Requested by CLI command reload",
                    "rr_sys_ver": "7.0(3)I7(4)",
                    "rr_service": "",
                    "manufacturer": "Cisco Systems, Inc",
                    "TABLE_package_list": {
                        "ROW_package_list": {
                            "package_id": {}
                        }
                    }
                }
            }
        }
    }
}

```

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

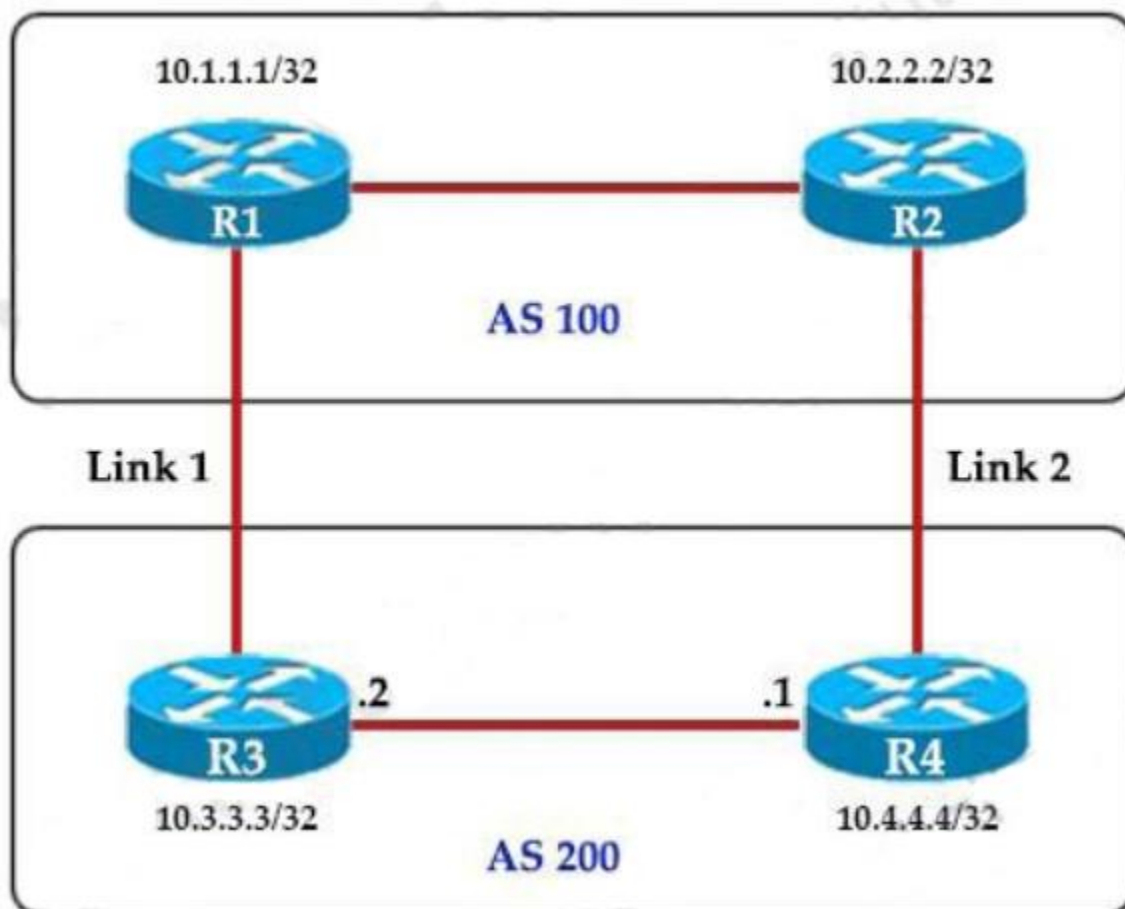
Correct Answer: D

103. 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

104. Refer to the exhibit.



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

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

Correct Answer: A

Explanation: Local preference is an indication to the AS about which path has preference to exit the AS in order to reach a certain network. A path with a higher local preference is preferred. The default value for local preference is 100.

Unlike the weight attribute, which is only relevant to the local router, local preference is an attribute that routers exchange in the same AS. The local preference is set with the “bgp default local-preference value” command.

In this case, both R3 & R4 have exit links but R4 has higher local-preference so R4 will be chosen as the preferred exit point from AS 200.

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

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

Correct Answer: C

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

106. 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_SSHpolice cir 100000
exceed-action drop
!!!
Interface GigabitEthernet0/1

```
ip address 209.165.200.225 255.255.255.0
ip access-group CoPP_SSH 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 ... 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
!
```

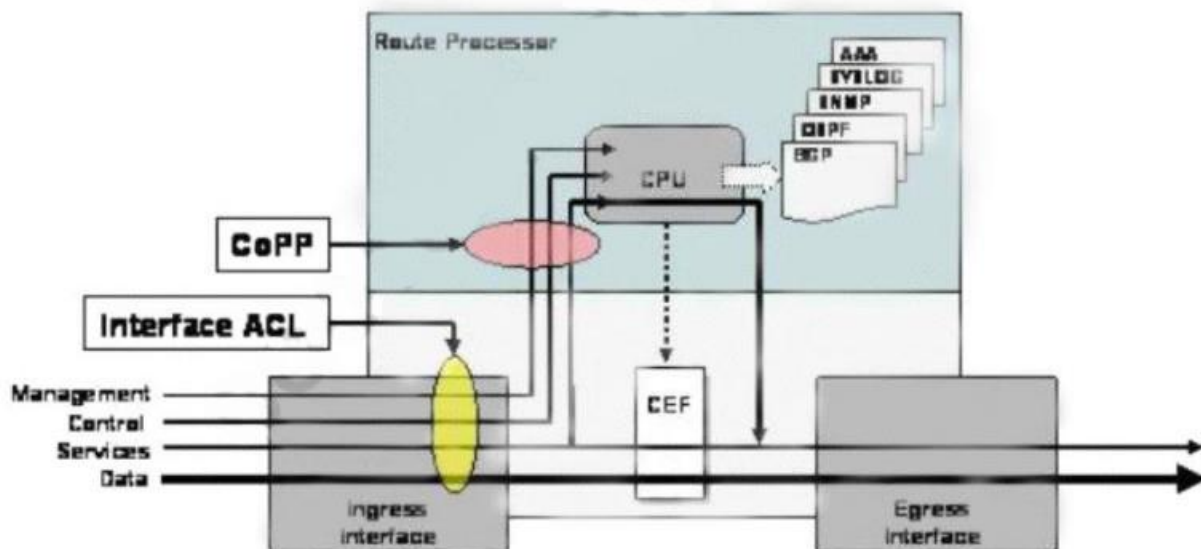
D.

```
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

Explanation: CoPP protects the route processor on network devices by treating route processor resources as a separate entity with its own ingress interface (and in some implementations, egress also). CoPP is used to police traffic that is destined to the route processor of the router such as:

- + routing protocols like OSPF, EIGRP, or BGP.
- + Gateway redundancy protocols like HSRP, VRRP, or GLBP.
- + Network management protocols like telnet, SSH, SNMP, or RADIUS.



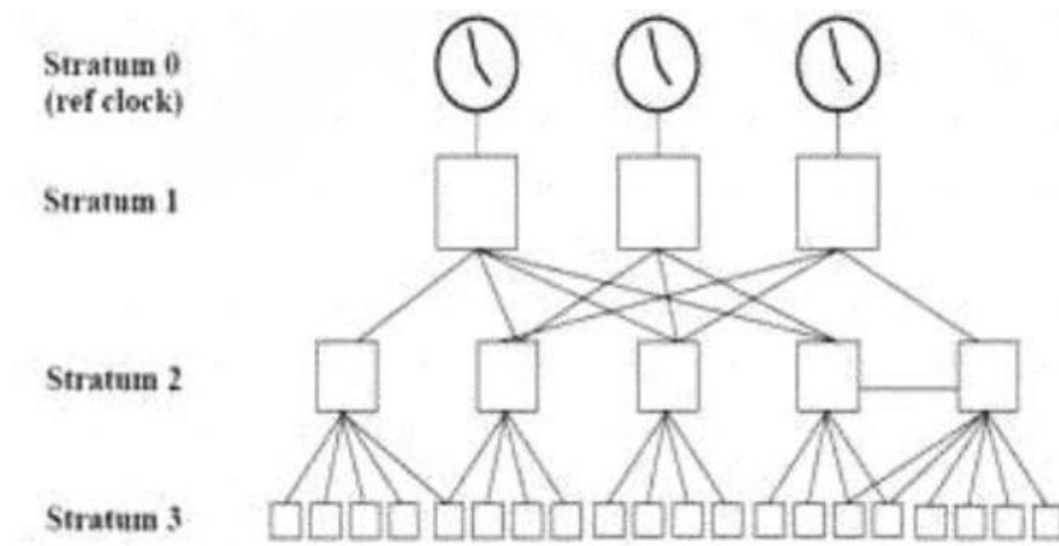
Therefore we must apply the CoPP to deal with SSH because it is in the management plane. CoPP must be put under “control-plane” command.

107. 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

Explanation: The stratum levels define the distance from the reference clock. A reference clock is a stratum 0 device that is assumed to be accurate and has little or no delay associated with it. Stratum 0 servers cannot be used on the network but they are directly connected to computers which then operate as stratum-1 servers. A stratum 1 time server acts as a primary network time standard.



A stratum 2 server is connected to the stratum 1 server; then a stratum 3 server is connected to the stratum 2 server and so on. A stratum 2 server gets its time via NTP packet requests from a stratum 1 server. A stratum 3 server gets its time via NTP packet requests from a stratum-2 server... A stratum server may also peer with other stratum servers at the same level to provide more stable and robust time for all devices in the peer group (for example a stratum 2 server can peer with other stratum 2 servers).

NTP uses the concept of a stratum to describe how many NTP hops away a machine is from an authoritative time source. A stratum 1 time server typically has an authoritative time source (such as a radio or atomic clock, or a Global Positioning System (GPS) time source) directly attached, a stratum 2 time server receives its time via NTP from a stratum 1 time server, and so on.

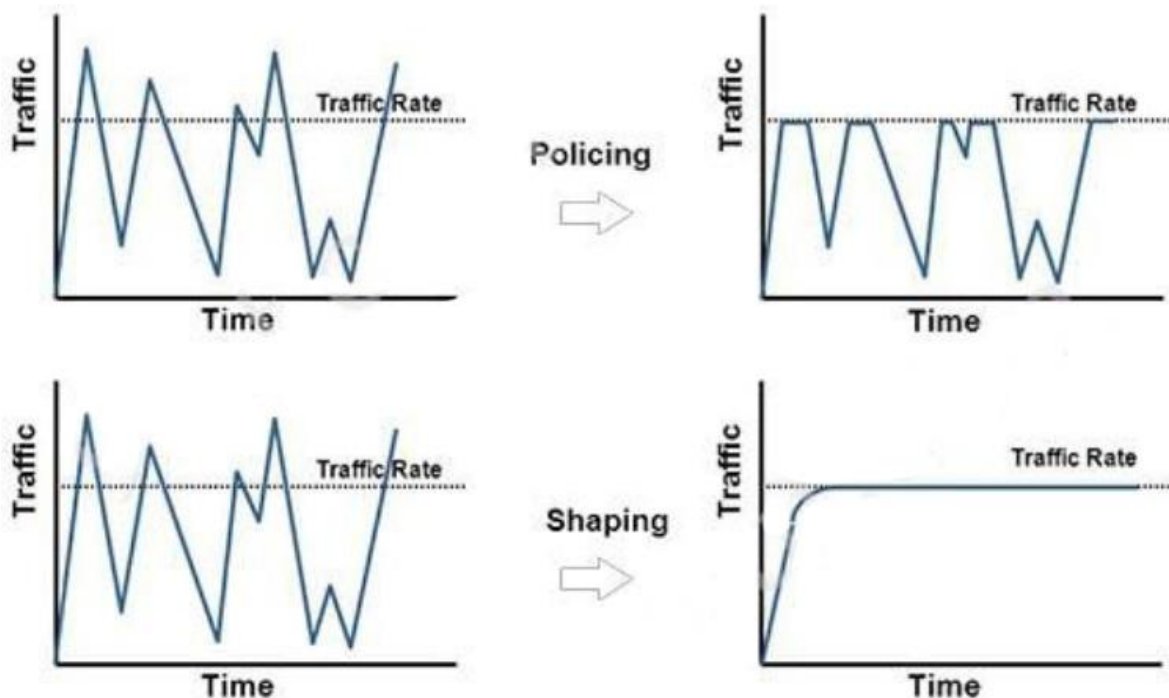
Reference: <https://www.cisco.com/c/en/us/td/docs/routers/asr920/configuration/guide/bsm/16-6-1/b-sm-xe-16-6-1-asr920/bsm-time-calendar-set.html>

108. How does QoS traffic shaping alleviate network congestion?

- A. It drops packets when traffic exceeds a certain bitrate.
- **B. It buffers and queue 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

Explanation: Traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time. The result of traffic shaping is a smoothed packet output rate.



109. An engineer is describing QoS to a client. Which two facts apply to traffic policing? (Choose two)

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

Correct Answer: CE

Explanation: Traffic policing propagates bursts. When the traffic rate reaches the configured maximum rate (or committed information rate), excess traffic is dropped (or remarked). The

result is an output rate that appears as a saw-tooth with crests and troughs.

Unlike traffic shaping, traffic policing does not cause delay.

Classification (which includes traffic policing, traffic shaping and queuing techniques) should take place at the network edge. It is recommended that classification occur as close to the source of the traffic as possible.

Also according to this [Cisco link](#), “policing traffic as close to the source as possible”.

110. 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

Explanation: PIM dense mode (PIM-DM) uses a push model to flood multicast traffic to every corner of the network. This push model is a brute-force method of delivering data to the receivers. This method would be efficient in certain deployments in which there are active receivers on every subnet in the network. PIM-DM initially floods multicast traffic throughout the network. Routers that have no downstream neighbors prune the unwanted traffic. This process repeats every 3 minutes.

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 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 an RP. The RP must be administratively configured in the network.

Answer C seems to be correct but it is not, PIM sparse mode uses sources (not receivers) to register with the RP. Sources register with the RP, and then data is forwarded down the shared tree to the receivers.

111. 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

Explanation: Locator ID Separation Protocol (LISP) is a network architecture and protocol that implements the use of two namespaces instead of a single IP address:

+ Endpoint identifiers (EIDs)—assigned to end hosts.

+ Routing locators (RLOCs)—assigned to devices (primarily routers) that make up the global

routing system.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xr-3s/irl-xr-3s-book/irl-overview.html

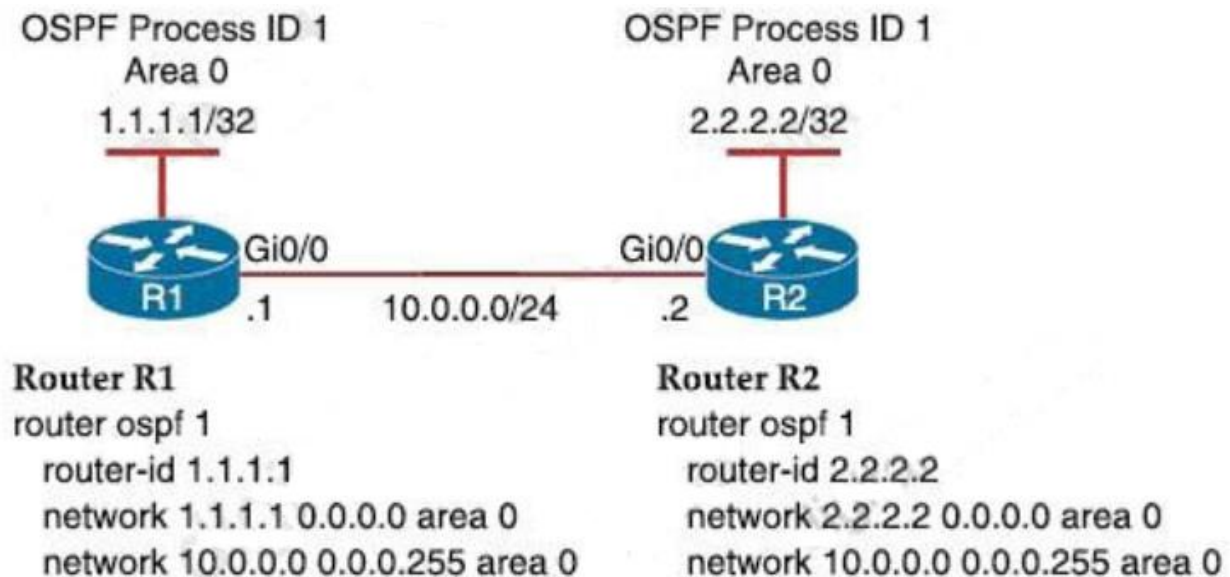
112. Which First Hop Redundancy Protocol should be used to meet a design requirements for more efficient default bandwidth usage across multiple devices?

- **A. GLBP**
- B. LCAP
- C. HSRP
- D. VRRP

Correct Answer: A

Explanation: The main disadvantage of HSRP and VRRP is that only one gateway is elected to be the active gateway and used to forward traffic whilst the rest are unused until the active one fails. Gateway Load Balancing Protocol (GLBP) is a Cisco proprietary protocol and performs the similar function to HSRP and VRRP but it supports load balancing among members in a GLBP group.

113. Refer to the exhibit.



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

- A. R1 (config-if) #interface Gi0/0
R1 (config-if) #ip ospf network point-to-point

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

B. R1 (config-if) #interface Gi0/0
R1 (config-if) #ip ospf network broadcast
R2(config-if)#interface Gi0/0
R2(config-if)#ip ospf network broadcast

C. R1(config-if)#interface Gi0/0
R1(config-if)#ip ospf database-filter all out
R2(config-if)#interface Gi0/0
R2(config-if)#ip ospf database-filter all out

D. R1(config-if)#interface Gi0/0
R1(config-if)#ip ospf priority 1
R2(config-if)#interface Gi0/0
R2(config-if)#ip ospf priority 1

Correct Answer: A

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

114. 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

Explanation: Broadcast radiation is the accumulation of broadcast and multicast traffic on a computer network.

Extreme amounts of broadcast traffic constitute a broadcast storm.

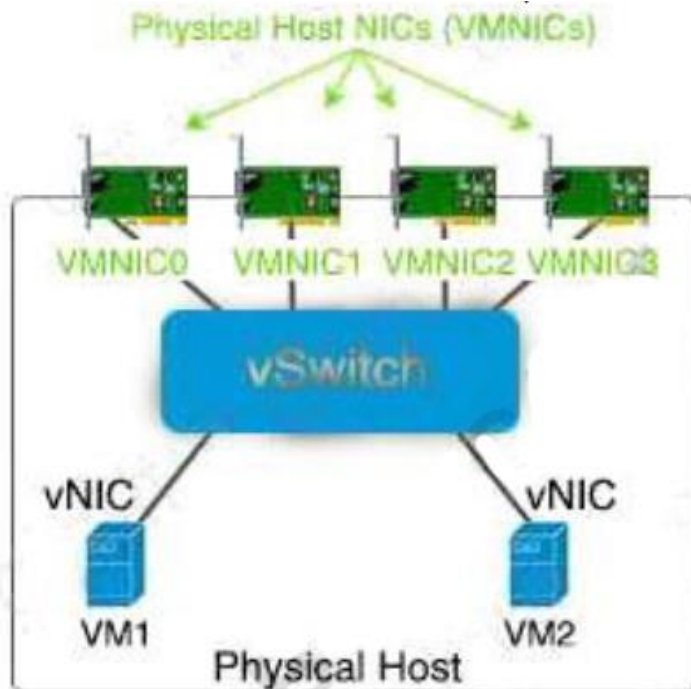
The amount of broadcast traffic you should see within a broadcast domain is directly proportional to the size of the broadcast domain. Therefore if the layer 2 domain in virtual machine environment is too large, broadcast radiation may occur -> VLANs should be used to reduce broadcast radiation.

Also if virtual machines communicate via broadcast too much, broadcast radiation may occur. Another reason for broadcast radiation is using a trunk (to extend VLANs) from the network switch to the physical server.

Note about the structure of virtualization in a hypervisor:

Hypervisors provide virtual switch (vSwitch) that Virtual Machines (VMs) use to communicate with other VMs on the same host. The vSwitch may also be connected to the host's physical NIC to allow VMs to get layer 2 access to the outside world.

Each VM is provided with a virtual NIC (vNIC) that is connected to the virtual switch. Multiple vNICs can connect to a single vSwitch, allowing VMs on a physical host to communicate with one another at layer 2 without having to go out to a physical switch.



Although vSwitch does not run Spanning-tree protocol but vSwitch implements other loop prevention mechanisms. For example, a frame that enters from one VMNIC is not going to go out of the physical host from a different VMNIC card.

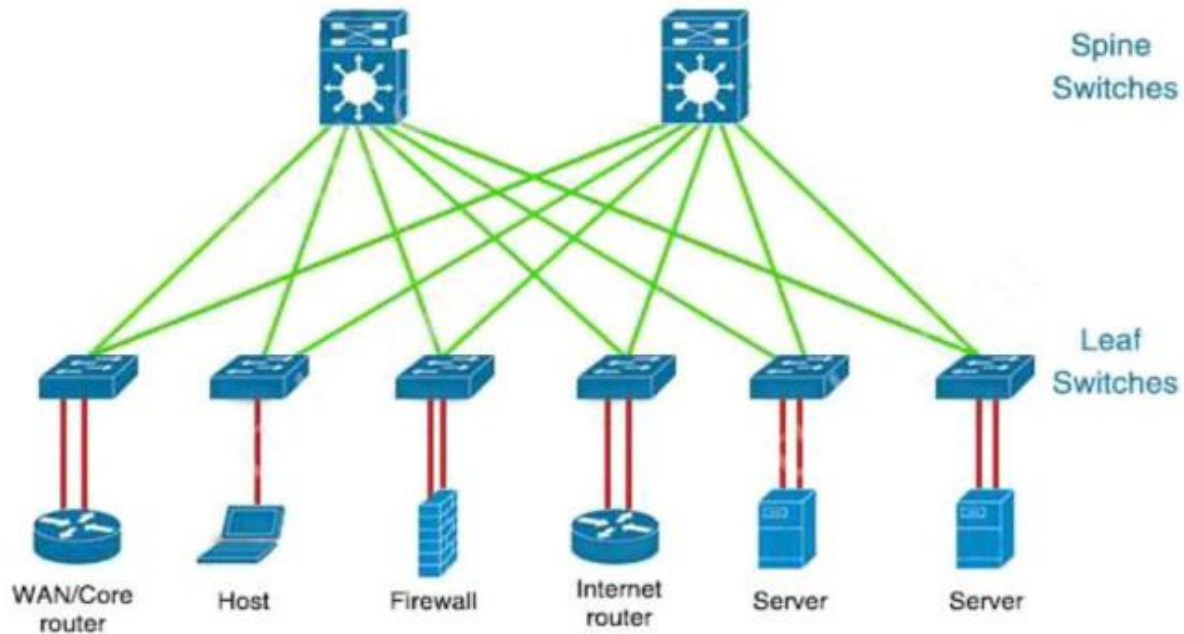
115. A company plans to implement intent-based networking in its campus infrastructure. Which design facilitates a migrate from a traditional campus design to a programmer fabric designer?

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

Correct Answer: C

Explanation: Intent-based Networking (IBN) transforms a hardware centric, manual network into a controller-led network that captures business intent and translates it into policies that can be automated and applied consistently across the network. The goal is for the network to continuously monitor and adjust network performance to help assure desired business outcomes.

IBN builds on software-defined networking (SDN). SDN usually uses spine-leaf architecture, which is typically deployed as two layers: spines (such as an aggregation layer), and leaves (such as an access layer).



116. 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

Explanation: A prerequisite for configuring Mobility Groups is “All controllers must be configured with the same virtual interface IP address”. If all the controllers within a mobility group are not using the same virtual interface, inter controller roaming may appear to work, but the handoff does not complete, and the client loses connectivity for a period of time. -> Answer B is correct.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/mobility_groups.html

117. 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

Explanation: One of the best practices to secure REST APIs is using password hash. Passwords must always be hashed to protect the system (or minimize the damage) even if it is compromised in some hacking attempts. There are many such hashing algorithms which can prove really effective for password security e.g. PBKDF2, bcrypt and scrypt algorithms.

Other ways to secure REST APIs are: Always use HTTPS, Never expose information on URLs (Usernames, passwords, session tokens, and API keys should not appear in the URL), Adding Timestamp in Request, Using OAuth, Input Parameter Validation.

Reference: <https://restfulapi.net/security-essentials/>

We should not use MD5 or any SHA (SHA-1, SHA-256, SHA-512...) algorithm to hash password as they are not totally secure.

Note: A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

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

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

Correct Answer: D

119. 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 client manager in prevent colleague making changes to the device 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

Explanation: The example below shows the usage of lock command:

```
def demo(host, user, names):  
    With manager. Connect(host=host, port=22, username=user) as m:  
        With m.locked(target='running'):  
            for n in names:  
                m.edit_config (target='running', config=template % n)
```

The command “m.locked (target='running')” causes a lock to be acquired on the running datastore.

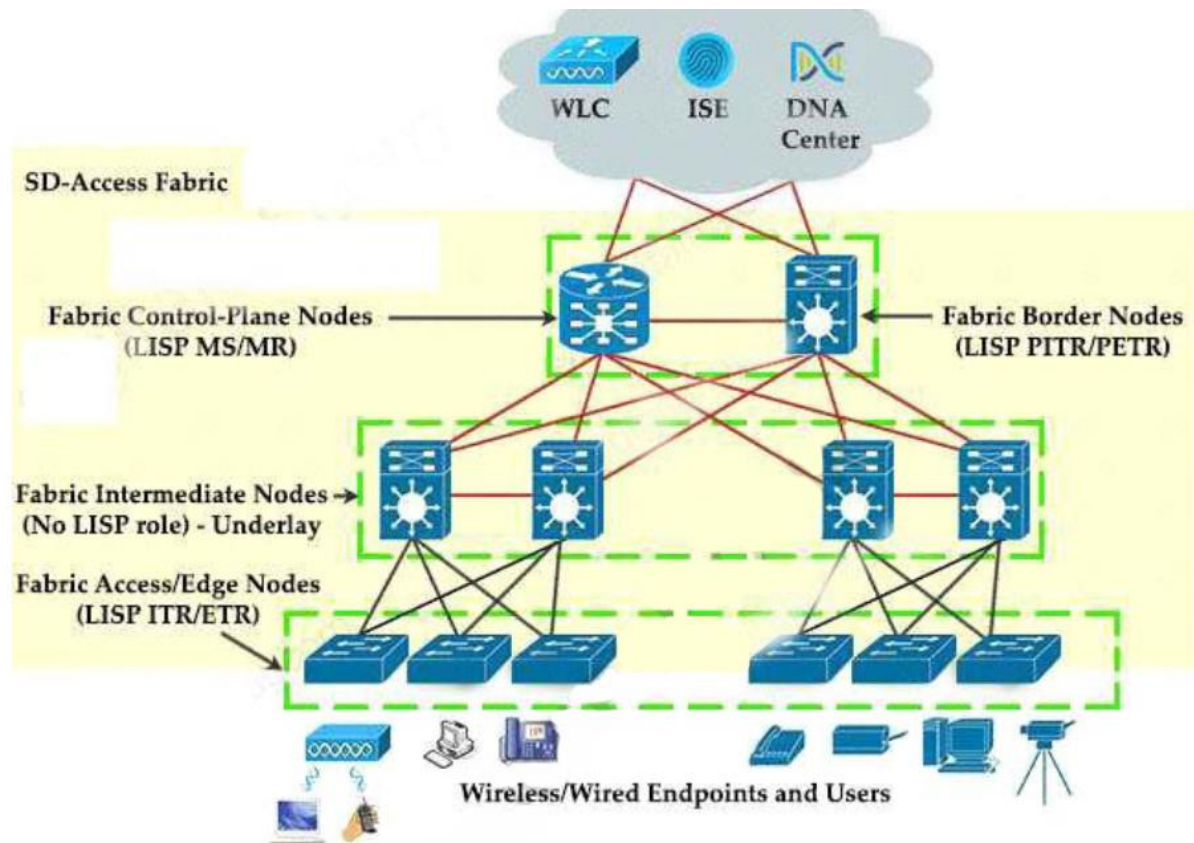
120. What are two device roles in Cisco SD-Access fabric? (Choose two)

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

Correct Answer: CE

Explanation: There are five basic device roles in the fabric overlay:

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

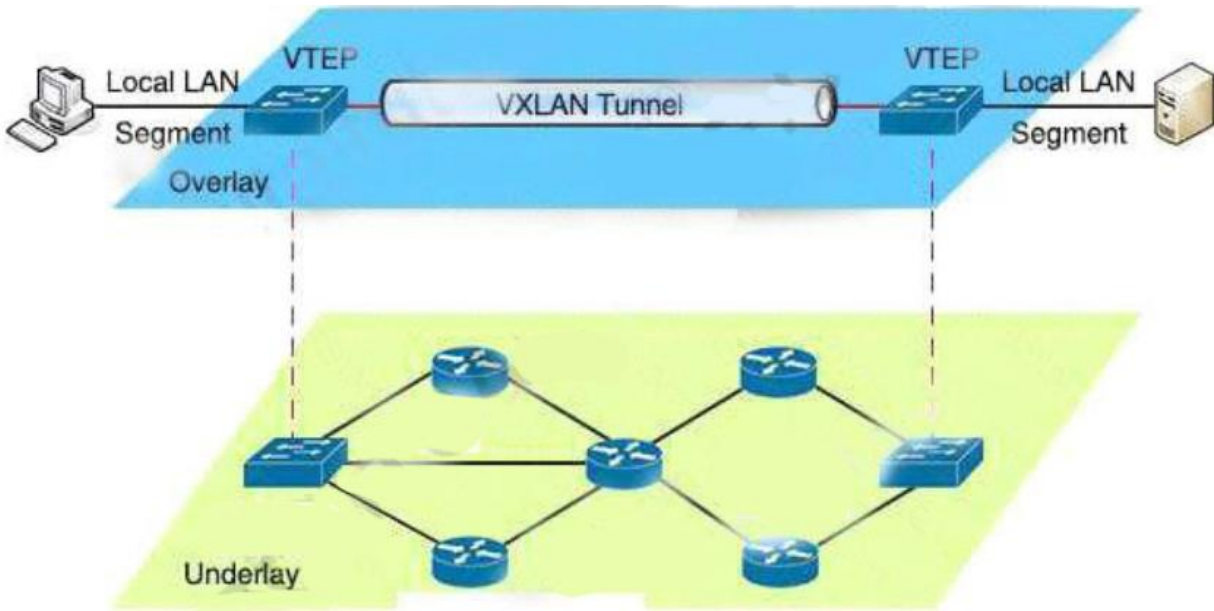


121. Which action is a function of VTEP in VXLAN?

- 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

Explanation: VTEPs connect between Overlay and Underlay network and they are responsible for encapsulating frame into VXLAN packets to send across IP network (Underlay) then decapsulating when the packets leaves the VXLAN tunnel.



122. 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

Explanation:

The Cisco DNA Center open platform for intent-based networking provides 360- degree extensibility across multiple components, including:

+ 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.

...

<https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-cent-plat-sol-over-cte-en.html>

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

- **A. vBond**
- B. vSmart
- C. vManage

- D. vEdge

Correct Answer: A

Explanation: + Orchestration plane (vBond) assists in securely onboarding the SD-WAN WAN Edge routers into the SD-WAN overlay. The vBond controller, or orchestrator, authenticates and authorizes the SD-WAN components onto the network. The vBond orchestrator takes an added responsibility to distribute the list of vSmart and vManage controller information to the WAN Edge routers. vBond is the only device in SD-WAN that requires a public IP address as it is the first point of contact and authentication for all SD-WAN components to join the SD-WAN fabric. All other components need to know the vBond IP or DNS information.

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

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

Correct Answer: BD

Explanation: A bare-metal hypervisor (Type 1) is a layer of software we install directly on top of a physical server and its underlying hardware. There is no software or any operating system in between, hence the name bare-metal hypervisor. A Type 1 hypervisor is proven in providing excellent performance and stability since it does not run inside Windows or any other operating system. These are the most common type 1 hypervisors:

- + VMware vSphere with ESX/ESXi
- + KVM (Kernel-Based Virtual Machine)
- + Microsoft Hyper-V
- + Oracle VM
- + Citrix Hypervisor (formerly known as Xen Server)

125. 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

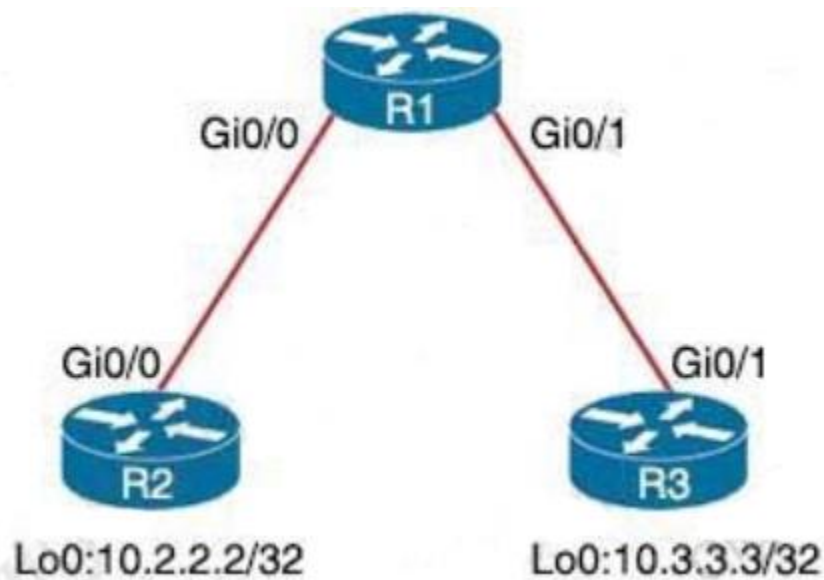
Correct Answer: C

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

connectivity degradation. To address these issues we have created Cisco's Wireless Service Assurance and a new AP mode called "sensor" mode. Cisco's Wireless Service Assurance platform has three components, namely, Wireless Performance Analytics, Real-time Client Troubleshooting, and Proactive Health Assessment. 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.

Reference: [Here](#)

126. 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.

```
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

Explanation: We cannot filter traffic that is originated from the local router (R3 in this case) so we can only configure the ACL on R1 or R2. “Weekend hours” means from Saturday morning through Sunday night so we have to configure: “periodic weekend 00:00 to 23:59”.

Note: The time is specified in 24-hour time (hh:mm), where the hours range from 0 to 23 and the minutes range from 0 to 59.

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

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

Correct Answer: B

Explanation: Cisco DNA Center provides an interactive editor called Template Editor to author CLI templates. Template Editor is a centralized CLI management tool to help design a set of device configurations that you need to build devices in a branch. When you have a site, office, or branch that uses a similar set of devices and configurations, you can use Template Editor to build generic configurations and apply the configurations to one or more devices in the branch.

[Reference](#)

128. A client device roams between access points located on different floors in an atrium. The access points joined to the same controller and configuration in local mode. The access points are in different IP addresses, but the client VLAN in the group same. What type of roam occurs?

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

Correct Answer: D

Explanation:

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

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

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

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

[Here](#)

129. What does the LAP send when multiple WLCs respond to the CISCO_CAPWAP-CONTROLLER.localdomain hostname during the CAPWAP discovery and join process?

- A. broadcast discover request
- B. join request to all the WLCs
- **C. unicast discovery request to each WLC**
- D. Unicast discovery request to the first WLC that resolves the domain name

Correct Answer: C

Explanation: 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.

Reference: [Here](#)

130. 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 233 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

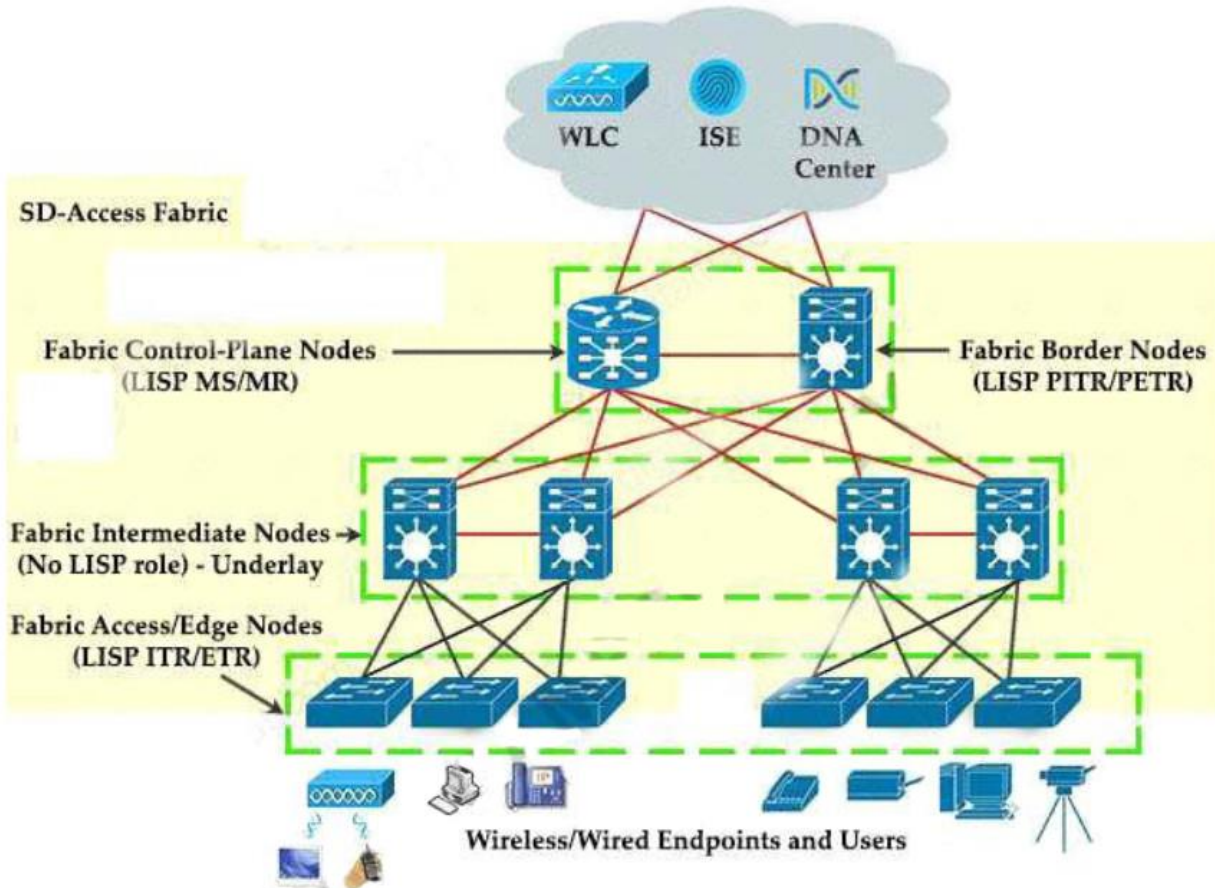
Correct Answer: A

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

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

Correct Answer: B

Explanation: + Fabric edge node: This fabric device (for example, access or distribution layer device) connects wired endpoints to the SDA fabric.



132. Refer to the exhibit.

```
access-list 1 permit 172.16.1.0 0.0.0.255
ip nat inside source list 1 interface gigabitethernet0/0 overload
```

The inside and outside interfaces in the NAT configuration of this device have been correctly identified. What is the effect of this configuration?

- A. dynamic NAT
- B. static NAT
- C. PAT
- D. NAT64

Correct Answer: C

Explanation: The command “ip nat inside source list 1 interface gigabitethernet0/0 overload” translates all source addresses that pass access list 1, which means 172.16.1.0/24 subnet, into an address assigned to gigabitethernet0/0 interface. Overload keyword allows to map multiple IP addresses to a single registered IP address (many-to-one) by using different ports so it is called Port Address Translation (PAT).

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

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

Correct Answer: B

Explanation:

The goal of the Cyber Threat Defense solution is to introduce a design and architecture that can help facilitate the discovery, containment, and remediation of threats once they have penetrated into the network interior.

Cisco Cyber Threat Defense version 2.0 makes use of several solutions to accomplish its objectives:

- * NetFlow and the Lancope StealthWatch System
 - Broad visibility
 - User and flow context analysis
 - Network behavior and anomaly detection
 - Incident response and network forensics
- * Cisco FirePOWER and FireSIGHT
 - Real-time threat management
 - Deeper contextual visibility for threats bypassing the perimeters
 - URL control
- * Advanced Malware Protection (AMP)
 - Endpoint control with AMP for Endpoints
 - Malware control with AMP for networks and content
- * Content Security Appliances and Services
 - Cisco Web Security Appliance (WSA) and Cloud Web Security (CWS)
 - Dynamic threat control for web traffic
 - Outbound URL analysis and data transfer controls
 - Detection of suspicious web activity
- Cisco Email Security Appliance (ESA)
 - Dynamic threat control for email traffic
 - Detection of suspicious email activity
- * Cisco Identity Services Engine (ISE)
 - User and device identity integration with Lancope StealthWatch
 - Remediation policy actions using pxGrid

https://www.cisco.com/c/dam/en/us/td/docs/security/network_security/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf

134. Which feature of EIGRP is not supported in OSPF?

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

Correct Answer: A

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

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

Correct Answer: A

Explanation: Ransomware are malicious software that locks up critical resources of the users. Ransomware uses well-established public/private key cryptography which leaves the only way of recovering the files being the payment of the ransom, or restoring files from backups.

Cisco Advanced Malware Protection (AMP) for Endpoints Malicious Activity Protection (MAP) engine defends your endpoints by monitoring the system and identifying processes that exhibit malicious activities when they execute and stops them from running. Because the MAP engine detects threats by observing the behavior of the process at run time, it can generically determine if a system is under attack by a new variant of ransomware or malware that may have eluded other security products and detection technology, such as legacy signature-based malware detection. The first release of the MAP engine targets identification, blocking, and quarantine of ransomware attacks on the endpoint.

Reference: <https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/white-paper-c11-740980.pdf>

136. 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

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

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

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

Correct Answer: A

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

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

Correct Answer: A

138. Wireless users report frequent disconnections from the wireless network. While troubleshooting a network engineer finds that after the user a disconnect, the connection reestablishes automatically without any input required. The engineer also notices these message logs.

Which action reduces the user impact?

```
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
```

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

Correct Answer: A

Explanation: These message logs inform that the radio channel has been reset (and the AP must be down briefly). With dynamic channel assignment (DCA), the radios can frequently switch from one channel to another but it also makes disruption. The default DCA interval is 10 minutes, which is matched with the time of the message logs. By increasing the DCA interval, we can reduce the number of times our users are disconnected for changing radio channels.

139. 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

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

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

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

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

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

Correct Answer: D

Explanation: The “aaa authentication login default local group tacacs+” command is broken down as follows:

- + The ‘aaa authentication’ part is simply saying we want to configure authentication settings.
- + The ‘login’ is stating that we want to prompt for a username/ password when a connection is made to the device.
- + The ‘default’ means we want to apply for all login connections (such as tty, vty, console and aux). If we use this keyword, we don’t need to configure anything else under tty, vty and aux lines. If we don’t use this keyword then we have to specify which line(s) we want to apply the authentication feature.
- + The ‘local group tacacs+’ means all users are authenticated using router’s local database (the first method). If the credentials are not found on the local database, then the TACACS+ server is used (the second method).

141. 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

Explanation: Control plane (vSmart) builds and maintains the network topology and make decisions on the traffic flows. The vSmart controller disseminates control plane information between WAN Edge devices, implements control plane policies and distributes data plane policies to network devices for enforcement.

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

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

Correct Answer: B

143. 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

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

Reference: [Here](#)

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

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

Correct Answer: B

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

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

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

145. 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 200
deny tcp host 10.10.10.1 eq 80 any
permit ip any any

B. ip access-list extended 10
deny tcp host 10.10.10.1 any eq 80
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 100
deny tcp host 10.10.10.1 any eq 80
permit ip any any

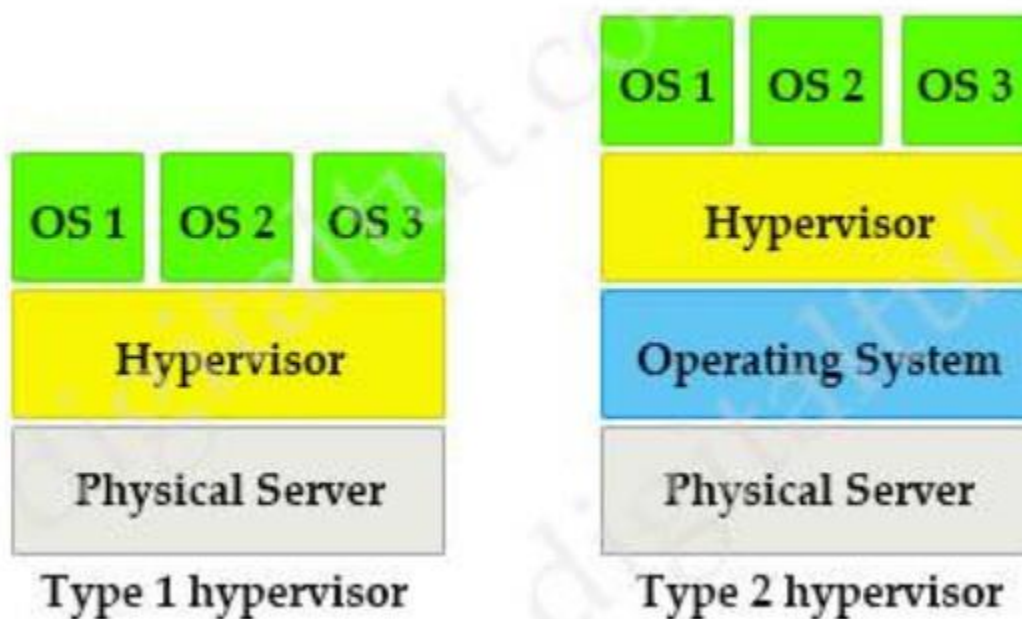
Correct Answer: D

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

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

Correct Answer: D

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



147. Refer to the exhibit. 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?

```
<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>
```

- 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: A

Explanation:

Accept and Content-type are both headers sent from a client (a browser) to a service. Accept header is a way for a client to specify the media type of the response content it is expecting and Contenttype is a way to specify the media type of request being sent from the client to the server. The response was sent in XML so we can say the Accept header sent was application/xml.

148. Which statement about LISP encapsulation in an EIGRP OTP implementation is true?

- A. LISP learns the next hop
- B. OTP uses LISP encapsulation to obtain routes from neighbors
- C. OTP uses LISP encapsulation for dynamic multipoint tunneling
- D. OTP maintains the LISP control plane

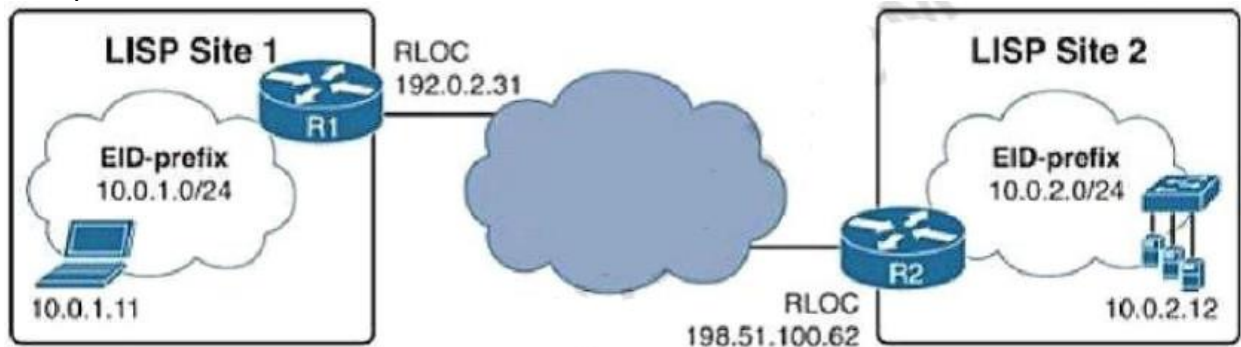
Correct Answer: C

Explanation: The EIGRP Over the Top solution can be used to ensure connectivity between disparate EIGRP sites.

This feature uses EIGRP on the control plane and Locator ID Separation Protocol (LISP) encapsulation on the data plane to route traffic across the underlying WAN architecture. EIGRP is used to distribute routes between customer edge (CE) devices within the network, and the traffic forwarded across the WAN architecture is LISP encapsulated.

EIGRP OTP only uses LISP for the data plane, EIGRP is still used for the control plane. Therefore we cannot say OTP uses LISP encapsulation for dynamic multipoint tunneling as this requires encapsulating both data and control plane traffic -> Answer 'OTP uses LISP encapsulation for dynamic multipoint tunneling' is not correct.

In OTP, EIGRP serves as the replacement for LISP control plane protocols (therefore EIGRP will learn the next hop, not LISP -> Answer 'LISP learns the next hop' is not correct). Instead of doing dynamic EID-to-RLOC mappings in native LISP-mapping services, EIGRP routers running OTP over a service provider cloud create targeted sessions, use the IP addresses provided by the service provider as RLOCs, and exchange routes as EIDs. Let's take an example:



If R1 and R2 ran OTP to each other, R1 would learn about the network 10.0.2.0/24 from R2 through EIGRP, treat the prefix 10.0.2.0/24 as an EID prefix, and take the advertising next hop 198.51.100.62 as the RLOC for this EID prefix. Similarly, R2 would learn from R1 about the network 10.0.1.0/24 through EIGRP, treat the prefix 10.0.1.0/24 as an EID prefix, and take the advertising next hop 192.0.2.31 as the RLOC for this EID prefix. On both routers, this information would be used to populate the LISP mapping tables. Whenever a packet from 10.0.1.0/24 to 10.0.2.0/24 would arrive at R1, it would use its LISP mapping tables just like in ordinary LISP to discover that the packet has to be LISP encapsulated and tunneled toward 198.51.100.62, and vice versa. The LISP data plane is reused in OTP and does not change; however, the native LISP mapping and resolving mechanisms are replaced by EIGRP.

149. Refer to the exhibit. Which command must be applied to R2 for an OSPF neighborship to form?



```

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

```

- A. network 20.1.1.2.0.0.0.0 area 0
- B. network 20.1.1.2 255.255.0.0. area 0
- C. network 20.1.1.2.0.0.255.255 area 0
- D. network 20.1.1.2 255.255.255 area 0

Correct Answer: A

Explanation: The network 20.0.0.0 0.0.0.255 area 0 command on R2 did not cover the IP address of Fa1/1 interface of R2 so OSPF did not run on this interface. Therefore we have to use the command “network 20.1.1.2 0.0.255.255 area 0” to turn on OSPF on this interface.

Note: The command “network 20.1.1.2 0.0.255.255 area 0” can be used too so this answer is also correct but answer C is the best answer here.

The network 0.0.0.0 255.255.255.255 area 0 command on R1 will run OSPF on all active interfaces of R1.

150. Which two statements about VRF-lite are true? (Choose two)

- A. It can support multiple customers on a single switch
- B. It supports most routing protocols, including EIGRP, ISIS, and OSPF
- C. It should be used when a customer’s router is connected to an ISP over OSPF
- D. It can increase the packet switching rate
- E. It supports MPLS-VRF label exchange and labeled packets

Correct Answer: AC

Explanation: VRF-lite does not support IGRP and ISIS.

•VRF-lite does not support all MPLS-VRF functionality: label exchange, LDP adjacency, or

labeled packets.

- VRF-lite does not affect the packet switching rate.
- The capability vrf-lite subcommand under router ospf should be used when configuring OSPF as the routing protocol between the PE and the CE.

Reference: [here](#)

151. How are the Cisco Express Forwarding table and the FIB related to each other?

- **A. Cisco Express Forwarding uses a FIB to make IP destination prefix-based switching decisions correct**
- B. The FIB is used to populate the Cisco Express Forwarding table
- C. There can be only one FIB but multiple Cisco Express Forwarding tables on IOS devices
- D. The Cisco Express Forwarding table allows route lookups to be forwarded to the route processor for processing before they are sent to the FIB

Correct Answer: A

Explanation: The Forwarding Information Base (FIB) table – CEF uses a FIB to make IP destination prefix based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and these changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table.

152. 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 1 monitors activity on VLAN 50 of a remote switch
- B. SPAN session 2 only monitors egress traffic exiting port FastEthernet 0/14.
- C. SPAN session 2 monitors all traffic entering and exiting port FastEthernet 0/15.
- **D. RSPAN session 1 is incompletely configured for monitoring**

Correct Answer: D

Explanation: SW1 has been configured with the following commands:

```
SW1(config)#monitor session 1 source remote vlan 50
SW1(config)#monitor session 2 source interface fa0/14
SW1(config)#monitor session 2 destination interface fa0/15
```

The session 1 on SW1 was configured for Remote SPAN (RSPAN) while session 2 was configured for local SPAN. For RSPAN we need to configure the destination port to complete the configuration.

Note: In fact we cannot create such a session like session 1 because if we only configure Source RSPAN VLAN 50 (with the command monitor session 1 source remote vlan 50) then we will receive a Type: Remote Source Session (not Remote Destination Session).

153. Which EIGRP feature allows the use of leak maps?

- A. neighbor
- **B. stub**
- C. offset-list
- D. address-family

Correct Answer: B

Explanation: If we configured an EIGRP stub router so that it only advertises connected and summary routes.

But we also want to have an exception to this rule then we can configure a leak-map. For example:

```
R4(config-if)#router eigrp 1
R4(config-router)#eigrp stub
R4(config)#ip access-list standard R4_L0opback0
R4(config-std-nacl)#permit host 4.4.4.4
R4(config)#route-map R4_L0opback0_LEAKMAP
R4(config-route-map)#match ip address R4_L0opback0
R4(config)#router eigrp 1
R4(config-router)#eigrp stub leak-map
```

As we can see the leak-map feature goes long with 'eigrp stub' command.

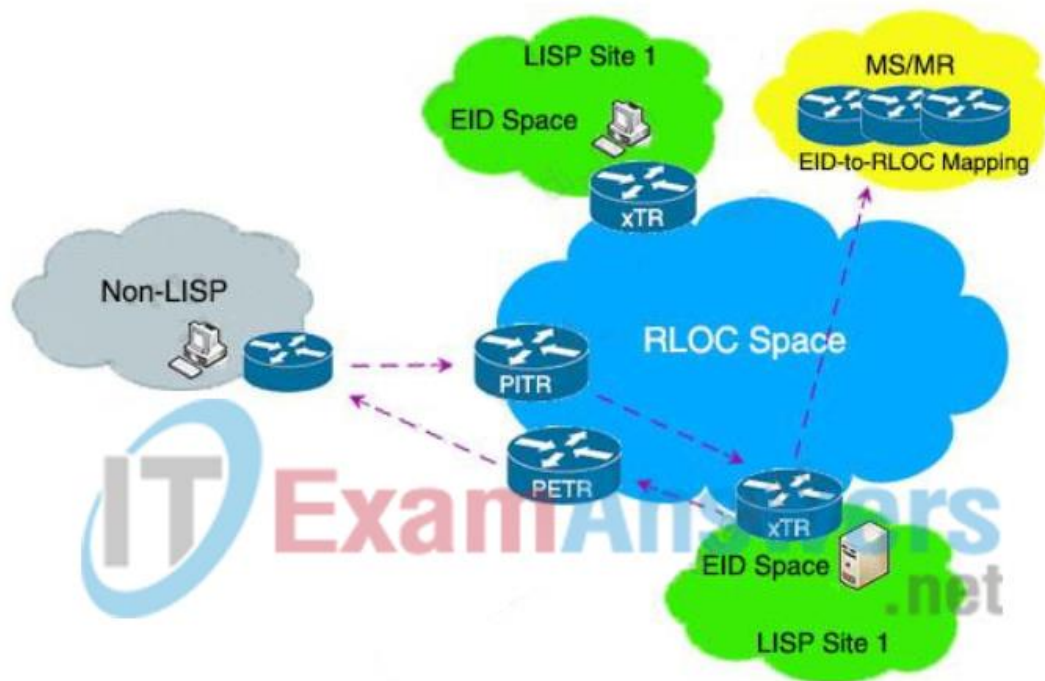
154. Which two LISP infrastructure elements are needed to support LISP to non-LISP internetworking? (Choose two)

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

Correct Answer: AC

Explanation: In this question we suppose that we only need to send packets from LISP site to non-LISP site successfully. We don't care about the way back (if we care about the way back then all PETR, PITR, MS & MR are needed).

Proxy Egress Tunnel Router (PETR): A LISP device that de-encapsulates packets from LISP sites to deliver them to non-LISP sites.



When the xTR in LISP Site 1 want to sends traffic to Non-LISP site, the ITR (not PETR) needs a Map Resolver (MR) to send Map Request to. When the ITR (the xTR in LISP Site 1 in the figure above) receives negative MAP-Reply packet from MR, it caches that prefix and map it to the PETR.

Good reference: [Here](#)

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

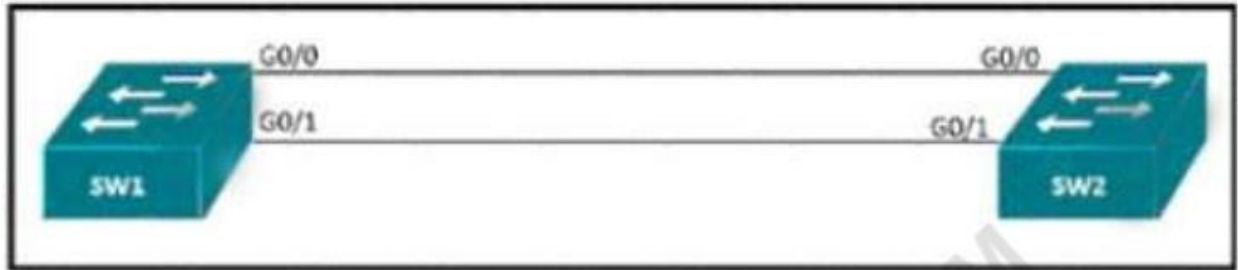
- A. dBi
- B. EIRP

- C. mW
- D. dBm

Correct Answer: C

Explanation: Output power is measured in mW (milliwatts). answer 'dBm' milliwatt is equal to one thousandth (103) of a watt.

156. Refer to the exhibit.



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

```
%PM-SP-4-ERR_DISABLE: bpduguard error detected on Gi0/0, putting Gi0/0 in errdisable state.
```

Which command set resolves this error?

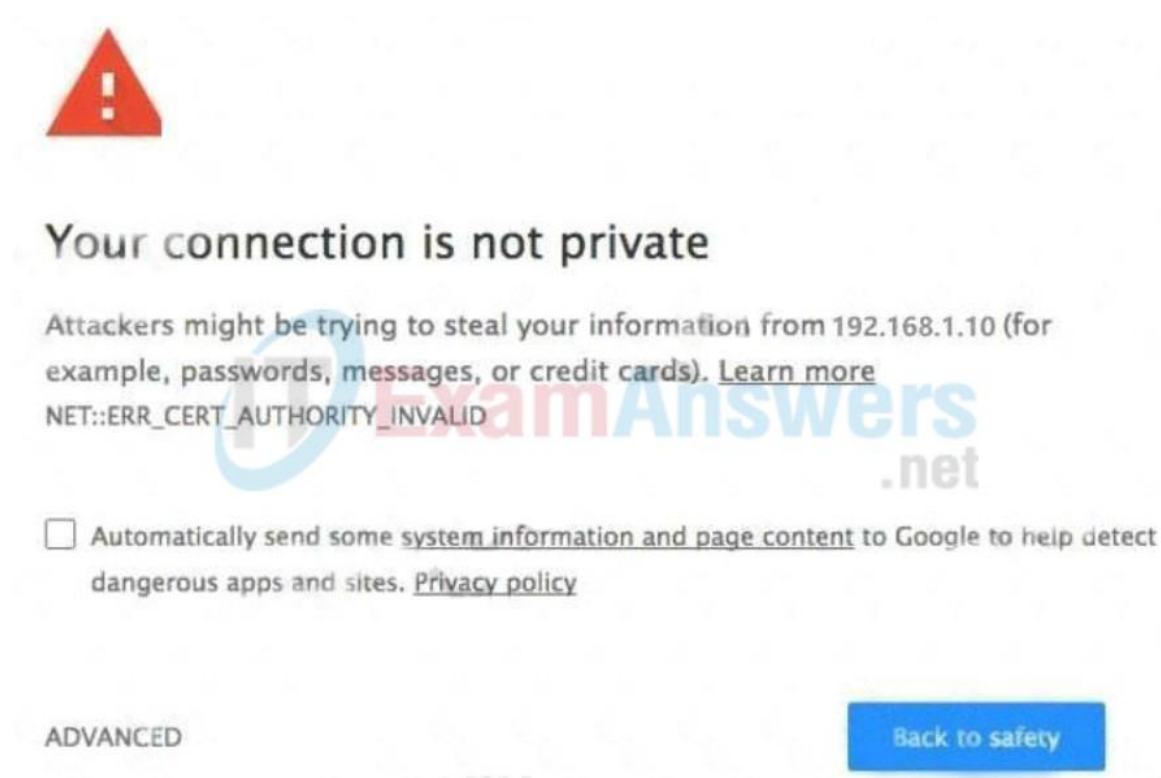
- A.
 Sw1(config)# interface G0/0
 Sw1(config-if)# spanning-tree bpduguard enable
 Sw1(config-if)# shut
 Sw1(config-if)# no shut
- B.
 Sw1(config)# interface G0/0
 Sw1(config-if)# no spanning-tree bpduguard enable
 Sw1(config-if)# shut
 Sw1(config-if)# no shut
- C.
 Sw1(config)# interface G0/1
 Sw1(config-if)# spanning-tree bpduguard enable
 Sw1(config-if)# shut
 Sw1(config-if)# no shut
- D.
 Sw1(config)# interface G0/0

```
Sw1(config-if)# no spanning-tree bpdupfilter
Sw1(config-if)# shut
Sw1(config-if)# no shut
```

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

Correct Answer: B

157. Refer to the exhibit.



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

Explanation: If you're a website owner and your website displays this error message, then there could be two reasons why the browser says the cert authority is invalid: + You're using a self-signed SSL certificate, OR + The certificate authority (CA) that issued your SSL certificate isn't trusted by your web browser.

158. Refer to the exhibit.

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

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

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

Correct Answer: C

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

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

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

Correct Answer: C

Explanation: From the “Tunnel protocol/transport GRE/IP” line, we can deduce this tunnel is using the default IPv4 Layer-3 tunnel mode. We can return to this default mode with the `tunnel mode gre ip` command.

160. What is the result of applying this access control list?

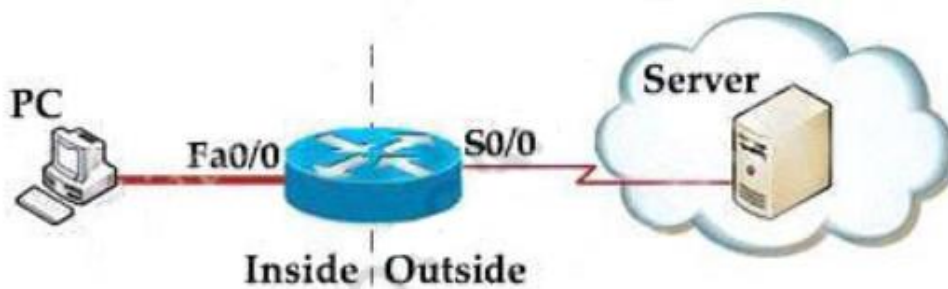
```
ip access-list extended STATEFUL
10 permit tcp any any established
20 deny ip any any
```

- 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

Explanation: The **established** keyword is only applicable to TCP access list entries to match TCP segments that have the ACK and/or RST control bit set (regardless of the source and

destination ports), which assumes that a TCP connection has already been established in one direction only. Let's see an example below:



Suppose you only want to allow the hosts inside your company to telnet to an outside server but not vice versa, you can simply use an “established” access-list like this:

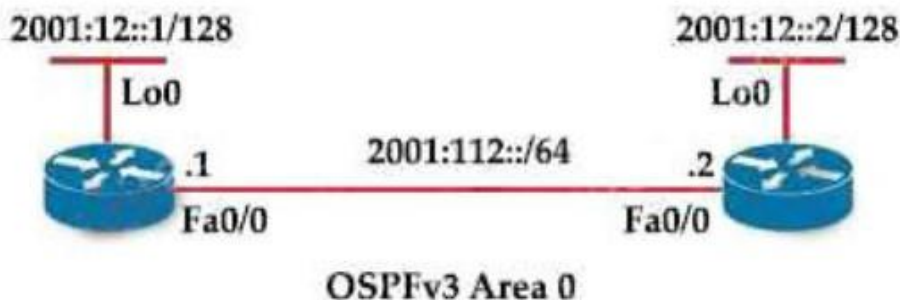
```
access-list 100 permit tcp any any established
access-list 101 permit tcp any any eq telnet
!
interface S0/0
ip access-group 100 in
ip access-group 101 out
```

161. 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 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: C

162. Refer to the exhibit. Which IPv6 OSPF network type is applied to interface Fa0/0 of R2 by default?

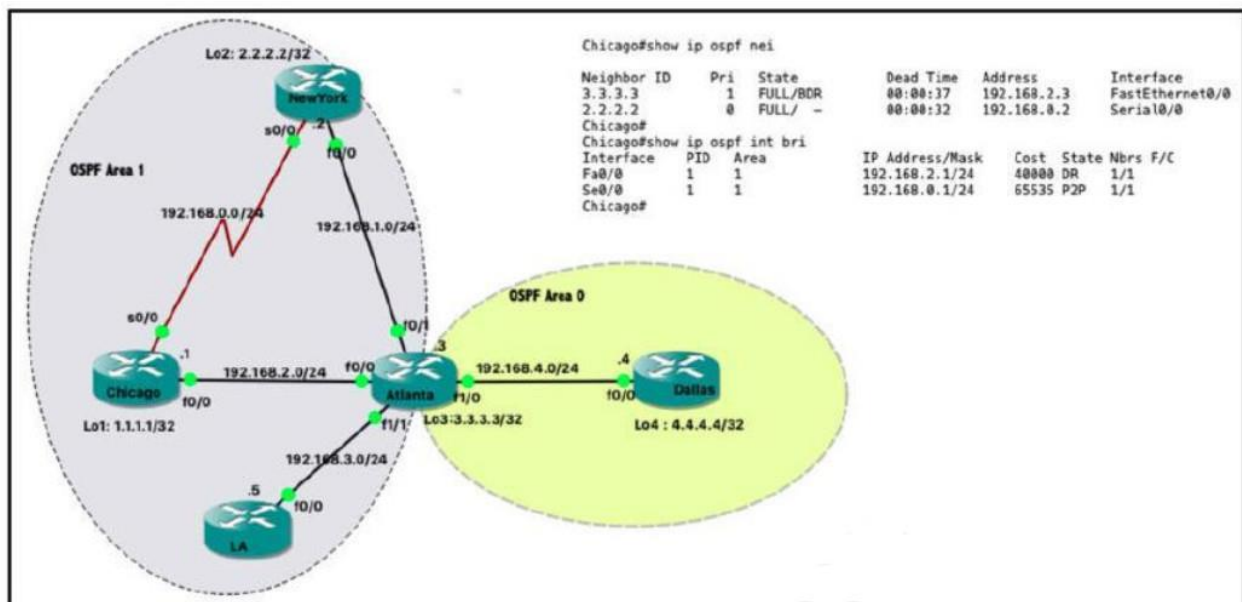


- A. multipoint
- **B. broadcast**
- C. Ethernet
- D. point-to-point

Correct Answer: B

Explanation: The Broadcast network type is the default for an OSPF enabled ethernet interface (while Point-toPoint is the default OSPF network type for Serial interface with HDLC and PPP encapsulation).

163. Refer the exhibit. 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

164. 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

Explanation: Cisco IOS software basically supports two modes of CEF load balancing: On per-destination or perpacket basis.

For per destination load balancing a hash is computed out of the source and destination IP address (-> Answer 'It combines the source and destination IP addresses to create a hash for each destination' is correct). This hash points to exactly one of the adjacency entries in the adjacency table (-> Answer 'Each hash maps directly to a single entry in the adjacency table' is correct), providing that the same path is used for all packets with this source/destination address pair. If per packet load balancing is used the packets are distributed round robin over the available paths. In either case the information in the FIB and adjacency tables provide all the necessary forwarding information, just like for nonload balancing operation.

The number of paths used is limited by the number of entries the routing protocol puts in the routing table, the default in IOS is 4 entries for most IP routing protocols with the exception of BGP, where it is one entry. The maximum number that can be configured is 6 different paths -> Answer 'Cisco Express Forwarding can load-balance over a maximum of two destinations' is not correct.

165. What is the main function of VRF-lite?

- A. To connect different autonomous systems together to share routes
- B. To allow devices to use labels to make Layer 2 Path decisions
- C. To route IPv6 traffic across an IPv4 backbone
- **D. To segregate multiple routing tables on a single device**

Correct Answer: D

166. 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

Explanation: The southbound protocol used by APIC is OpFlex that is pushed by Cisco as the protocol for policy enablement across physical and virtual switches.

Southbound interfaces are implemented with some called Service Abstraction Layer (SAL), which talks to the network elements via SNMP and CLI.

Note: Cisco OpFlex is a southbound protocol in a software-defined network (SDN).

167. An engineer reviews a router's logs and discovers the following entry. What is the event's logging severity level?

Router# *Feb 03 11:13:44 334: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up

- A. notification
- **B. error**
- C. informational
- D. warning

Correct Answer: B

Explanation: Syslog levels are listed below:

Level	Keyword	Description
0	emergencies	System is unusable
1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist
6	informational	Informational messages
7	debugging	Debugging messages

Number 3 in %LINK-3-UPDOWN is the severity level of this message so in this case it is errors.

168. Which characteristic distinguishes Ansible from Chef?

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

Correct Answer: C

Explanation: Ansible works by connecting to your nodes and pushing out small programs, called “Ansible modules” to them. These programs are written to be resource models of the desired state of the system. Ansible then executes these modules (over SSH by default), and removes them when finished.

Chef is a much older, mature solution to configure management. Unlike Ansible, it does require an installation of an agent on each server, named chef-client. Also, unlike Ansible, it has a Chef server that each client pulls configuration from.

169. 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

170. 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/forwarding
- C. easy virtual network
- **D. overlay network**

Correct Answer: D

Explanation: An overlay network creates a logical topology used to virtually connect devices that are built over an arbitrary physical underlay topology.

An overlay network is created on top of the underlay network through virtualization (virtual networks). The data plane traffic and control plane signaling are contained within each virtualized network, maintaining isolation among the networks and an independence from the underlay network.

SD-Access allows for the extension of Layer 2 and Layer 3 connectivity across the overlay through the services provided by through LISP.

Reference: [Click here](#)

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



```
R1(config)# ip nat inside source static 10.70.5.1 10.45.1.7
```

A.

```
R1(config)#interface GigabitEthernet0/0
```

```
R1(config)#ip nat outside
```

```
R1(config)#interface GigabitEthernet0/1
```

```
R1(config)#ip nat inside
```

B.

```
R1(config)#interface GigabitEthernet0/0
```

```
R1(config)#ip nat outside
```

```
R1(config)#interface GigabitEthernet0/1
```

```
R1(config)#ip nat inside
```

C.

```
R1(config)#interface GigabitEthernet0/0
```

```
R1(config)#ip nat inside
```

```
R1(config)#interface GigabitEthernet0/1
```

```
R1(config)#ip nat outside
```

D.

```
R1(config)#interface GigabitEthernet0/0
```

```
R1(config)#ip nat inside
```

```
R1(config)#interface GigabitEthernet0/1
```

```
R1(config)#ip nat outside
```

Correct Answer: B

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

```
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
```

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

Correct Answer: A

173. 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
key chain cisco123
key 1
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

```

```

R2
key chain cisco123
key 1
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

```

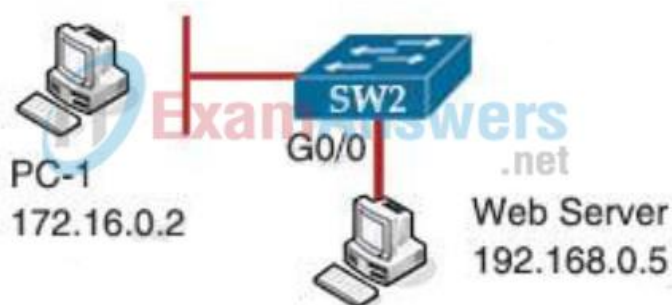
- A. HSRPv1
- B. GLBP
- C. VRRP
- D. HSRPv2

Correct Answer: A

Explanation: The “virtual MAC address” is 0000.0c07.acXX (XX is the hexadecimal group number) so it is using HSRPv1.

Note: HSRP Version 2 uses a new MAC address which ranges from 0000.0C9F.F000 to 0000.0C9F.FFFF.

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



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

Correct Answer: C

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

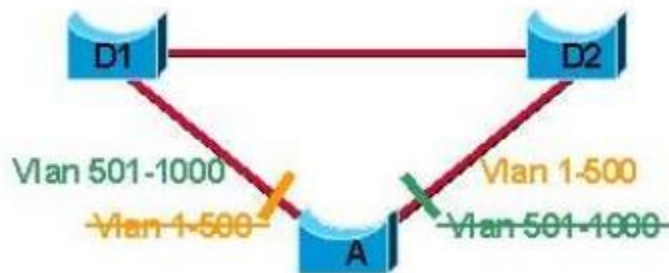
175. What would be the preferred way to implement a loopless switch network where there are 1500 defined VLANs and it is necessary to load the shared traffic through two main aggregation points based on the VLAN identifier?

- A. 802.1D
- **B. 802.1s**
- C. 802.1W
- D. 802.1AE

Correct Answer: B

Explanation: Where to Use MST

This diagram shows a common design that features access Switch A with 1000 VLANs redundantly connected to two distribution Switches, D1 and D2. In this setup, users connect to Switch A, and the network administrator typically seeks to achieve load balancing on the access switch Uplinks based on even or odd VLANs, or any other scheme deemed appropriate.



176. 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: D

Explanation: replacing the process of manual configuration. Data models are written in a standard, industry-defined language. Although configurations using CLIs are easier (more human-friendly), automating the configuration using data models results in scalability.

177. 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

178. Refer to the exhibit.

```
(WLC) >show interface summary
Interface Name          Vlan Id
-----
deadnet                 999
users1                  14
users2                  15
users3                  16

(WLC) >show wlan 1
WLAN Identifier . . . . . 1
Network Name (SSID) . . . . . wlan1
AAA Policy Override . . . . . Enabled
Interface . . . . . deadnet
FlexConnect Local Switching . . . . . Enabled
FlexConnect Central Association . . . . . Disabled
flexconnect Central Dhcp Flag . . . . . Disabled
flexconnect nat-pat Flag . . . . . Disabled
flexconnect DNS Override Flag . . . . . Disabled
flexconnect PPPoE pass-through . . . . . Disabled
flexconnect local-switching IP-source-guar . . . . . Disabled
FlexConnect Vlan based Central Switching . . . . . Enabled
FlexConnect Local Authentication . . . . . Disabled
FlexConnect Learn IP Address . . . . . Enabled

(WLC) >show ap config general FlexAP1
AP Mode . . . . . FlexConnect
FlexConnect Vlan mode : . . . . . Enabled
Native ID : . . . . . 1
WLAN 1 : . . . . . 10 (AP-Specific)
FlexConnect VLAN ACL Mappings
Vlan : . . . . . 10
Ingress ACL : . . . . . None
Egress ACL : . . . . . None
VLAN with least priority : . . . . . 13
FlexConnect Group . . . . . flexgroup1
Group VLAN ACL Mappings
Vlan : . . . . . 11
Ingress ACL : . . . . . None
Egress ACL : . . . . . None
Vlan : . . . . . 12
```

A wireless client is connecting to FlexAP1 which is currently working standalone mode. The AAA authentication process is returning the following AVPs:

```
Tunnel-Private-Group-Id(81): 15
Tunnel-Medium-Type(65): IEEE-802(6)
Tunnel-Type(64): VLAN(13)
```

Which three behaviors will the client experience? (Choose three.)

- A. While the AP is in standalone mode, the client will be placed in VLAN 15.
- **B. While the AP is in standalone mode, the client will be placed in VLAN 10.**
- C. When the AP transitions to connected mode, the client will be de-authenticated.
- D. While the AP is in standalone mode, the client will be placed in VLAN 13.
- E. When the AP is in connected mode, the client will be placed in VLAN 13.
- **F. When the AP transitions to connected mode, the client will remain associated.**
- **G. When the AP is in connected mode, the client will be placed in VLAN 15.**
- H. When the AP is in connected mode, the client will be placed in VLAN 10.

Correct Answer: BFG

179. 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

Explanation: Locator ID Separation Protocol (LISP) is a network architecture and protocol that implements the use of two namespaces instead of a single IP address:

+ Endpoint identifiers (EIDs) – assigned to end hosts.

+ Routing locators (RLOCs) – assigned to devices (primarily routers) that make up the global routing system.

180. Which variable in an EEM applet is set when you use the sync yes option?

- A. \$_cli_result
- **B. \$_exit_status**
- C. \$_string_result
- D. \$_result

Correct Answer: B

Explanation: With Synchronous (sync yes), the CLI command in question is not executed until the policy exits.

Whether or not the command runs depends on the value for the variable _exit_status.

If _exit_status is 1, the command runs, if it is 0, the command is skipped.

181. 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?

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

Option A

```
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
```

Option B

```
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
```

Option C

```
interface Vlan10
 no ip vrf forwarding Clients
!
interface Vlan20
```

```
no ip vrf forwarding Servers
!  
interface Vlan30  
no ip vrf forwarding Printers
```

Option D

```
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
```

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

Correct Answer: D

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

182. 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

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

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

- A. SIP flow information
- B. Wi-Fi multimedia

- C. traffic specification
- D. VoIP media session awareness

Correct Answer: C

184. Which data modeling language is commonly used by NETCONF?

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

Correct Answer: B

Explanation: Cisco IOS XE supports the Yet Another Next Generation (YANG) data modeling language. YANG can be used with the Network Configuration Protocol (NETCONF) to provide the desired solution of automated and programmable network operations. NETCONF(RFC6241) is an XML-based protocol that client applications use to request information from and make configuration changes to the device. YANG is primarily used to model the configuration and state data used by NETCONF operations.

185. Refer to the exhibit. Which two commands ensure that DSW1 becomes root bridge for VLAN 10 and 20?

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

```
DSW1#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 -----
```

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

Correct Answer: BE

Explanation: Priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

From the second command output (show spanning-tree mst) we learn that MST1 includes VLANs 10 & 20. Therefore if we want DSW1 to become root bridge for these VLANs we need

to set the MST 1 region to root ->The command “spanning-tree mst 1 root primary” can do the trick. In fact, this command runs a macro and sets the priority lower than the current root.

Also we can see the current root bridge for these VLANs has the priority of 32769 (default value + sysid) so we can set the priority of DSW1 to a specific lower value. But notice that the priority must be a multiple of 4096.

186. 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 of 26

Correct Answer: A

Explanation: CoS value 5 is commonly used for VOIP and CoS value 5 should be mapped to DSCP 46. DSCP 46 is defined as being for EF (Expedited Forwarding) traffic flows and is the value usually assigned to all interactive voice and video traffic. This is to keep the uniformity from end-to-end that DSCP EF (mostly for VOICE RTP) is mapped to COS 5.

Note:

+ CoS is a L2 marking contained within an 802.1q tag,. The values for CoS are 0 – 7

+ DSCP is a L3 marking and has values 0 – 63

+ The default DSCP-to-CoS mapping for CoS 5 is DSCP 40

187. 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 correct
- E. It uses active traffic monitoring correct
- F. SNMP access is not supported

Correct Answer: DE

Explanation: IP SLAs allows Cisco customers to analyze IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce the frequency of network outages. IP SLAs uses active traffic monitoring-the generation of traffic in a continuous, reliable, and predictable manner-for measuring network performance.

Being Layer-2 transport independent, IP SLAs can be configured end-to-end over disparate networks to best reflect the metrics that an end-user is likely to experience.

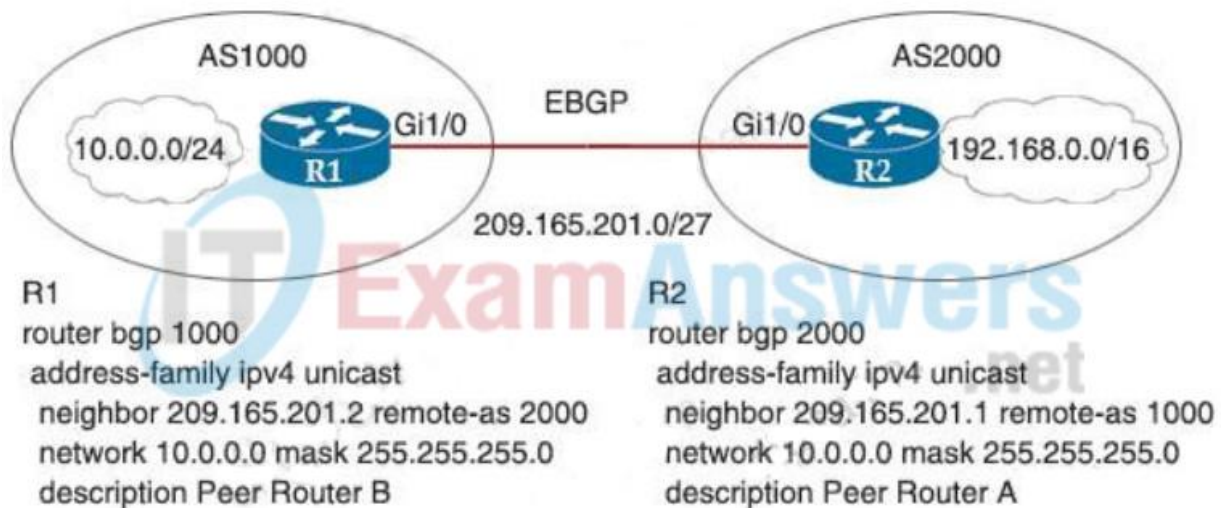
Reference: [Here](#)

188. 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

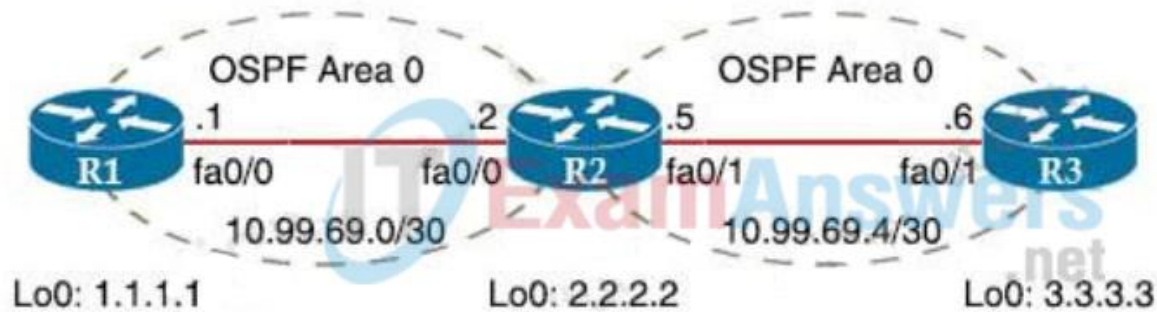
189. Refer to the exhibit. Which two commands are needed to allow for full reachability between AS 1000 and AS 2000? (Choose two)



- A. R1#network 19.168.0.0 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

190. Refer to the exhibit. R1 is able to ping the R3 fa0/1 interface. Why do the extended pings fail?



```
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>
```

- 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

Explanation: If the DF bit is set, routers cannot fragment packets. From the output below, we learn that the maximum MTU of R2 is 1492 bytes while we sent ping with 1500 bytes. Therefore these ICMP packets were dropped.

Note: Record option displays the address(es) of the hops (up to nine) the packet goes through.

191. 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 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

Explanation: In fact, VRRP has the preemption enabled by default so we don't need the `vrrp 10 preempt` command. The default priority is 100 so we don't need to configure it either. But notice that the correct command to configure the virtual IP address for the group is `vrrp 10 ip {ipaddress}` (not `vrrp group 10 ip ...`) and this command does not include a subnet mask.

192. 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. run on a virtual server and includes its own operating system

Correct Answer: B

Explanation: There are two types of hypervisors: type 1 and type 2 hypervisor.

In type 1 hypervisor (or native hypervisor), the hypervisor is installed directly on the physical server. Then instances of an operating system (OS) are installed on the hypervisor. Type 1 hypervisor has direct access to the hardware resources. Therefore they are more efficient than hosted architectures. Some examples of type 1 hypervisor are VMware vSphere/ESXi, Oracle VM Server, KVM and Microsoft Hyper-V.

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



193. 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 correct
- D. NETCONF
- E. Python

Correct Answer: C

194. 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

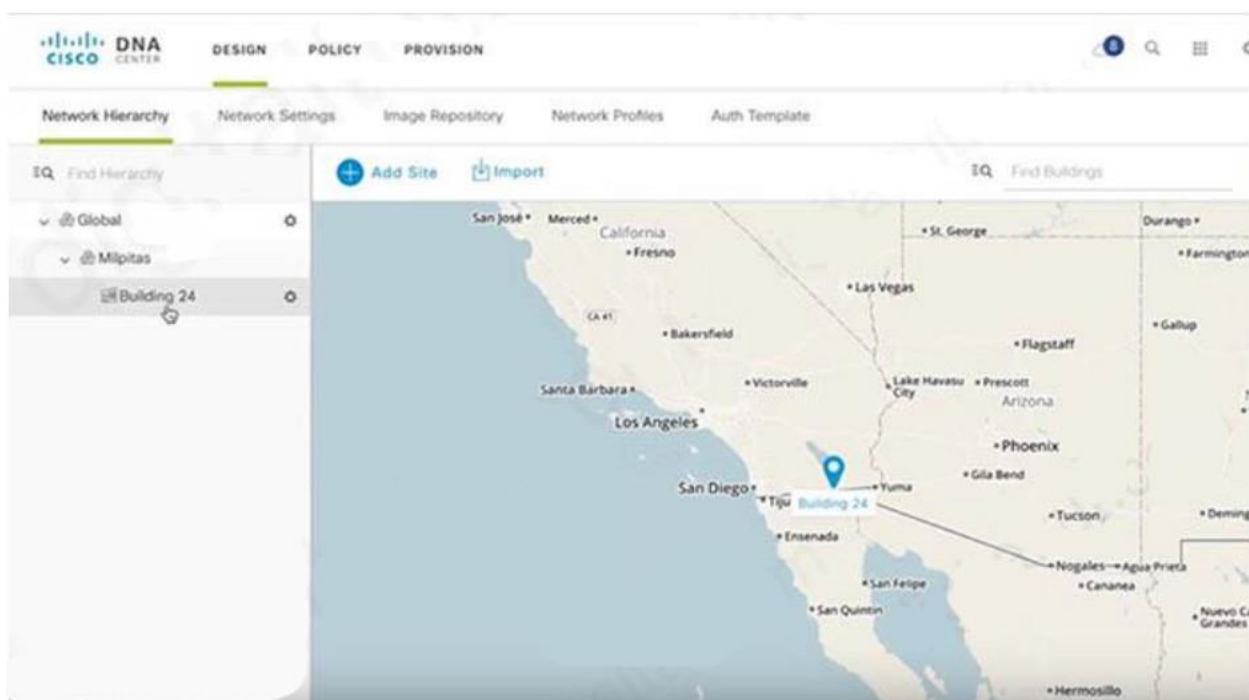
- C. by organization
- D. by hostname naming convention

Correct Answer: A

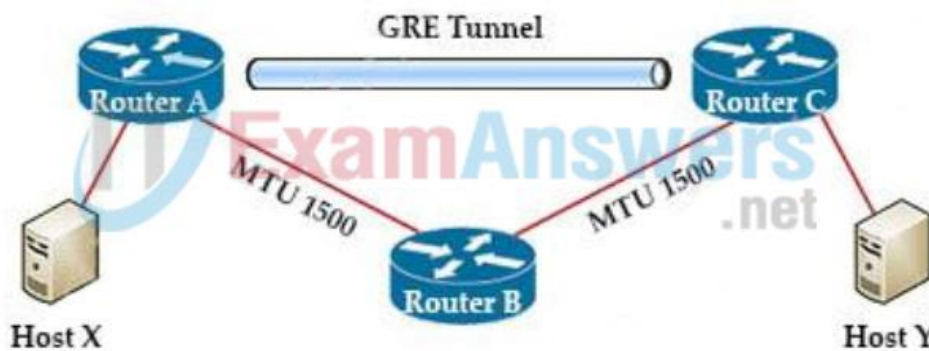
Explanation: You can create a network hierarchy that represents your network's geographical locations.

Your network hierarchy can contain sites, which in turn contain buildings and areas. You can create site and building IDs to easily identify where to apply design settings or configurations later.

Reference: [Here](#)



195. 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

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

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

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

196. 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**

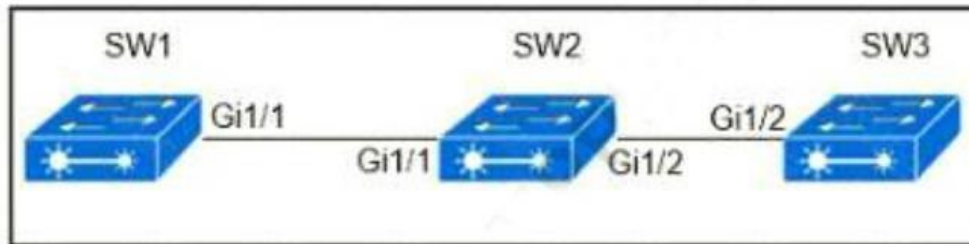
Correct Answer: DF

Explanation: Locator ID Separation Protocol (LISP) is a network architecture and protocol that implements the use of two namespaces instead of a single IP address:

+ Endpoint identifiers (EIDs)-assigned to end hosts.

+ Routing locators (RLOCs)-assigned to devices (primarily routers) that make up the global routing system.

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.
SW2(config)#interface gi1/2
SW2(config)#switchport trunk allowed vlan 10
- B.
SW1(config)#interface gi1/1
SW1(config)#switchport trunk allowed vlan 1-9,11-4094
- C.
SW2(config)#interface gi1/2
SW2(config)#switchport trunk allowed vlan 1-9,11-4094
- D.
SW2(config)#interface gi1/1
SW2(config)#switchport trunk allowed vlan 10
- A. Option A
 - B. Option B
 - C. Option C
 - D. Option D

Correct Answer: C

198. 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

Explanation: The Intent API is a Northbound REST API that exposes specific capabilities of the Cisco DNA Center platform. The Intent API provides policy-based abstraction of business intent, allowing focus on an outcome rather than struggling with individual mechanisms steps.

Reference: [Here](#)

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

```
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
!
```

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

Correct Answer: A

Explanation: The command `ip nat inside source list 10 interface FastEthernet0/1 overload` configures NAT to overload on the address that is assigned to the Fa0/1 interface.

200. A GRE tunnel is down with the error message %TUN-5-RECUR DOWN:

Tunnel0 temporarily disabled due to recursive routing error.

Which two options describe possible causes of the error? (Choose two)

- A. There is link flapping on the tunnel
- B. Incorrect destination IP addresses are configured on the tunnel
- C. The tunnel mode and tunnel IP address are misconfigured
- D. There is instability in the network due to route flapping
- E. The tunnel destination is being routed out of the tunnel interface

Correct Answer: DE

Explanation: The %TUN-5-RECURDOWN: Tunnel0 temporarily disabled due to recursive routing error message means that the generic routing encapsulation (GRE) tunnel router has discovered a recursive routing problem. This condition is usually due to one of these causes:

- + A misconfiguration that causes the router to try to route to the tunnel destination address using the tunnel interface itself (recursive routing)
- + A temporary instability caused by route flapping elsewhere in the network

201. 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

202. 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

Explanation: Because some PE routers might receive routing information they do not require, a basic requirement is to be able to filter the MP-iBGP updates at the ingress to the PE router so that the router does not need to keep this information in memory. The Automatic Route Filtering feature fulfills this filtering requirement. This feature is available by default on all PE routers, and no additional configuration is necessary to enable it. Its function is to filter automatically VPN-IPv4 routes that contain a route target extended community that

does not match any of the PE's configured VRFs. This effectively discards any unwanted VPN-IPv4 routes silently, thus reducing the amount of information that the PE has to store in memory
-> Answer 'PE1 will reject the route due to automatic route filtering' is correct.

203. 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

204. 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

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

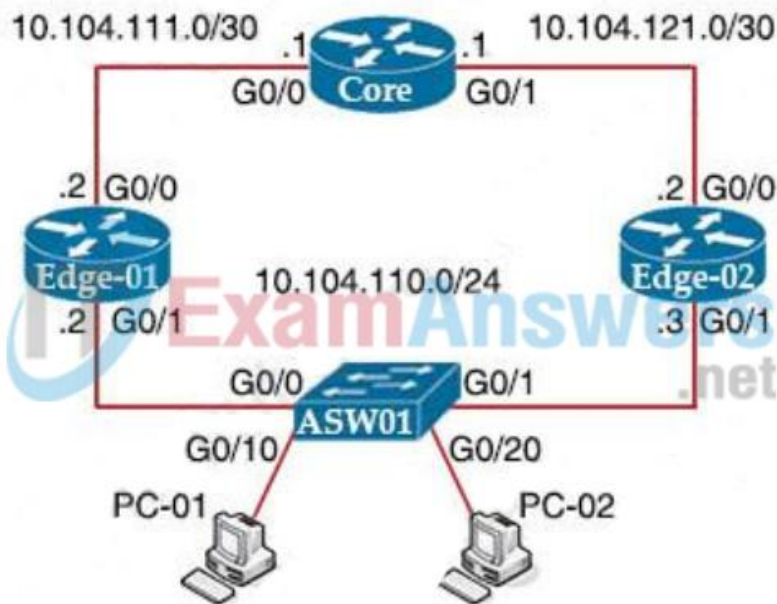
- A. Omnidirectional
- B. dipole
- C. patch
- **D. Yagi**

Correct Answer: D

Explanation: Yagi Antenna

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

206. Refer to the exhibit. Edge-01 is currently operational as the HSRP primary with priority 110. Which command on Edge-02 causes it to take over the forwarding role when Edge-01 is down?



- A. standby 10 priority
- **B. standby 10 preempt**
- C. standby 10 track
- D. standby 10 timers

Correct Answer: B

Explanation: The `preempt` command enables the HSRP router with the highest priority to immediately become the active router.

207. 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: C

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

- A. Cisco Express Forwarding is required to load-balance across interfaces
- **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. EIGRP supports 6 unequal-cost paths**

Correct Answer: BE

Explanation: EIGRP provides a mechanism to load balance over unequal cost paths (or called unequal cost load balancing) through the “variance” command. In other words, EIGRP will install all paths with $\text{metric} < \text{variance} * \text{best metric}$ into the local routing table, provided that it meets the feasibility condition to prevent routing loop. The path that meets this requirement is called a feasible successor. If a path is not a feasible successor, it is not used in load balancing. Note: The feasibility condition states that, the Advertised Distance (AD) of a route must be lower than the feasible distance of the current successor route.

209. 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

Explanation: “Punt” is often used to describe the action of moving a packet from the fast path (CEF) to the route processor for handling.

Cisco Express Forwarding (CEF) provides the ability to switch packets through a device in a very quick and efficient way while also keeping the load on the router’s processor low. CEF is made up of two different main components: the Forwarding Information Base (FIB) and the Adjacency Table.

Process switching is the slowest switching methods (compared to fast switching and Cisco Express Forwarding) because it must find a destination in the routing table. Process switching must also construct a new Layer 2 frame header for every packet. With process switching, when a packet comes in, the scheduler calls a process that examines the routing table, determines which interface the packet should be switched to and then switches the packet. The problem is, this happens for the every packet.

Reference: [Click here](#)

210. Which QoS mechanism will prevent a decrease in TCP performance?

- A. Shaper
- B. Rate-Limit
- C. Policer
- D. Fair-Queue
- **E. WRED**
- F. LLQ

Correct Answer: E

Explanation: Weighted Random Early Detection (WRED) is just a congestion avoidance mechanism. WRED drops packets selectively based on IP precedence. Edge routers assign IP precedences to packets as they enter the network. When a packet arrives, the following events occur:

The average queue size is calculated.

2. If the average is less than the minimum queue threshold, the arriving packet is queued.
3. If the average is between the minimum queue threshold for that type of traffic and the maximum threshold for the interface, the packet is either dropped or queued, depending on the packet drop probability for that type of traffic.

4. If the average queue size is greater than the maximum threshold, the packet is dropped.

WRED reduces the chances of tail drop (when the queue is full, the packet is dropped) by selectively dropping packets when the output interface begins to show signs of congestion (thus it can mitigate congestion by preventing the queue from filling up). By dropping some packets early rather than waiting until the queue is full, WRED avoids dropping large numbers of packets at once and minimizes the chances of global synchronization. Thus, WRED allows the transmission line to be used fully at all times.

WRED generally drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, the higher the priority of a packet, the higher the probability that the packet will be delivered.

211. 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

Explanation: 6to4 tunnel is a technique which relies on reserved address space 2002::/16 (you must remember this range). These tunnels determine the appropriate destination address by combining the IPv6 prefix with the globally unique destination 6to4 border router's IPv4 address, beginning with the 2002::/16 prefix, in this format:

2002:border-router-IPv4-address::/48

For example, if the border-router-IPv4-address is 64.101.64.1, the tunnel interface will have an IPv6 prefix of 2002:4065:4001:1::/64, where 4065:4001 is the hexadecimal equivalent of 64.101.64.1. This technique allows IPv6 sites to communicate with each other over the IPv4 network without explicit tunnel setup but we have to implement it on all routers on the path.

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

- A. INIT
- B. listen

- C. full
- D. learning
- E. speak
- F. established

Correct Answer: ABE

Explanation: HSRP States When in operation, HSRP devices are configured into one of many states:

Active – This is the state of the device that is actively forwarding traffic.

Init or Disabled – This is the state of a device that is not yet ready or able to participate in HSRP.

Learn – This is the state of a device that has not yet determined the virtual IP address and has not yet seen a hello message from an active device.

Listen – This is the state of a device that is receiving hello messages.

Speak – This is the state of a device that is sending and receiving hello messages.

Standby – This is the state of a device that is prepared to take over the traffic forwarding duties from the active device.

213. 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. OnPrem 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

Explanation: AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to setup application scaling for

214. 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

Explanation: The time kept on a machine is a critical resource and it is strongly recommend that you use the security features of NTP to avoid the accidental or malicious setting of incorrect time. The two security features available are an access list-based restriction scheme and an encrypted authentication mechanism.

[Reference](#)

215. 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

Explanation: 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.

The SSO HSRP feature enables the Cisco IOS HSRP subsystem software to detect that a standby RP is installed and the system is configured in SSO redundancy mode. Further, if the active RP fails, no change occurs to the HSRP group itself and traffic continues to be forwarded through the current active gateway device.

Reference: [Click here](#)

216. Which three methods does Cisco DNA Center 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

Explanation: There are three ways for you to discover devices:

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

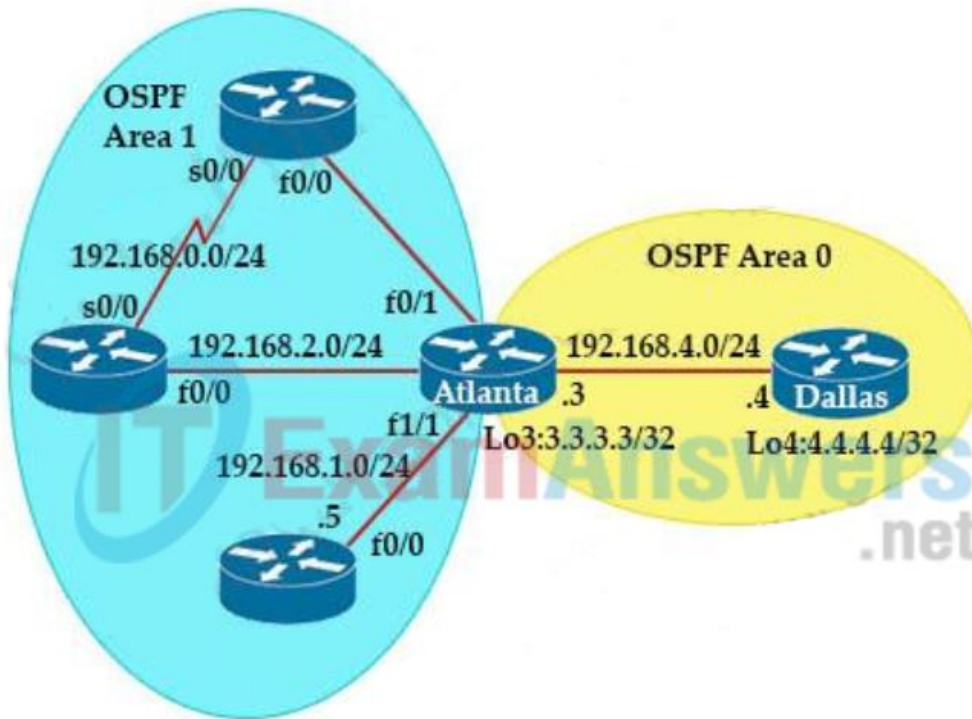
217. What is the primary effect of the spanning-tree portfast command?

- A. It enables BPDU messages
- **B. It minimizes spanning-tree convergence time**
- C. It immediately puts the port into the forwarding state when the switch is reloaded
- D. It immediately enables the port in the listening state

Correct Answer: B

Explanation: The purpose of Port Fast is to minimize the time interfaces must wait for spanning-tree to converge, it is effective only when used on interfaces connected to end stations.

218. 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?



Dallas#show ip route ospf

```

3.0.0.0/32 is subnetted, 1 subnets
O    3.3.3.3 [110/40001] via 192.168.4.3, 00:33:32, FastEthernet0/0
O IA 192.168.0.0/24 [110/145535] via 192.168.4.3, 00:33:32, FastEthernet0/0
O IA 192.168.1.0/24 [110/80000] via 192.168.4.3, 00:33:32, FastEthernet0/0
O IA 192.168.2.0/24 [110/80000] via 192.168.4.3, 00:33:32, FastEthernet0/0
O IA 192.168.3.0/24 [110/44000] via 192.168.4.3, 00:33:32, FastEthernet0/0

```

- 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

219. Refer to the exhibit. Which two statements about the EEM applet configuration are true? (Choose two.)

```

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 newline "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

```

- 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: BC

Explanation: When you use the sync yes option in the event cli command, the EEM applet runs before the CLI command is executed. The EEM applet should set the _exit_status variable to indicate whether the CLI command should be executed (_exit_status set to one) or not (_exit_status set to zero).

With the sync no option, the EEM applet is executed in background in parallel with the CLI command.

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

```

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

```

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

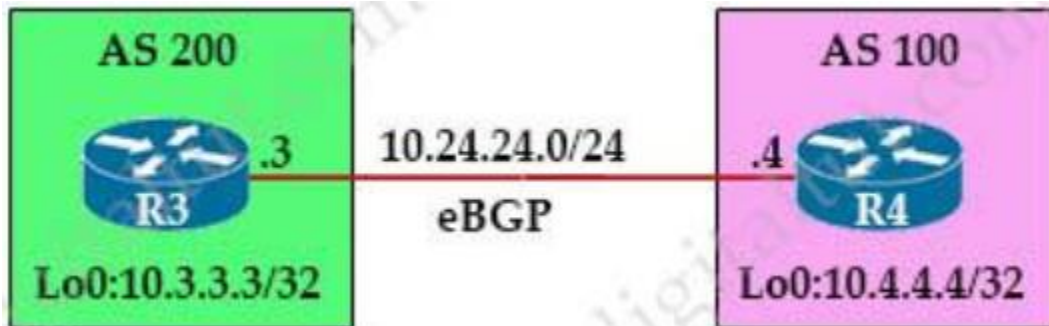
Correct Answer: A

Explanation: Missing Data Model RPC Error Reply Message

If a request is made for a data model that doesn't exist on the Catalyst 3850 or a request is made for a leaf that is not implemented in a data model, the Server (Catalyst 3850) responds with an empty data response. This is expected behavior.

Reference: [Click here](#)

221. 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
```

222. Which statement about dynamic GRE between a headend router and a remote router is true?

- A. The headend router learns the IP address of the remote end router statically
- B. A GRE tunnel without an IP address has a status of administratively down
- C. GRE tunnels can be established when the remote router has a dynamic IP address
- **D. The remote router initiates the tunnel connection**

Correct Answer: D

223. 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

Answer: CD

224. Which action is performed by Link Management Protocol in a Cisco stackwise virtual domain?

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

Answer: B

Explanation: The Link Management Protocol (LMP) performs the following functions: + Verifies link integrity by establishing bidirectional traffic forwarding, and rejects any unidirectional links + Exchanges periodic hellos to monitor and maintain the health of the links + Negotiates the version of StackWise Virtual header between the switches StackWise Virtual link role resolution

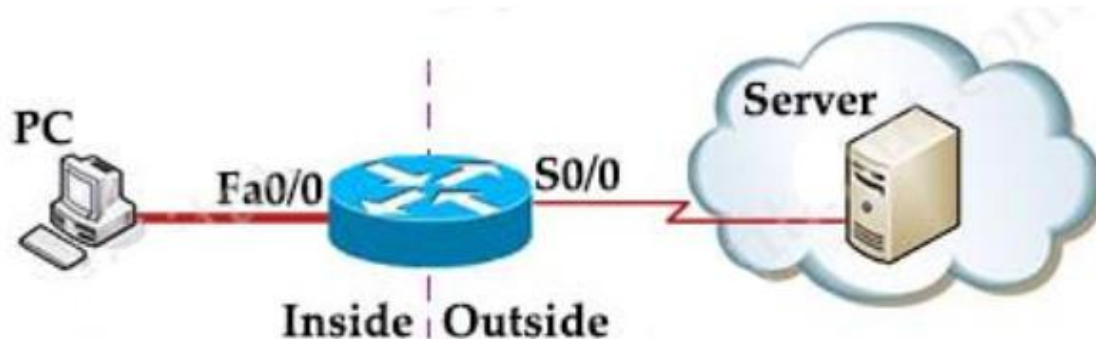
Reference: <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-stack-wp-cte-en.html>

225. An engineer must configure a 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 ip any any eq 21 tcp-ack
- C. access-list 10 permit tcp any any eq 21 established
- **D. access-list 110 permit tcp any any eq 21 established**

Correct Answer: D

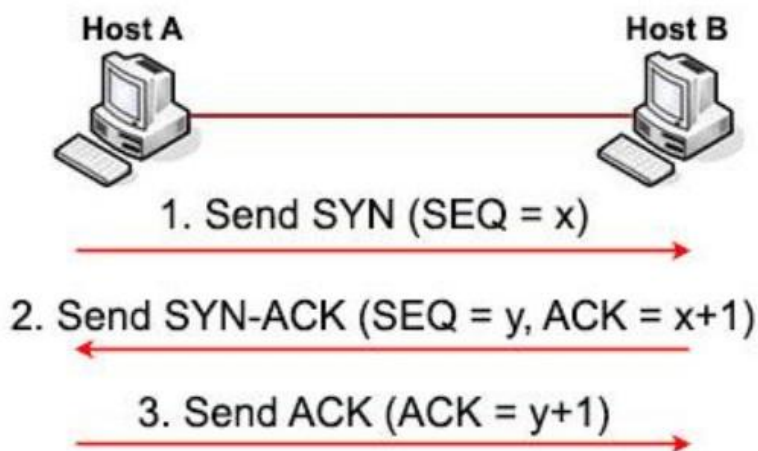
Explanation: The **established** keyword is only applicable to TCP access list entries to match TCP segments that have the ACK and/or RST control bit set (regardless of the source and destination ports), which assumes that a TCP connection has already been established in one direction only. Let's see an example below:



Suppose you only want to allow the hosts inside your company to telnet to an outside server but not vice versa, you can simply use an — "established" access-list like this:

```
access-list 100 permit tcp any any established
access-list 101 permit tcp any any eq telnet
!
interface S0/0
ip access-group 100 in
ip access-group 101 out
```

Note: Suppose host A wants to start communicating with host B using TCP. Before they can send real data, a three-way handshake must be established first. Let's see how this process takes place:



1. First host A will send a **SYN message** (a TCP segment with SYN flag set to 1, SYN is short for SYNchronize) to indicate it wants to setup a connection with host B. This message includes a

sequence (SEQ) number for tracking purpose. This sequence number can be any 32-bit number (range from 0 to 2^{32}) so we use —"x" to represent it.

2. After receiving SYN message from host A, host B replies with **SYN-ACK message** (some books may call it —SYN/ACK or —SYN, ACK message. ACK is short for ACKnowledge). This message includes a SYN sequence number and an ACK number:

+ SYN sequence number (let's called it "y") is a random number and does not have any relationship with Host A's SYN SEQ number.

+ ACK number is the next number of Host A's SYN sequence number it received, so we represent it with "x+1". It means —I received your part. Now send me the next part (x + 1)".

The SYN-ACK message indicates host B accepts to talk to host A (via ACK part). And ask if host A still wants to talk to it as well (via SYN part).

3. After Host A received the SYN-ACK message from host B, it sends an **ACK message** with ACK number "y+1" to host B. This confirms host A still wants to talk to host B.

226. In a Cisco SD-Access fabric, which control plane protocol is used for mapping and resolving endpoints?

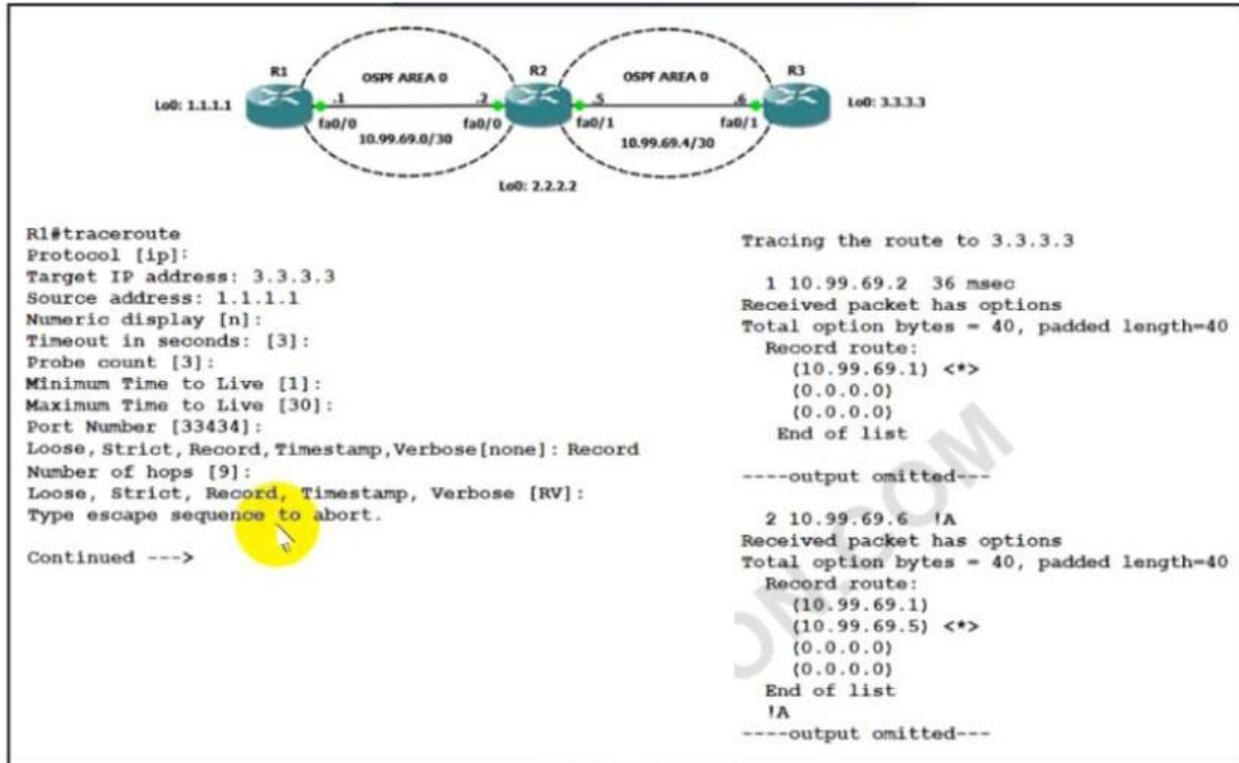
- A. DHCP
- B. VXLAN
- C. SXP
- **D. LISP**

Correct Answer: D

Explanation: We see in the traceroute result the packet could reach 10.99.69.5 (on R2) but it could not go any further so we can deduce an ACL on R3 was blocking it.

Note: Record option displays the address(es) of the hops (up to nine) the packet goes through.

227. Refer to the exhibit. The traceroute fails from R1 to R3. What is the cause of the failure?



- A. The loopback on R3 Is in a shutdown stale.
- B. An ACL applied Inbound on loopback0 of R2 Is dropping the traffic.
- **C. An ACL applied Inbound on fa0/1 of R3 is dropping the traffic.**
- D. Redistribution of connected routes into OSPF is not configured.

Correct Answer: C

Explanation: We see in the traceroute result the packet could reach 10.99.69.5 (on R2) but it could not go any further so we can deduce an ACL on R3 was blocking it.

Note: Record option displays the address(es) of the hops (up to nine) the packet goes through.

228. 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. onboard vEdge nodes into the SD-WAN fabric
- C. gather telemetry data from yEdge routers
- **D. distribute policies that govern data forwarding performed within the SD-WAN fabric**

Answer: D

Explanation: Control plane (vSmart) builds and maintains the network topology and make decisions on the traffic flows. The vSmart controller disseminates control plane information between WAN Edge devices, implements control plane policies and distributes data plane policies to network devices for enforcement.

229. Which deployment option of Cisco NGFW provides scalability?

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

Correct Answer: D

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

230. 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

Explanation: Fabric control plane node (C): One or more network elements that implement the LISP Map-Server (MS) and Map-Resolver (MR) functionality. The control plane node's host tracking database keep track of all endpoints in a fabric site and associates the endpoints to fabric nodes in what is known as an EID-to-RLOC binding in LISP.

Reference:

<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-macro-segmentationdeploy-guide.htm>

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

- A. both supervisors must be configured separately
- B. the multicast state is preserved during switchover
- C. must be combined with NSF to support uninterrupted Layer 2 operations
- **D. must be combined with NSF to support uninterrupted Layer 3 operations**

- **E. requires synchronization between supervisors in order to guarantee continuous connectivity**

Correct Answer: D,E

Explanation: against failure due to the Supervisor or loss of service because of software problems. The access layer typically provides Layer 2 services with redundant switches making up the distribution layer. The Layer 2 access layer can benefit from SSO deployed without NSF. Some Enterprises have deployed Layer 3 routing at the access layer. In that case, NSF/SSO can be used.

Cisco IOS Nonstop Forwarding(NSF) always runs with stateful switchover (SSO) and provides redundancy for Layer 3 traffic.

233. 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

Explanation: Once you know the complete combination of transmitter power level, the length of cable, and the antenna gain, you can figure out the actual power level that will be radiated from the antenna. This is known as the effective isotropic radiated power (EIRP), measured in dBm. EIRP is a very important parameter because it is regulated by governmental agencies in most countries. In those cases, a system cannot radiate signals higher than a maximum allowable EIRP. To find the EIRP of a system, simply add the transmitter power level to the antenna gain and subtract the cable loss.

234. 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

Explanation: When the primary controller (WLC-1) goes down, the APs automatically get registered with the secondary controller (WLC-2). The APs register back to the primary controller when the primary controller comes back on line.

235. Which two sources cause interference for Wi-Fi networks? (Choose two).

- **A. mirrored wall**
- B. 900MHz baby monitor
- **C. fish tank**
- D. DECT 6.0 cordless
- E. Incandescent lights

Correct Answer: A, C

Explanation: Windows can actually block your WiFi signal. How? Because the signals will be reflected by the glass.

Some new windows have transparent films that can block certain wave types, and this can make it harder for your WiFi signal to pass through.

Tinted glass is another problem for the same reasons. They sometimes contain metallic films that can completely block out your signal. Mirrors, like windows, can reflect your signal. They're also a source of electromagnetic interference because of their metal backings.

Reference: <https://dis-dot-dat.net/what-materials-can-block-a-wifi-signal/> An incandescent light bulb, incandescent lamp or incandescent light globe is an electric light with a wire filament heated until it glows. WiFi operates in the gigahertz microwave band. The FCC has strict regulations on RFI (radio frequency interference) from all sorts of things, including light bulbs - > Incandescent lights do not interfere Wi-Fi networks.

Note:

+ Many baby monitors operate at 900MHz and won't interfere with Wi-Fi, which uses the 2.4GHz band. + DECT cordless phone 6.0 is designed to eliminate wifi interference by operating on a different frequency.

There is essentially no such thing as DECT wifi interference.

236. 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

Explanation: By default, EIGRP metric is calculated:

metric = bandwidth + delay

While OSPF is calculated by:

OSPF metric = Reference bandwidth / Interface bandwidth in bps

(Or Cisco uses 100Mbps (10⁸) bandwidth as reference bandwidth. With this bandwidth, our

equation would be:

Cost = 10^8 /interface bandwidth in bps)

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

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

Correct Answer: B,E

Explanation: The Forwarding Information Base (FIB) contains destination reachability information as well as next hop information. This information is then used by the router to make forwarding decisions. The FIB allows for very efficient and easy lookups. Below is an example of the FIB table:

```
R2#show ip cef
```

Prefix	Next Hop	Interface
0.0.0.0/0	192.168.201.1	FastEthernet0/0
0.0.0.0/32	receive	
192.168.201.0/27	attached	FastEthernet0/0
192.168.201.0/32	receive	
192.168.201.1/32	192.168.201.1	FastEthernet0/0
192.168.201.2/32	receive	
192.168.201.31/32	receive	
224.0.0.0/4	drop	
224.0.0.0/24	receive	
255.255.255.255/32	receive	

The FIB maintains next-hop address information based on the information in the IP routing table (RIB).

Note: In order to view the Routing information base (RIB) table, use the **show ip route** command. To view the Forwarding Information Base (FIB), use the **show ip cef** command. RIB is in Control plane while FIB is in Data plane.

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

- **A. It creates two entries for each network node, one for Its identity and another for its location on the network.**

- B. It allows LISP to be applied as a network visualization overlay 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: A

Explanation: Locator ID Separation Protocol (LISP) solves this issue by separating the location and identity of a device through the Routing locator (RLOC) and Endpoint identifier (EID):

+ **Endpoint identifiers (EIDs)** – assigned to end hosts.

+ **Routing locators (RLOCs)** – assigned to devices (primarily routers) that make up the global routing system.

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

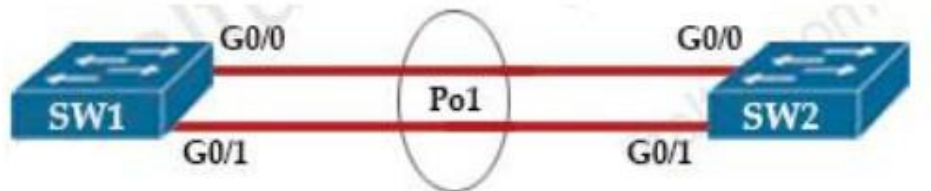


- A. Client 1 contact controller B by using an EoIP tunnel.
- B. CAPWAP tunnel is created between controller A and controller B.
- C. Client 1 uses an EoIP tunnel to contact controller A.
- **D. The client database entry moves from controller A to controller B.**

Correct Answer: D

Explanation: This is called Inter Controller-L2 Roaming. Inter-Controller (normally layer 2) roaming occurs when a client roam between two APs registered to two different controllers, where each controller has an interface in the client subnet. In this instance, controllers exchange mobility control messages (over UDP port 16666) and the client database entry is moved from the original controller to the new controller.

240. 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#  
08:33:23: %PM-4-ERR_DISABLE: channel-misconfig error detection on Gi0/0, putting  
Gi0/0 in err-disable state  
08:33:23: %PM-4-ERR_DISABLE: channel-misconfig error detection 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: A

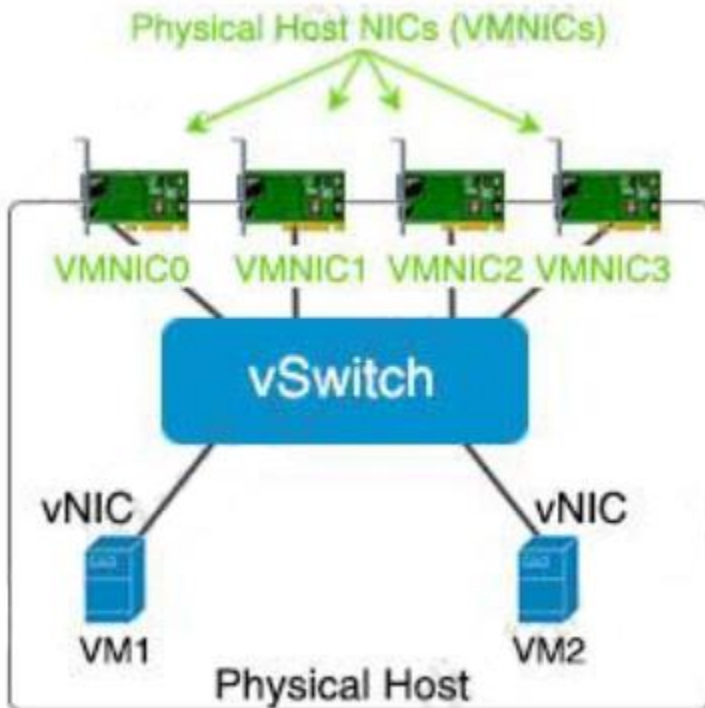
Explanation: In this case, we are using your EtherChannel without a negotiation protocol. As a result, if the opposite switch is not also configured for EtherChannel operation on the respective ports, there is a danger of a switching loop. The EtherChannel Misconfiguration Guard tries to prevent that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

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

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

Correct Answer: B

Explanation: Each VM is provided with a **virtual NIC (vNIC)** that is connected to the virtual switch. Multiple vNICs can connect to a single vSwitch, allowing VMs on a physical host to communicate with one another at layer 2 without having to go out to a physical switch.



242. Refer to the exhibit. What are two effects of this configuration? (Choose two.)

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

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

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

Correct Answer: A,D

243. Refer to the exhibit. These commands have been added to the configuration of a switch. Which command flags an error If It is added to this configuration?

```
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
```

- 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

Explanation: A monitor session can source from interfaces or VLANs – not both at the same time.

RSPAN consists of at least one RSPAN source session, an RSPAN VLAN, and at least one RSPAN destination session. You separately configure RSPAN source sessions and RSPAN destination sessions on different network devices. To configure an RSPAN source session on a device, you associate a set of source ports or source VLANs with an RSPAN VLAN.

Traffic monitoring in a SPAN session has these restrictions:

+ Sources can be ports or VLANs, but you cannot mix source ports and source VLANs in the same session.

Reference: [Here](#)

Therefore in this question, we cannot configure a source VLAN because we configured source ports for RSPAN session 1 already.

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

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

Correct Answer: A

Explanation: Cisco DNA Center allows customers to manage their non-Cisco devices through the use of a Software Development Kit (SDK) that can be used to create Device Packages for third-party devices.

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

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

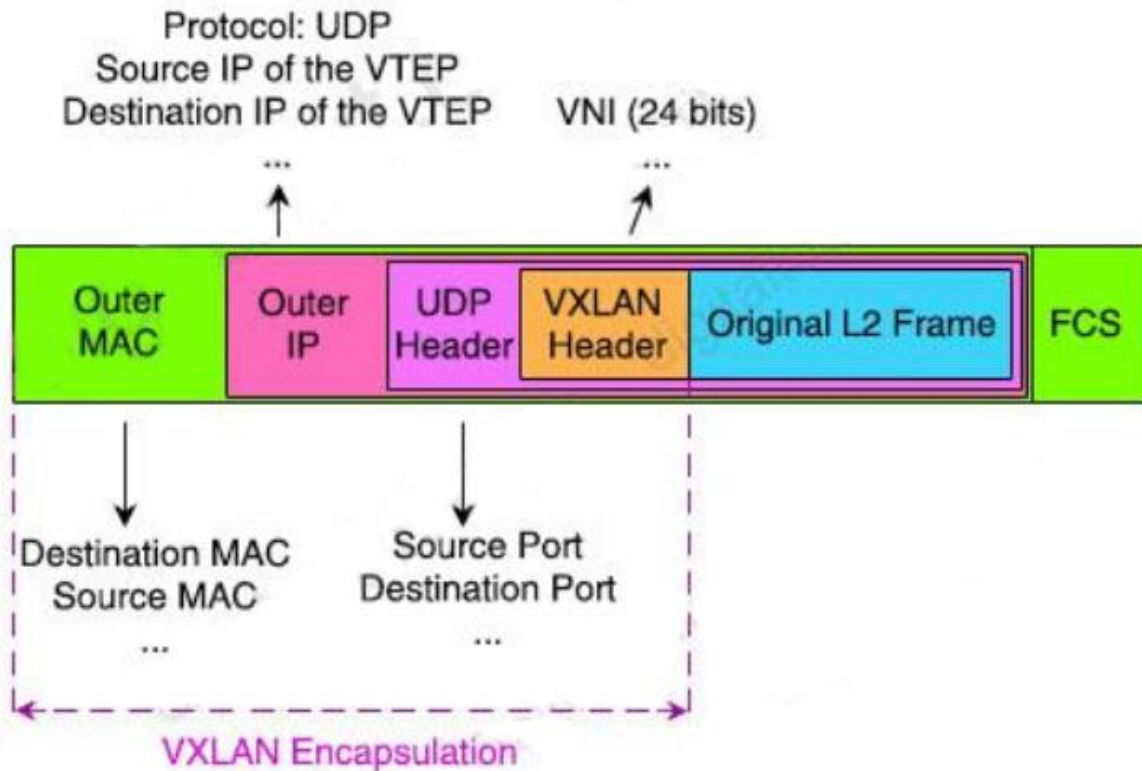
Correct Answer: C

Explanation: VXLAN uses an 8-byte VXLAN header that consists of a 24-bit VNID and a few reserved bits. The VXLAN header together with the original Ethernet frame goes in the UDP

payload.

The 24-bit VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments.

Let's see the structure of a VXLAN packet to understand how (note: VNI = VNID)



The key fields for the VXLAN packet in each of the protocol headers are:

- + **Outer MAC header** (14 bytes with 4 bytes optional) – Contains the MAC address of the source VTEP and the MAC address of the next-hop router. Each router along the packet's path rewrites this header so that the source address is the router's MAC address and the destination address is the next-hop router's MAC address.

- + **Outer IP header** (20 bytes)- Contains the IP addresses of the source and destination VTEPs.

- + **(Outer) UDP header** (8 bytes)- Contains source and destination UDP ports:

- Source UDP port: The VXLAN protocol repurposes this standard field in a UDP packet header. Instead of using this field for the source UDP port, the protocol uses it as a numeric identifier for the particular flow between VTEPs. The VXLAN standard does not define how this number is derived, but the source VTEP usually calculates it from a hash of some combination of fields from the inner Layer 2 packet and the Layer 3 or Layer 4 headers of the original frame.

– Destination UDP port: The VXLAN UDP port. The Internet Assigned Numbers Authority (IANA) allocates port 4789 to VXLAN.

+ **VXLAN header** (8 bytes)- Contains the 24-bit VNI (or VNID)

+ **Original Ethernet/L2 Frame** – Contains the original Layer 2 Ethernet frame.

246. 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 the engineer notices that the routers are not functioning as expected. Which action will resolve the configuration error?

R1 key chain cisco123 key 1 key-string Cisco123!	R2 key chain cisco123 key 1 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 Local virtual MAC address is 0000.0c07.ac0a (v1 default) Hello time 5 sec, hold time 15 sec Next hello sent in 2.704 secs Authentication MD5, key-chain "cisco123" Preemption enabled Active router is local Standby router is unknown Priority 255 (configured 255) Group name is "workstation-group" (cfgd)	Ethernet0/0 - Group 10 State is Active 17 state changes, last state change 00:03:33 Virtual IP address is 192.168.0.1 Active virtual MAC address is 0000.0c07.ac0a Local virtual MAC address is 0000.0c07.ac0a (v1 default) Hello time 10 sec, hold time 30 sec Next hello sent in 6.704 secs Authentication MD5, key-chain "cisco123" Preemption disabled Active router is local Standby router is unknown Priority 200 (configured 200) Group name is "workstation-group" (cfgd)

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

Correct Answer: B

Explanation: From the output exhibit, we notice that the key-string of R1 is "Cisco123!" (letter "C" is in capital) while that of R2 is "cisco123!". This causes a mismatch in the authentication so we have to fix their key-strings.

Note: key-string [encryption-type] *text-string*: Configures the text string for the key. The textstring argument is alphanumeric, case-sensitive, and supports special characters.

247. When reason could cause an OSPF neighborship to be in the EXSTART/EXCHANGE state?

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

Correct Answer: C

Explanation: When OSPF adjacency is formed, a router goes through several state changes before it becomes fully adjacent with its neighbor. The states are Down -> Attempt (optional) -> Init -> 2-Way -> Exstart -> Exchange -> Loading -> Full. Short descriptions about these states are listed below:

Down: no information (hellos) has been received from this neighbor.

Attempt: only valid for manually configured neighbors in an NBMA environment. In Attempt state, the router sends unicast hello packets every poll interval to the neighbor, from which hellos have not been received within the dead interval.

Init: specifies that the router has received a hello packet from its neighbor, but the receiving router's ID was not included in the hello packet

2-Way: indicates bi-directional communication has been established between two routers.

Exstart: Once the DR and BDR are elected, the actual process of exchanging link state information can start between the routers and their DR and BDR.

Exchange: OSPF routers exchange database descriptor (DBD) packets

Loading: In this state, the actual exchange of link state information occurs Full: routers are fully adjacent with each other (Reference:

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0e.shtml)

Neighbors Stuck in Exstart/Exchange State the problem occurs most frequently when attempting to run OSPF between a Cisco router and another vendor's router. The problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces don't match. If the router with the higher MTU sends a packet larger than the MTU set on the neighboring router, the neighboring router ignores the packet.

248. Refer to the exhibit. An engineer must configure a SPAN session. What is the effect of the configuration?

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

- 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

249. Refer to the exhibit. What are two effects of this configuration? (Choose two.)

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

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

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

Correct Answer: A,E

250. 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

Explanation: JWT or JSON Web Token is a string that is sent in the HTTP request (from client to server) to validate the authenticity of the client

251. 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

Explanation: ncclient is a Python library that facilitates client-side scripting and application development around the NETCONF protocol.

The above Python snippet uses the ncclient to connect and establish a NETCONF session to a Nexus device (which is also a NETCONF server).

252. 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

Explanation: SD-Access Wireless Architecture Control Plane Node –A Closer Look

Fabric Control-Plane Node is based on a LISP Map Server / Resolver

Runs the LISP Endpoint ID Database to provide overlay reachability information

+ A simple Host Database, that tracks Endpoint ID to Edge Node bindings (RLOCs)+ Host Database supports multiple types of Endpoint ID (EID), such as IPv4 /32, IPv6 /128* or MAC/48

+ Receives prefix registrations from Edge Nodes for wired clients, and from Fabric mode WLCs for wireless clients

+ Resolves lookup requests from FE to locate Endpoints

+ Updates Fabric Edge nodes, Border nodes with wireless client mobility and RLOC information

Reference: [Here](#)

253. Refer to the exhibit.

```

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

```

Which command set must be added to the configuration to analyze 50 packets out of every 100?

A.

```

sampler SAMPLER-1
mode random 1-out-of 2
flow FLOW-MONITOR-1

```

```

Interface GigabitEthernet 0/0/0
ip flow monitor SAMPLER-1 input

```

B.

```

sampler SAMPLER-1
no mode random 1-out-of 2
mode percent 50

```

```
interface GigabitEthernet 0/0/0
ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

C.

```
interface GigabitEthernet 0/0/0
ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

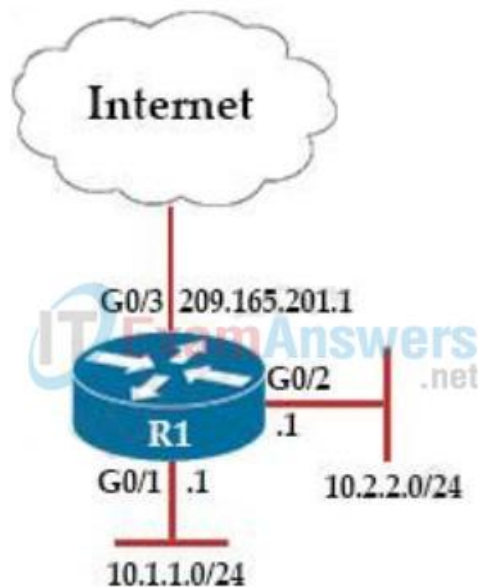
D.

```
flow monitor FLOW-MONITOR-1
record v4_r1
sampler SAMPLER-1
```

```
interface GigabitEthernet 0/0/0
ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

Correct Answer: C

254. 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?



Option A <pre>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</pre>	Option B <pre>access-list 10 permit 10.2.2.0 0.0.0.255 interface G0/3 ip nat outside interface G0/2 ip nat inside ip nat inside source list 10 209.165.201.1</pre>
Option C <pre>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</pre>	Option D <pre>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</pre>

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

Correct Answer: D

Explanation: The command `ip nat inside source list 10 interface G0/3 overload` configures NAT to overload (PAT) on the address that is assigned to the G0/3 interface.

255. Refer to the exhibit.

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

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

Option A access-list 23 permit 10.10.10.0 0.0.0.255 line vty 0 4 access-class 23 in transport input ssh	Option B access-list 23 permit 10.10.10.0 0.0.0.255 line vty 0 15 access-class 23 in transport input ssh
Option C access-list 23 permit 10.10.10.0 0.0.0.255 line vty 0 15 access-class 23 out transport input all	Option D access-list 23 permit 10.10.10.0 255.0.0.0 line vty 0 15 access-class 23 in transport input ssh

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

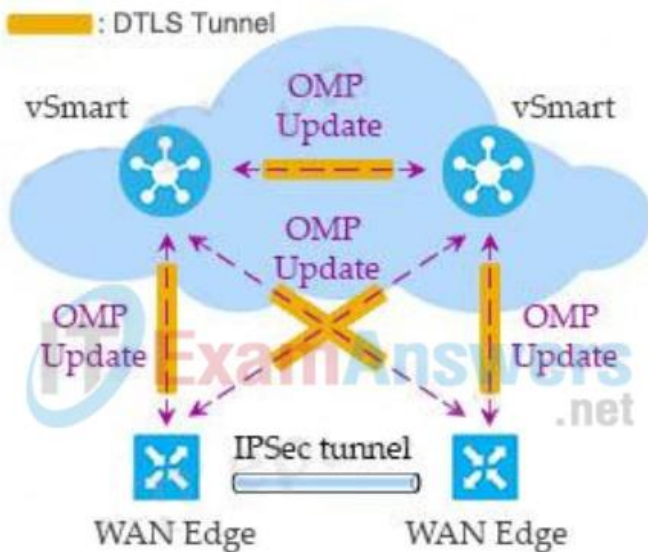
Correct Answer: B

256. 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

Explanation: Cisco SD-WAN uses Overlay Management Protocol (OMP) which manages the overlay network. OMP runs between the vSmart controllers and WAN Edge routers (and among vSmarts themselves) where control plane information, such as the routing, policy, and management information, is exchanged over a secure connection.



257. 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

Explanation: Stateful Switchover (SSO) provides protection for network edge devices with dual Route Processors (RPs) that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.

Reference: [Click here](#)

258. 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

Explanation: Query messages are used to elect the IGMP querier as follows:

1. When IGMPv2 devices start, they each multicast a general query message to the allsystems group address of 224.0.0.1 with their interface address in the source IP address field of the message.
2. When an IGMPv2 device receives a general query message, the device compares the source IP address in the message with its own interface address. The device with the lowest IP address on the subnet is elected the IGMP querier.
3. All devices (excluding the querier) start the query timer, which is reset whenever a general query message is received from the IGMP querier. If the query timer expires, it is assumed that the IGMP querier has gone down, and the election process is performed again to elect a new IGMP querier.

Reference: [Click here](#)

259. 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

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

Reference: [Click here](#)

260. 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
```

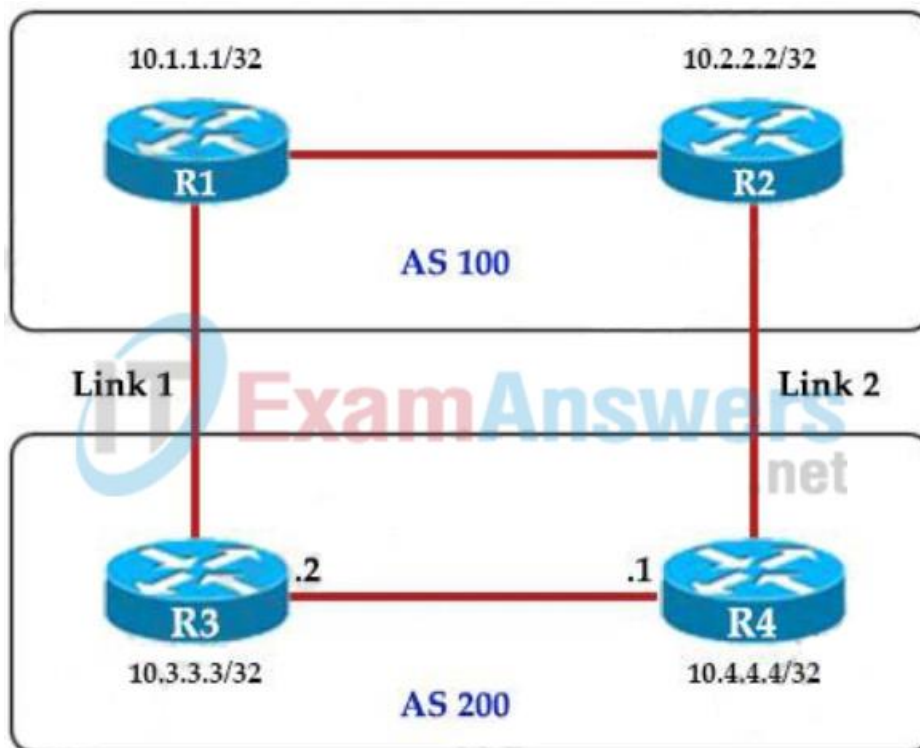
Which are two results of implementing this feature instead of traditional NetFlow? (Choose two)

- 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

Explanation: The “mode random one-out of 100” specifies that sampling uses the random mode and only take one sample out of every 100 packets.

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



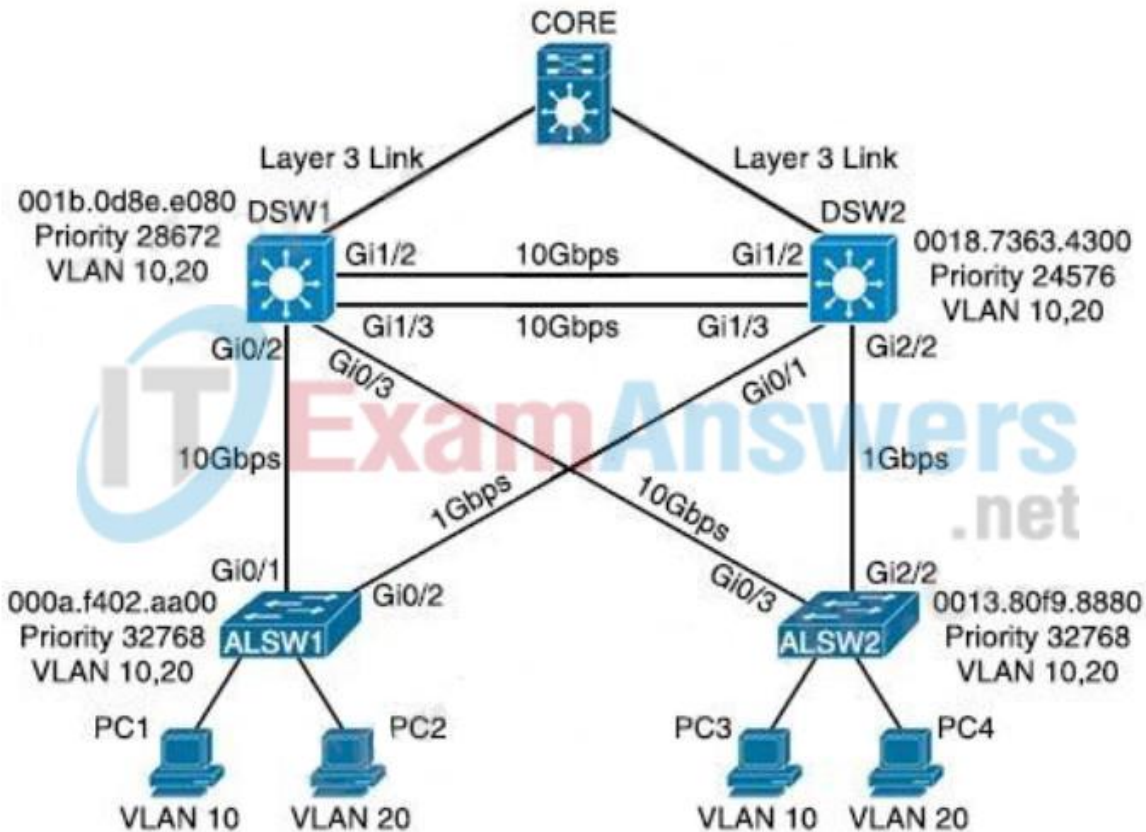
Option A R3(config)#route-map PREPEND permit 10 R3(config-route-map)#set as-path prepend 200 200 200 R3(config)# router bgp 200 R3(config-router)#neighbor 10.1.1.1 route- map PREPEND out	Option B R3(config)#route-map PREPEND permit 10 R3(config-route-map)#set as-path prepend 100 100 100 R3(config)# router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

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

Correct Answer: A

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

262. Refer to the exhibit. Assuming all links are functional, which path does PC1 take to reach DSW1?



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

Correct Answer: D

Explanation: In the topology above, we see DSW2 has lowest priority 24576 so it is the root bridge for VLAN 10 so surely all traffic for this VLAN must go through it. All of DSW2 ports must be in forwarding state. And:

- + The direct link between DSW1 and ALSW1 is blocked by STP.
- + The direct link between DSW1 and ALSW2 is also blocked by STP.

Therefore PC1 must go via this path: PC1 -> ALSW1 -> DSW2 -> DSW1.

263. A customer has deployed an environment with shared storage to allow for the migration of virtual machines between servers with dedicated operating systems that provide the virtualization platform. What is this operating system described as?

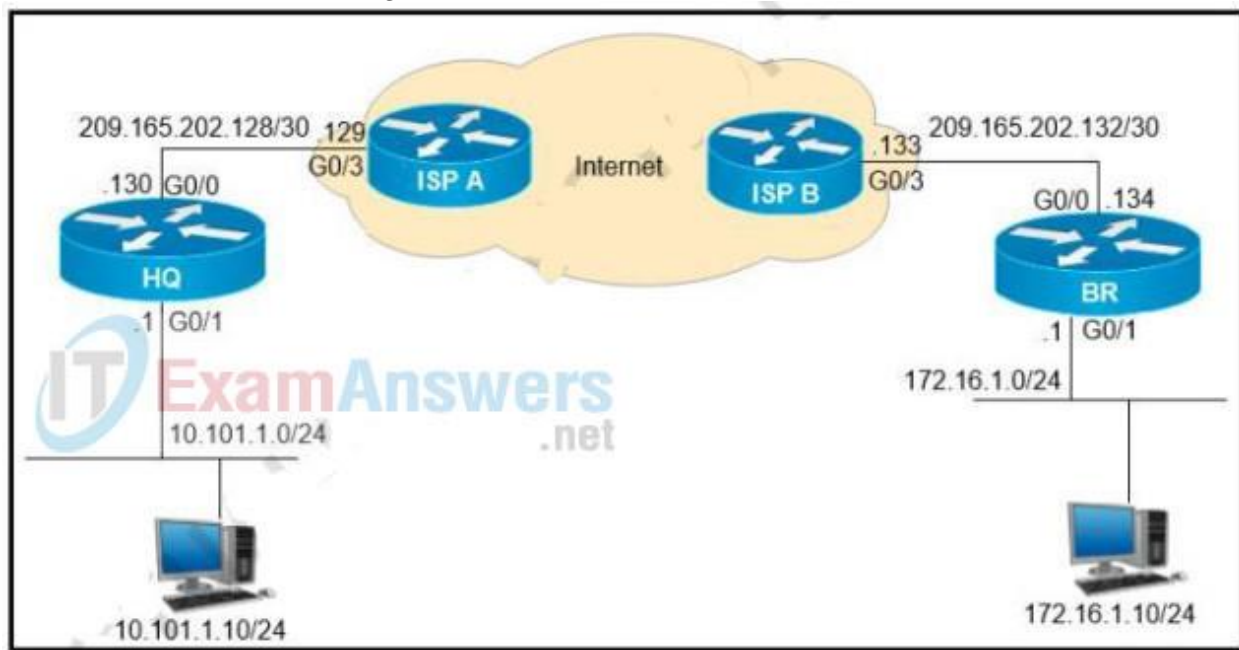
- **A. hosted virtualization**
- B. type 1 hypervisor

- C. container oriented
- D. decoupled

Correct Answer: A

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

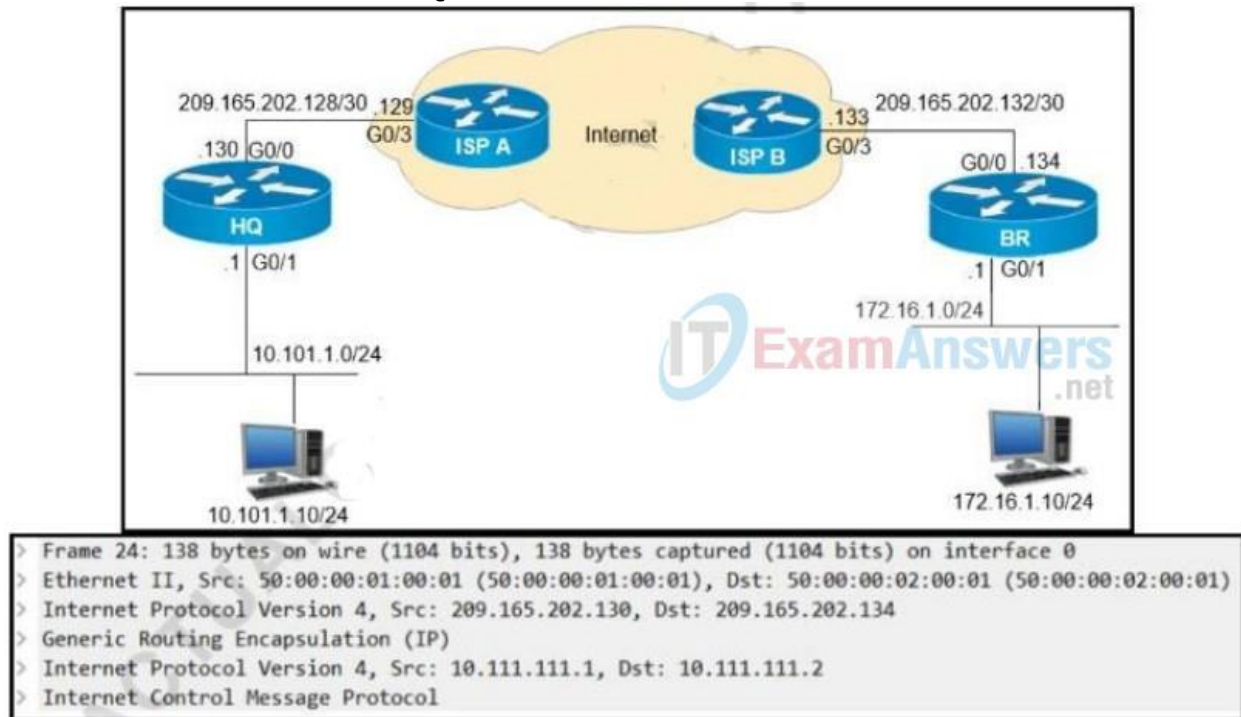
264. Refer to the exhibit. Which configuration must be applied to the HQ router to set up a GRE tunnel between the HQ and BR routers?



- A. ☐ interface Tunnell
ip address 209.165.202.130 255.255.255.252
tunnel source GigabitEthernet0/0
tunnel destination 209.165.202.129
- B. ☐ interface Tunnell
ip address 10.111.111.1 255.255.255.0
tunnel source GigabitEthernet0/0
tunnel destination 209.165.202.133
- C. ☐ interface Tunnell
ip address 10.111.111.1 255.255.255.0
tunnel source GigabitEthernet0/0
tunnel destination 209.165.202.129
- D. ☒ interface Tunnell
ip address 10.111.111.1 255.255.255.0
tunnel source GigabitEthernet0/0
tunnel destination 209.165.202.134

Correct Answer: D

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



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

Correct Answer: A

Explanation: In the above output, the IP address of “209.165.202.130” is the tunnel source IP while the IP 10.111.1.1 is the tunnel IP address.

An example of configuring GRE tunnel is shown below:

R1 (GRE config only) <pre> interface s0/0/0 ip address 63.1.27.2 255.255.255.0 interface tunnel0 ip address 10.0.0.1 255.255.255.0 tunnel mode gre ip //this command can be ignored tunnel source s0/0 tunnel destination 85.5.24.10 </pre>	R2 (GRE config only) <pre> interface s0/0/0 ip address 85.5.24.10 255.255.255.0 interface tunnel1 ip address 10.0.0.2 255.255.255.0 tunnel source 85.5.24.10 tunnel destination 63.1.27.2 </pre>
---	--

266. 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

267. 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

Explanation: 172.16.50.5 in hex is We will have the answer from this paragraph: “TLV values for the Option 43 suboption: Type + Length + Value. Type is always the suboption code 0xf1. Length is the number of controller management IP addresses times 4 in hex. Value is the IP address of the controller listed sequentially in hex. For example, suppose there are two controllers with management interface IP addresses, 192.168.10.5 and 192.168.10.20. The type is 0xf1. The length is $2 * 4 = 8 = 0x08$. The IP addresses translates to c0a80a05 (192.168.10.5) and c0a80a14 (192.168.10.20). When the string is assembled, it yields f108c0a80a05c0a80a14. The Cisco IOS IT Certification Guaranteed, The Easy Way! 81command that is added to the DHCP scope is option 43 hex f108c0a80a05c0a80a14.”

Reference: [Click](#)

Therefore in this question the option 43 in hex should be “F104.AC10.3205 (the management IP address of 172.16.50.5 in hex is AC.10.32.05).

268. Refer to the exhibit. Which password allows access to line con 0 for a username of “tommy” under normal operation?

```
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
```

- **A. Cisco**
- B. local
- C. 0 Cisco
- D. Tommy

Correct Answer: A

Explanation: In this question, there are two different passwords for user “tommy”: + In the TACACS+ server, the password is “Tommy” + In the local database of the router, the password is “Cisco”.

From the line “login authentication local” we know that the router uses the local database for authentication so the password should be “Cisco”.

Note: “... password 0 ...” here means unencrypted password.

269. 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

270. 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?

```
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
```

A.

```
ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 global
ip route vrf Customer 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
```

B.

```
ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customer2 ip route vrf Customer
192.168.1.200 255.255.255.255 192.168.1.1 Customer1
```

C.

```
ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customer1 ip route vrf Customer
192.168.1.200 255.255.255.255 192.168.1.1 Customer2
```

D.

```
ip route vrf Customer1 172.16.1.1 255.255.255.255 172.16.1.1 global
ip route vrf Customer 192.168.1.200 255.255.255.0 192.168.1.1 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: A

Explanation: Static routes directly between VRFs are not supported so we cannot configure a direct static route between two VRFs.

The command “ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 global” means in VRF Customer1, in order to reach destination 172.16.1.0/24 then we use the next hop IP address 172.16.1.1 in the global routing table. And the command “ip route 192.168.1.0 255.255.255.0 Vlan10” tells the router “to reach 192.168.1.0/24, send to Vlan 10”.

271. 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?

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

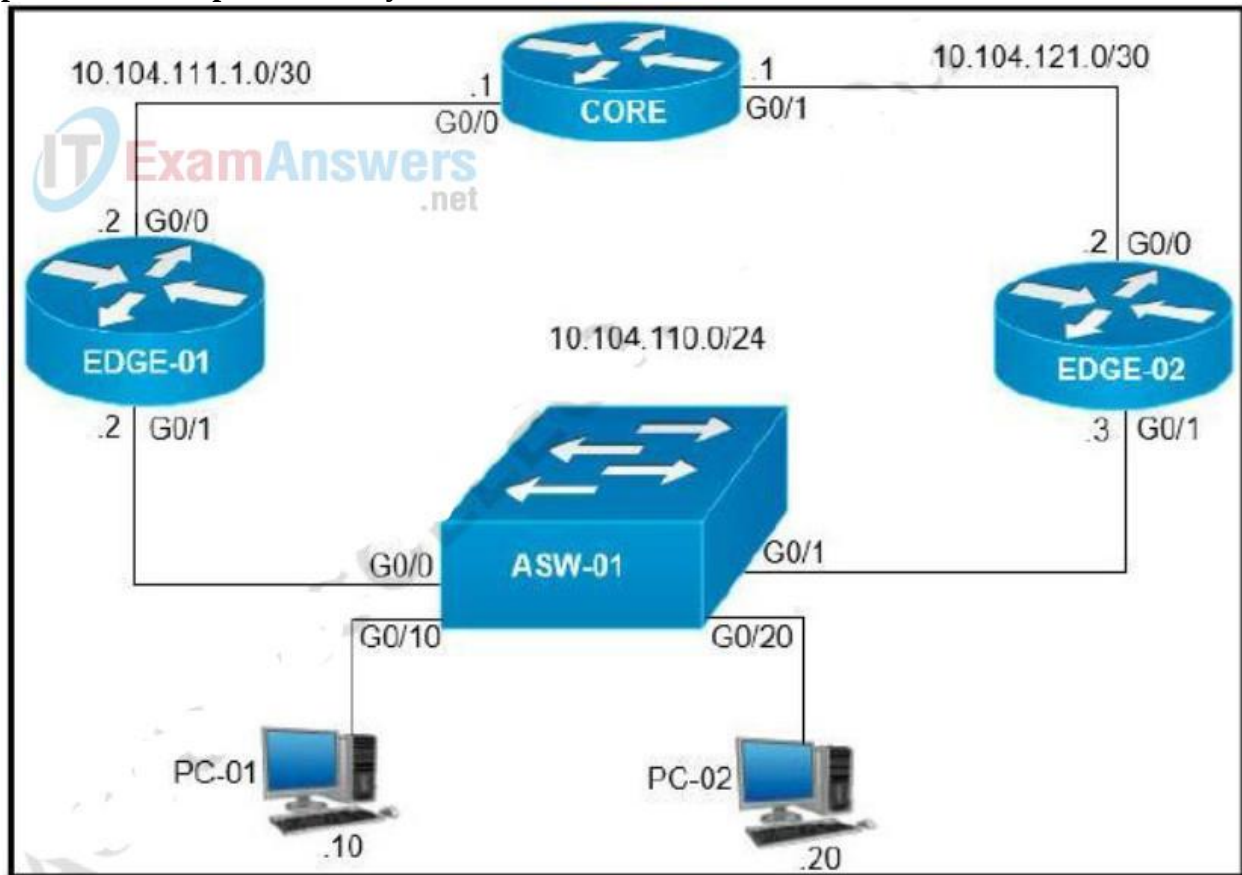
- **A. It remains in err-disabled state until the shutdown/no shutdown command is entered in the interface configuration mode.**
- B. It remains in err-disabled state until the errdisable recovery cause failed-port-state command is entered in the global configuration mode.
- C. It remains in err-disabled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

Explanation: Seems someone maybe trying to insert a switch into that port which sends bpd packets. The port is configured to not allow this so it goes into an error disable mode and shuts the port down. You have to do a shut and no shut on the port to bring it back up. However, it may go down again if the device sending bpd's is still active on the port.

272. 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

273. 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

Explanation: In SD-Access the control plane is based on LISP (Locator/ID Separation Protocol), the data plane is based on VXLAN (Virtual Extensible LAN), the policy plane is based on Cisco TrustSec, and the management plane is enabled and powered by Cisco DNA Center.

[https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#:~:text=In%20SD%](https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#:~:text=In%20SD%20)

274. An engineer is configuring GigabitEthernet1/0/0 for VRRP. When the router has the highest priority in group 5, it must assume the master role. Which command set should the engineer add to the configuration to accomplish this task?

```
interface GigabitEthernet1/0/0
description To IDF A 38-72-100-76
ip address 172.16.13.2 255.255.255.0
```

- ☐ standby 5 ip 172.16.13.254
standby 5 priority 100
standby 5 preempt
- ☐ vrrp 5 ip 172.16.13.254 255.255.255.0
vrrp 5 track 1 decrement 10
vrrp 5 preempt
- ☐ standby 5 ip 172.16.13.254
standby 5 priority 100
standby 5 track 1 decrement 10
- ☐ vrrp 5 ip 172.16.13.254
vrrp 5 priority 100

Correct Answer: B

275. 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

Explanation: There are two types of hypervisors: type 1 and type 2 hypervisor.

In type 1 hypervisor (or native hypervisor), the hypervisor is installed directly on the physical server.

Then instances of an operating system (OS) are installed on the hypervisor. Type 1 hypervisor has direct access to the hardware resources. Therefore they are more efficient than hosted architectures.

Some examples of type 1 hypervisor are VMware vSphere/ESXi, Oracle VM Server, KVM and Microsoft Hyper-V.

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

Type 1 is more efficient and well performing, it is also more secure than type 2 because the flaws and vulnerabilities that are endemic to Operating Systems are often absent from Type 1, bare metal hypervisors.

Type 1 has better performance, scalability and stability but supported by limited hardware.

276. Refer to the exhibit. What is required to configure a second export destination for IP address 192.168.10.1?

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

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

Correct Answer: B

Explanation: To configure multiple NetFlow export destinations to a router, use the following commands in global configuration mode:

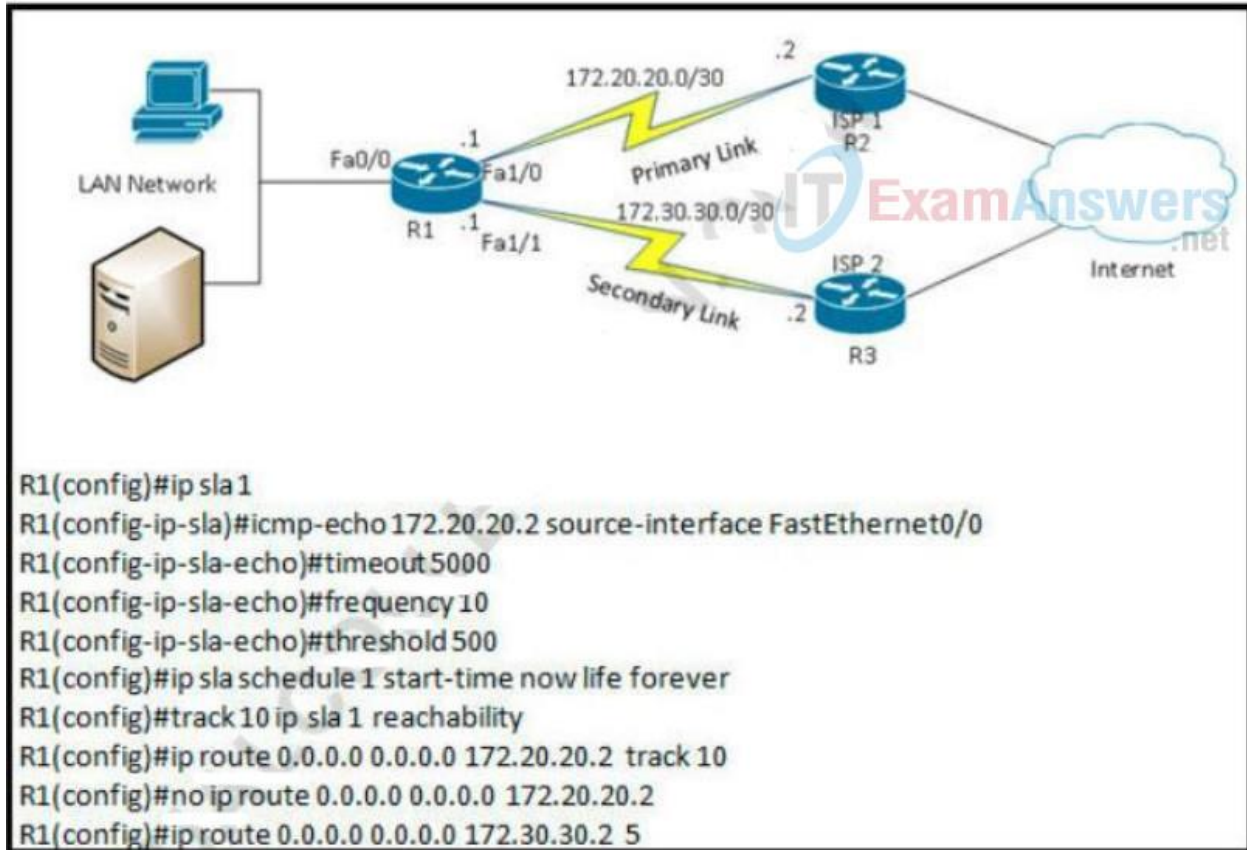
Step 1: Router(config)# ip flow-export destination ip-address udp-port

Step 2: Router(config)# ip flow-export destination ip-address udp-port

The following example enables the exporting of information in NetFlow cache entries:

ip flow-export destination 10.42.42.1 9991 ip flow-export destination 10.0.101.254 1999

277. 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: C D

278. 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

Explanation: A 401 error response indicates that the client tried to operate on a protected resource without providing the proper authorization. It may have provided the wrong credentials or none at all.

Note: answer 'HTTP Status Code 200' 4xx code indicates a "client error" while a 5xx code indicates a "server error".

Reference: <https://restfulapi.net/http-status-codes/>

279. A wireless consultant is designing a high-density wireless network for a lecture hall for 1000 students Which antenna type is recommended for this environment?

- A. sector antenna
- B. dipole antenna
- C. parabolic dish
- **D. omnidirectional antenna**

Correct Answer: D

Explanation: Directional antennas Directional antennas come in many different styles and shapes. An antenna does not offer any added power to the signal; it simply redirects the energy it receives from the transmitter. By redirecting this energy, it has the effect of providing more energy in one direction and less energy in all other directions. As the gain of a directional antenna increases, the angle of radiation usually decreases, providing a greater coverage distance but with a reduced coverage angle. Directional antennas include patch antennas and parabolic dishes. Parabolic dishes have a very narrow RF energy path, and the installer must be accurate in aiming these types of antennas at each other.



Omnidirectional antennas An omnidirectional antenna is designed to provide a 360-degree radiation pattern. This type of antenna is used when coverage in all directions from the antenna is required. The standard 2.14-dBi “rubber duck” is one style of omnidirectional antenna. Omnidirectional antenna -> Therefore Omnidirectional antenna is best suited for a high-density wireless network in a lecture hall.

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

```
Router#sh| run | b vty

line vty 0 4
  session-timeout 30
  exec-timeout 20 0
  session-limit 30
  login local
line vty 5 15
  session-timeout 30
  exec-timeout 20 0
  session-limit 30
  login local
```

A.
line vty 0 15
absolute-timeout 600

B.
line vty 0 15
exec-timeout

C.
line vty 0 15
exec-timeout 10 0

D.
line vty 0 4
exec-timeout 600
Correct Answer: C

Explanation: The “exec-timeout” command is used to configure the inactive session timeout on the console port or the virtual terminal. The syntax of this command is:

exec-timeout minutes [seconds]

Therefore we need to use the “exec-timeout 10 0” command to set the user inactivity timer to 600 seconds (10 minutes).

281. Refer to the exhibit. Which command must be applied to Routed to bring the GRE tunnel to an up/up state?

```
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#
```

- 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

Explanation: In order to make a Point-to-Point GRE Tunnel interface in up/up state, two requirements must be met: + A valid tunnel source (which is in up/up state and has an IP address configured on it) and tunnel destination must be configured + A valid tunnel destination is one which is routable. However, it does not have to be reachable.

282. 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

Explanation: First-in, first-out (FIFO): FIFO entails no concept of priority or classes of traffic. With FIFO, transmission of packets out the interface occurs in the order the packets arrive, which means no QoS.

283. Refer to the exhibit. isco 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

284. 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: B

Explanation: Root guard does not allow the port to become a STP root port, so the port is always STP-designated. If a better BPDU arrives on this port, root guard does not take the BPDU into account and elect a new STP root. Instead, root guard puts the port into the root-inconsistent STP state which is equal to a listening state. No traffic is forwarded across this port.

Reference: <http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html>

285. 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: C D E

286. Which DHCP option provides the CAPWAP APs with the address of the wireless controller(s)?

- **A. 43**
- B. 66
- C. 69
- D. 150

Correct Answer: A

Explanation: DHCP option 43 is an option used for providing Wireless LAN Controller IP addresses to the AP. The DHCP option 43 is used to notify the AP to convert into CAPWAP AP.

287. 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

Explanation: SDA Roaming 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.

Intra-xTR

When a client on a fabric enabled WLAN, roams from an access point to another access point on the same access-switch, it is called Intra-xTR. Here, the local client database and client history table are updated with the information of the newly associated access point.

Inter-xTR.

When a client on a fabric enabled WLAN, roams from an access point to another access point on a different access-switch, it is called Inter-xTR.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/mobility.html

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

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

Correct Answer: C

Explanation: Access Points

+ AP is directly connected to FE (or to an extended node switch)

+ AP is part of Fabric overlay

289. 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

Explanation: Fabric mode APs continue to support the same wireless media services that traditional APs support;

apply AVC, quality of service (QoS), and other wireless policies; and establish the CAPWAP

control plane to the fabric WLC. Fabric APs join as local-mode APs and must be directly connected to the fabric edge node switch to enable fabric registration events, including RLOC assignment via the fabric WLC. The fabric edge nodes use CDP to recognize APs as special wired hosts, applying special port configurations and assigning the APs to a unique overlay network within a common EID space across a fabric. The assignment allows management simplification by using a single subnet to cover the AP infrastructure at a fabric site.

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

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

```
DSW2#sh spanning-tree vlan 10

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

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

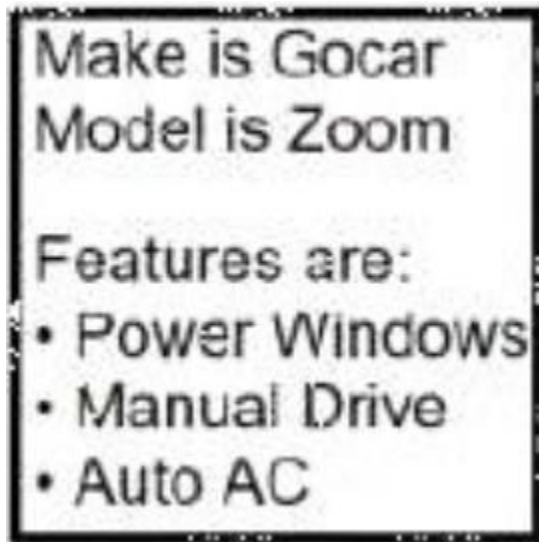
Interface                Role Sts Cost      Prio.Nbr Type
-----
Fa1/0/7                  Desg FWD 2       128.9    P2p Peer (STP)
Fa1/0/10                  Desg FWD 4       128.12   P2p Peer (STP)
Fa1/0/11                  Desg FWD 2       128.13   P2p Peer (STP)
Fa1/0/12                  Desg FWD 2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

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

Correct Answer: A

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

291. 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

Explanation: JSON syntax structure: + uses curly braces {} to hold objects and square brackets [] to hold arrays + JSON data is written as key/value pairs + A key/value pair consists of a key (must be a string in double quotation marks ""), followed by a colon :, followed by a value. For example: "name": "John" + Each key must be unique + Values must be of type string, number, object, array, boolean or null + Multiple key/value within an object are separated by commas , JSON can use arrays. Arrays are used to store multiple values in a single variable. For example:

```
{  
  "name": "John",  
  "age": 30,  
  "cars": [ "Ford", "BMW", "Fiat" ]  
}
```

In the above example, "cars" is an array which contains three values "Ford", "BMW" and "Fiat".

Note: Although our correct answer above does not have curly braces to hold objects but it is still

the best choice here.

```
{  
  "Make": "Gocar",  
  "Model": "Zoom",  
  "Features": ["Power Windows", "Manual Dnve", "Auto AC"]  
}
```

Results

valid JSON

292. 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: A

Explanation: If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the syslog servers. For example, if you set the syslog level to Notifications (severity level 5), only those messages whose severity is between 0 and 5 are sent to the syslog servers.

<https://www.cisco.com/c/en/us/support/docs/wireless/4100-series-wireless-lan-controllers/107252-WLC-Syslog-Server.html>

293. 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

Explanation: When using Ternary Content Addressable Memory (TCAM) inside routers it's used for faster address lookup that enables fast routing.

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

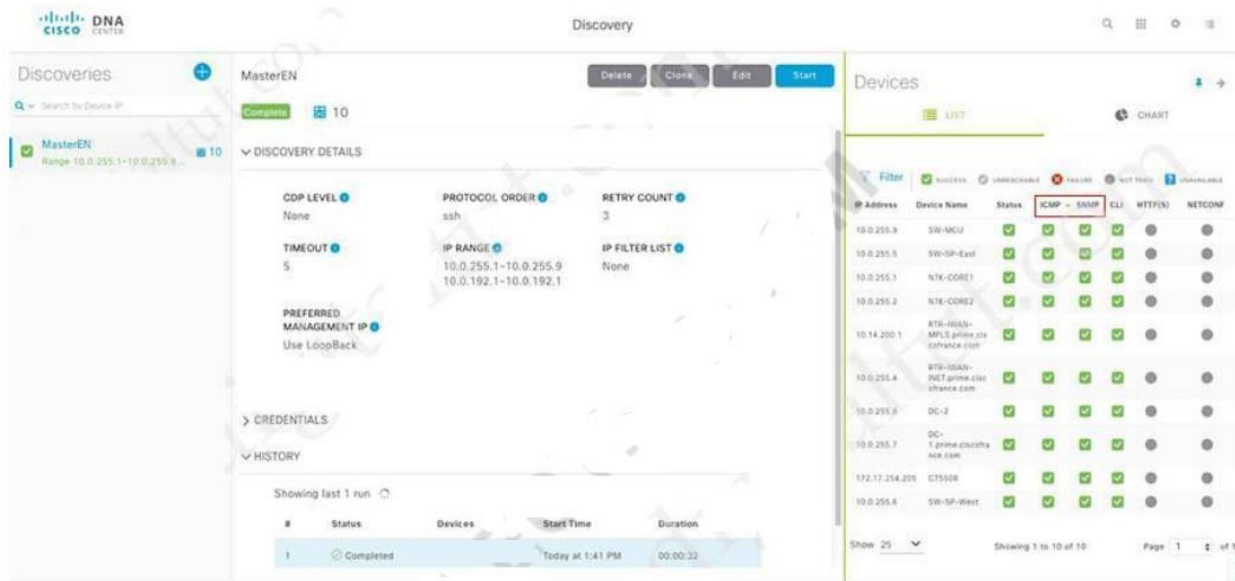
Besides Longest-Prefix Matching, TCAM in today's routers and multilayer Switch devices are used to store ACL, QoS and other things from upper-layer processing.

294. Which two southbound interfaces originate from Cisco DNA Center and terminate at fabric underlay switches? (Choose two)

- **A. ICMP: Discovery**
- B. UDP 67: DHCP
- C. TCP 23: Telnet
- D. UDP 6007: NetFlow
- **E. UDP 162: SNMP**

Correct Answer: A E

Explanation: In the figure below, we can see ICMP & SNMP can reach to underlay switches.



295. What is the function of a control-plane node in a Cisco SD-Access solution?

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

Correct Answer: A

Explanation: 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

Reference: [Click here](#)

296. 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. NSF**
- C. BFD
- D. RP failover

Correct Answer: B

297. 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

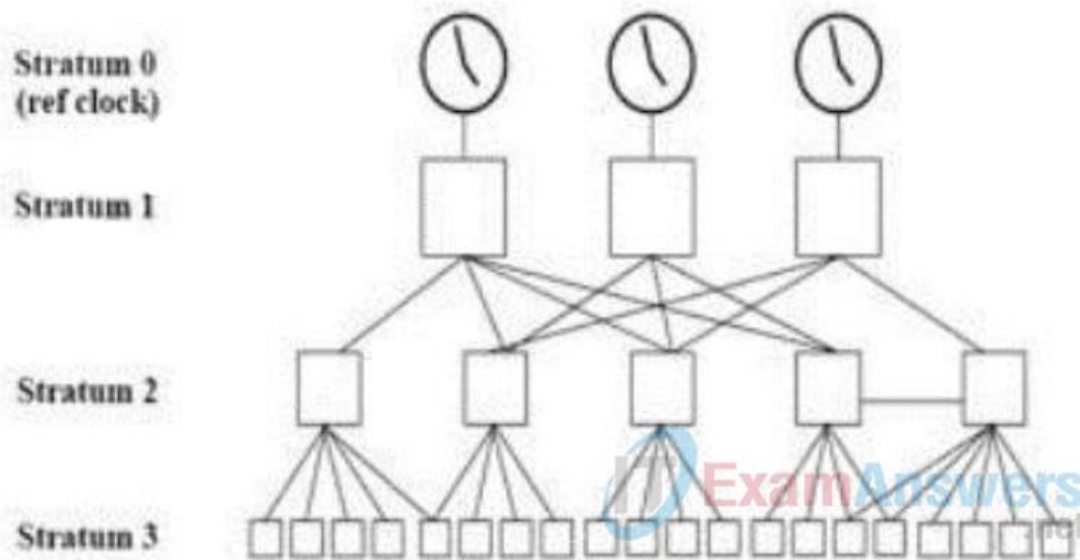
Explanation: If you have Cisco SD-Access implemented and DNA Center becomes unreachable then the wired and wireless network will continue to forward packets as usual. There will be no impact to network performance or behavior. Yes you will be able to SSH / telnet / console into switches and wireless network infrastructure as usual. For the period DNA Center is unreachable, Assurance data will be lost, and you will not be able to make configuration changes to the Cisco SD-Access network.

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

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

Correct Answer: C

Explanation: The stratum levels define the distance from the reference clock. A reference clock is a stratum 0 device that is assumed to be accurate and has little or no delay associated with it. Stratum 0 servers cannot be used on the network but they are directly connected to computers which then operate as stratum-1 servers. A stratum 1 time server acts as a primary network time standard.



A stratum 2 server is connected to the stratum 1 server; then a stratum 3 server is connected to the stratum 2 server and so on. A stratum 2 server gets its time via NTP packet requests from a stratum 1 server. A stratum 3 server gets its time via NTP packet requests from a stratum-2 server...

299. What is a characteristic of a next-generation firewall?

- A. only required at the network perimeter
- B. required in each layer of the network
- C. filters traffic using Layer 3 and Layer 4 information only
- **D. provides intrusion prevention**

Correct Answer: D

Explanation: A next generation firewall adds additional features such as application control, integrated intrusion prevention (IPS) and often more advanced threat prevention capabilities like sandboxing.

300. Which two components are supported by LISP? (choose two)

- **A. proxy ETR**
- **B. egress tunnel router**
- C. route reflector

- D. HMAC algorithm
- E. spoke

Correct Answer: A B

Explanation: [Click here](#)

An Egress Tunnel Router (ETR) connects a site to the LISP-capable part of a core network (such as the Internet), publishes EID-to-RLOC mappings for the site, responds to MapRequest messages, and decapsulates and delivers LISP-encapsulated user data to end systems at the site.

A LISP proxy ETR (PETR) implements ETR functions on behalf of non-LISP sites. A PETR is typically used when a LISP site needs to send traffic to non-LISP sites but the LISP site is connected through a service provider that does not accept nonroutable EIDs as packet sources. PETRs act just like ETRs but for EIDs that send traffic to destinations at non-LISP sites

301. 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 OCA 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: A C

Explanation: In the 5GHz spectrum some of the channels used by 802.11 are subject to Dynamic Frequency Selection (DFS) requirements. This is due to our clients coexistence with other RF technologies such as Maritime, Aviation and Weather RADAR.

Dynamic Frequency Selection (DFS) is the process of detecting radar signals that must be protected against interference from 5.0 GHz (802.11a/h) radios, and upon detection switching the operating frequency of the 5.0 GHz (802.11a/h) radio to one that is not interfering with the radar systems.

Reference: [Click here](#)

Although DFS helps reduce interference with radar systems but “DFS channels” refer to the 5GHz channels that require DFS check. In other words, DFS channels are channels that may interfere with radar signal.

Therefore we should disable these DFS channels -> Answer C is correct.

UNII-2 (5.250-5.350 GHz and 5.470-5.725 GHz) which contains channels 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, and 140 are permitted in the United States, but shared with radar systems.

Therefore, APs operating on UNII-2 channels are required to use Dynamic Frequency Selection (DFS) to avoid interfering with radar signals. If an AP detects a radar signal, it must immediately stop using that channel and randomly pick a new channel.

Reference: [Click here](#)

302. Refer to the exhibit. What does the output confirm about the switch's spanning tree configuration?

```
Root ID    Priority    24596
Address    001b.7363.4300
Cost       2
Port       13 (FastEthernet1/0/11)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

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

Interface Role Sts Cost Prio.Mbr 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

VLAN 20
Spanning tree enabled protocol ieee
```

- 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 PVST+.**
- D. The spanning-tree operation mode for this switch is IEEE

Correct Answer: C

Explanation: The default spanning-tree mode in Cisco switch is PVST+. This spanning-tree mode is based on the IEEE 802.1D standard and Cisco proprietary extensions. PVST+ is same as standard IEEE 802.1D but it runs on each VLAN. In the output we see the line “Spanning tree enabled protocol ieee” under “VLAN 20” so it can say the switch is running in PVST+ mode.

303. 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

Explanation: OSPF maintains information about all the networks and running routers in its area. Each time there is a change within the area, all routers need to re-sync their database and then run SPF again. This process makes it more CPU intensive. EIGRP, on the other hand, has triggered and incremental updates. Therefore EIGRP is more efficient in terms of CPU usage and memory.

304. 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 allows the host hardware to be directly accessed**
- D. Para-virtualization lacks support for containers

Correct Answer: C

Explanation: Paravirtualization works differently from the full virtualization. It doesn't need to simulate the hardware for the virtual machines. The hypervisor is installed on a physical server (host) and a guest OS is installed into the environment. Virtual guests aware that it has been virtualized, unlike the full virtualization (where the guest doesn't know that it has been virtualized) to take advantage of the functions.

In full virtualization, guests will issue a hardware calls but in paravirtualization, guests will directly communicate with the host (hypervisor) using drivers.

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

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

Correct Answer: C

306. 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

Explanation: Unlike HSRP or GLBP, VRRP is an open standard. Only VRRPv3 supports both IPv4 and IPv6.

307. Which unit measures the power of a radio signal with reference to 1 milliwatt?

- A. dBw
- **B. dBm**
- C. mW
- D. dBi

Correct Answer: B

Explanation: dBm is an abbreviation for “decibels relative to one milliwatt,” where one milliwatt (1 mW) equals 1/1000 of a watt. It follows the same scale as dB. Therefore 0 dBm = 1 mW, 30 dBm = 1 W, and -20 dBm = 0.01 mW

308. 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

Explanation: MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1x Extensible Authentication Protocol (EAP-TLS) or Pre Shared Key (PSK) framework.

309. Refer to the exhibit. What happens to access interfaces where VLAN 222 is assigned?

```

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

```

- A. STP BPDU guard is enabled
- B. A description "RSPAN" is added
- **C. They are placed into an inactive state**
- D. They cannot provide PoE

Correct Answer: C

Explanation:

```

SW5#sh int status

```

Port	Name	Status	Vlan	Duplex	Speed	Type
Et0/0		connected	trunk	a-full	auto	RJ45
Et0/1		notconnect	1	auto	auto	RJ45
Et0/2		notconnect	1	auto	auto	RJ45
Et0/3		inactive	222	a-full	auto	RJ45
Po5		notconnect	unassigned	auto	auto	

Access ports (including voice VLAN ports) on the RSPAN VLAN are put in the inactive state.

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

```

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

```

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

Correct Answer: C

311. 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. Fabric endpoints are connected directly to the border node
- C. Traffic within the fabric always goes through the control plane 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: A D

Explanation: There are five basic device roles in the fabric overlay:

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

312. 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 SDWAN 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

Explanation: Data policy operates on the data plane in the Cisco SD-WAN overlay network and affects how data traffic is sent among Cisco SD-WAN devices in the network. The Cisco SD-WAN architecture defines two types of data policy, centralized data policy, which controls the flow of data traffic based on the IP header fields in the data packets and based on network segmentation, and localized data policy, which controls the flow of data traffic into and out of interfaces and interface queues on the devices.

Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/tech_notes/sda_fabric_troubleshooting/b_cisco_sda_fabric_troubleshooting_guide.html

313. Refer to the exhibit. What step resolves the authentication issue?

TYPE	PROT	SYSTEM IP	ID	ID	PRIVATE IP			
PUBLIC IP				PORT	LOCAL COLOR	PROXY	STATE	UPTIME

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			

POST ▼ https://192.168.100.80:12442/i_security_check

Params Authorization Headers (8) **Body** Pre-request Script Tests Settings

☐ none ☐ form-data ☒ x-www-form-urlencoded ☐ raw ☐ binary ☐ GraphQL

KEY	VALUE	DESCRIPTION
☒ i_username	admin	
☒ i_password	admin	

Key Value Description

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*

- A. use basic authentication
- B. change the port to 12446
- **C. target 192.168.100.82 in the URI**
- D. restart the vsmart host

Correct Answer: C

Explanation: The first figure is the output of the “show control connections” command. From this figure we learned that the 192.168.100.82 so we need to connect to this IP address (not 192.168.100.80).

314. Refer to the exhibit. Which action resolves the EtherChannel issue between SW2 and SW3?

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	Pol(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	Pol(SD)	LACP	Gi0/0(I) Gi0/1(I)

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

Correct Answer: D

315. Refer to the exhibit. 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)

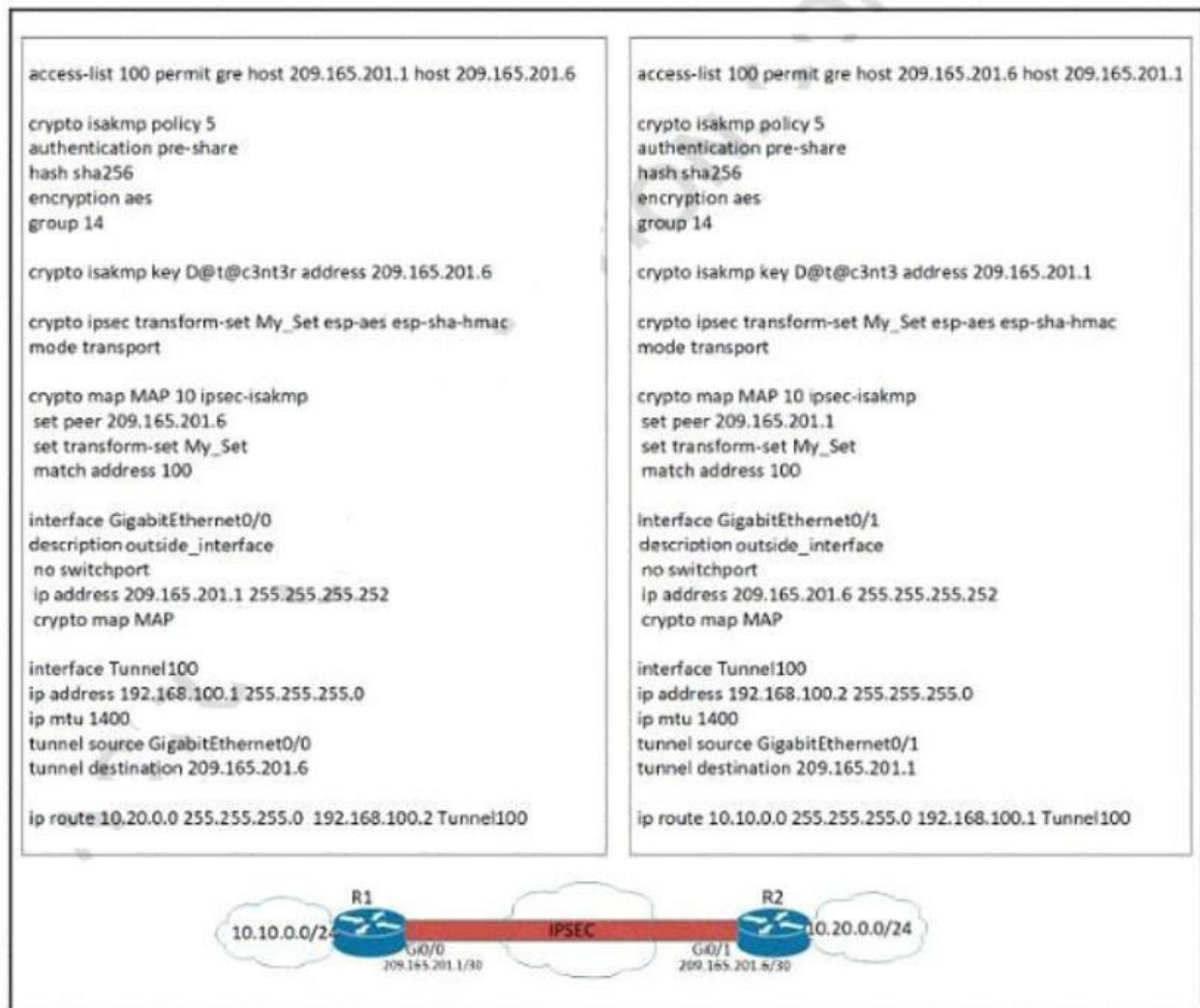
```
Current configuration : 142 bytes
vrf definition STAFF
!
!
interface GigabitEthernet1
 vrf forwarding STAFF
 no ip address
 negotiation auto
 no mop enabled
 no mop sysid
end
```

- 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: B E

316. Refer to the exhibit. 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. Create an IPsec profile, associate the transform-set, and apply the profile to the tunnel interface.**
- 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. Remove all configuration related to crypto map from R1 and R2 and eliminate the ACL 100**

Correct Answer: B D

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



```
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
```

A)

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

B)

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

C)

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

D)

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

- **A. Option A**

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

Correct Answer: A

318. Which encryption hashing algorithm does NTP use for authentication?

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

Correct Answer: B

Explanation: An example of configuring NTP authentication is shown below:

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

319. What is a VPN in a Cisco SD-WAN deployment?

- A. common exchange point between two different services
- B. attribute to identify a set of services offered in specific places in the SD-WAN fabric
- **C. virtualized environment that provides traffic isolation and segmentation in the SD-WAN fabric**
- D. virtual channel used to carry control plane information

Correct Answer: C

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

- A. host
- B. mainframe
- C. container
- **D. virtual machine**

Correct Answer: D

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

- A. Increase minimum mandatory data rate
- **B. Reduce AP transmit power**
- **C. Disable 2.4 GHz and use only 5 GHz.**

- D. Enable Fastlane.
- E. Reduce channel width from 40 MHz to 20 MHz

Correct Answer: B C

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

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

Correct Answer: A

Explanation: DNA Controller – Enterprise SDN Controller (e.g. DNA Center) provides GUI management and abstraction via Apps that share context

Identity Services – External ID System(s) (e.g. ISE) are leveraged for dynamic Endpoint to Group mapping and Policy definition

Analytics Engine – External Data Collector(s) (e.g. NDP) are leveraged to analyze Endpoint to App flows and monitor fabric status

Reference: https://www.cisco.com/c/dam/global/da_dk/assets/training/seminaria-materials/Software_Defined_Access_2017.pdf

323. Which deployment option of Cisco NGFW provides scalability?

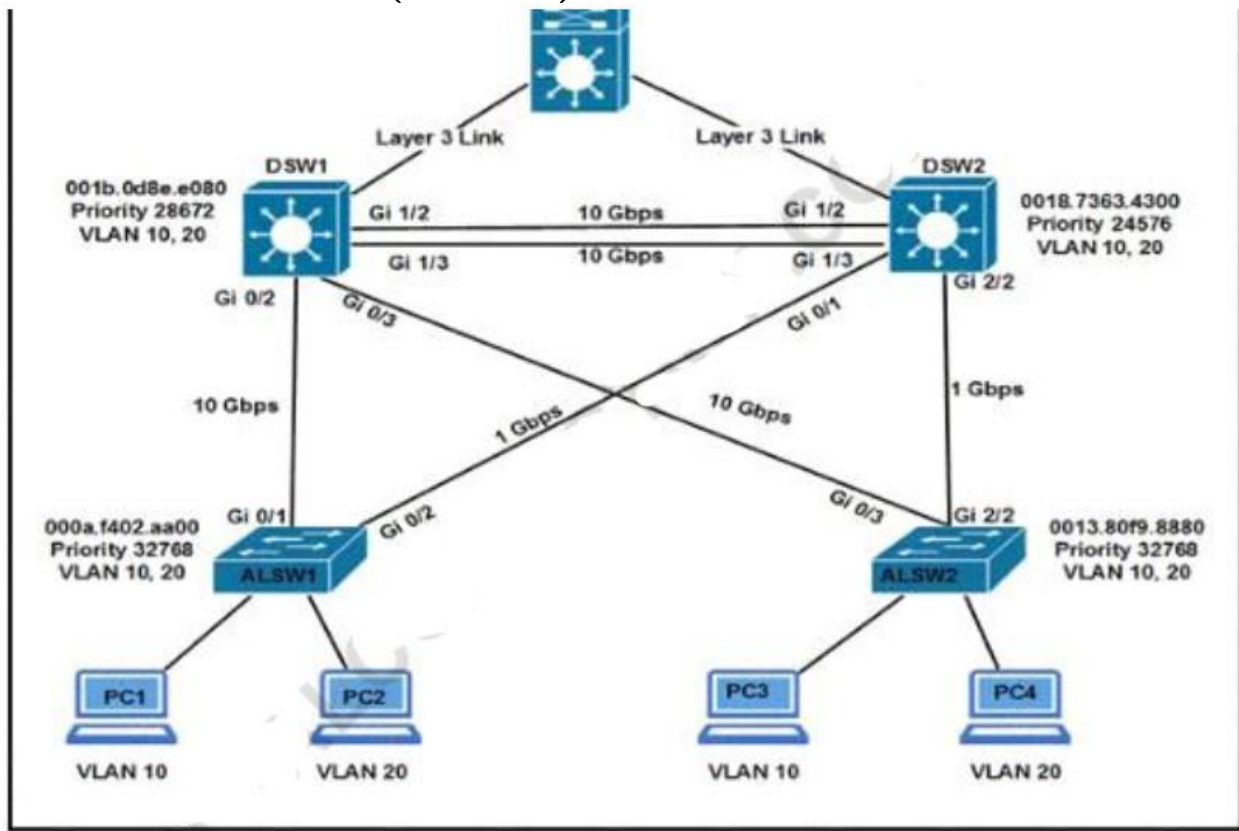
- **A. clustering**
- B. Inline tap
- C. high availability
- D. tap

Correct Answer: A

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

324. Refer to the exhibit. All switches are configured with the default port priority value. Which two commands ensure that traffic from PC1 is forwarded over Gi1/3 trunk port

between DWS1 and DSW2? (Choose two)



- A. DSW2(config-if)#spanning-tree port-priority 128
- **B. DSW2(config-if)#spanning-tree port-priority 16**
- **C. DSW2(config-if)#interface gi1/3**
- D. DSW1(config-if)#interface gi1/3
- E. DWS1(config-if)#spanning-tree port-priority 0

Correct Answer: BC

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

- A. provide QoS prioritization services such as marking, queueing, and classification for critical network traffic
- **B. provide redundant Layer 3 point-to-point links between the core devices for more predictable and faster convergence**
- C. provide advanced network security features such as 802.1X, DHCP snooping, VACLs, and port security
- D. provide redundant aggregation for access layer devices and first-hop redundancy protocols such as VRRP

Correct Answer: B

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

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

Correct Answer: B E

327. 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

Correct Answer: A C

328. Which data is properly formatted with JSON?

A)

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

B)

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

C)

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

D)

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

- A. Option
- B. Option

- **C. Option**
- D. Option

Correct Answer: C

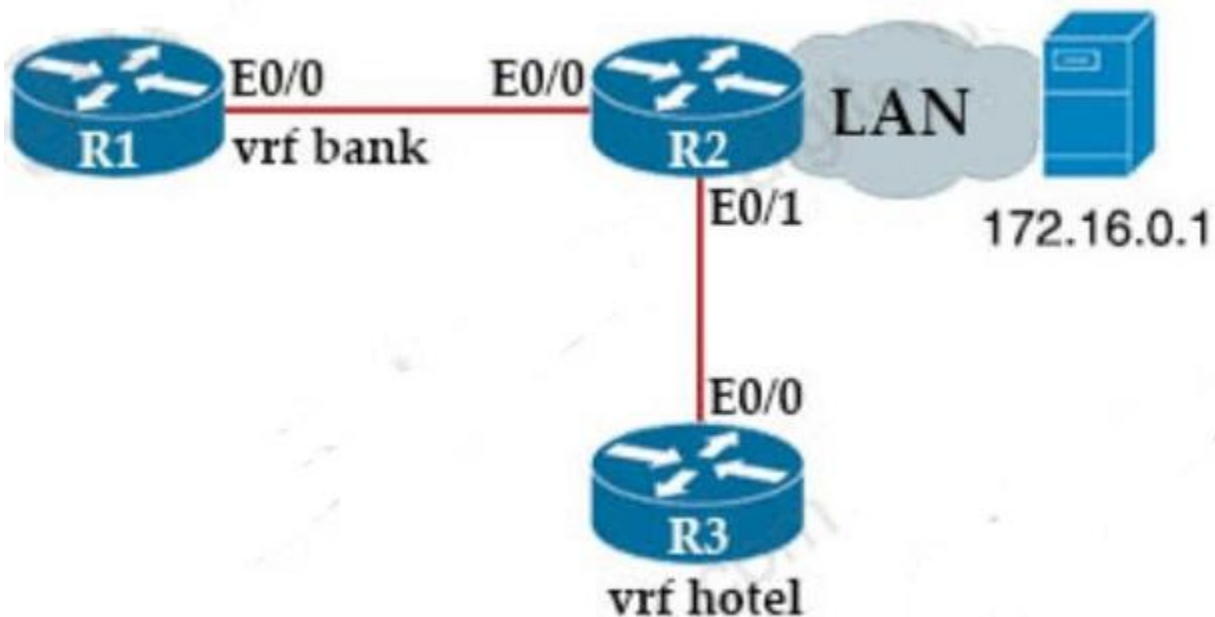
329. Which outcome is achieved with this Python code?

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

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

Correct Answer: C

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



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
```

Option 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	Option B 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
Option C 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	Option 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

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

Correct Answer: C

331. 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 14:55:23"
  ]
}
```

A)

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

B)

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

C)

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

D)

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

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

Correct Answer: D

332. What is YANG used for?

- A. scraping data via CLI
- B. processing SNMP read-only polls
- **C. describing data models**
- D. providing a transport for network configuration data between client and server

Correct Answer: C

Explanation: YANG is used to model each protocol based on RFC 6020.

Reference: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/datamodels/configuration/xen-16/data-models-xe-16-book/yang-netconf.html>

333. Refer to the exhibit. Which JSON syntax is derived from this data?

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

A)

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

B)

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

C)

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

D)

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

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

Correct Answer: D

334. Refer to the exhibit. Which two facts does the device output confirm? (Choose two)

```
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-Vl503-1" (default)
```

- **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: A B

335. 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 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

Explanation: The %TUN-5-RECURDOWN: Tunnel0 temporarily disabled due to recursive routing error message means that the generic routing encapsulation (GRE) tunnel router has discovered a recursive routing problem. This condition is usually due to one of these causes:
+ A misconfiguration that causes the router to try to route to the tunnel destination address using the tunnel interface itself (recursive routing)
+ A temporary instability caused by route flapping elsewhere in the network
Reference: <https://www.cisco.com/c/en/us/support/docs/ip/enhan>

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

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

Correct Answer: C D

Explanation: In a Cisco Unified Wireless network, the LAPs must first discover and join a WLC before they can service wireless clients.

However, this presents a question: how did the LAPs find the management IP address of the controller when it is on a different subnet?

If you do not tell the LAP where the controller is via DHCP option 43, DNS resolution of “Cisco-capwap-controller.local_domain”, or statically configure it, the LAP does not know where in the network to find the management interface of the controller.

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

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

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

Correct Answer: B

Explanation: Cisco Stealthwatch is a comprehensive, network telemetry-based, security monitoring and analytics solution that streamlines incident response through behavioral analysis; detecting denial of service attacks, anomalous behaviour, malicious activity and insider threats. Based on a scalable enterprise architecture, Stealthwatch provides near real-time situational awareness of all users and devices on the network.

Reference: <https://www.endace.com/cisco-stealthwatch-solution-brief.pdf>

Note: Although answer A seems to be correct but in fact, Stealthwatch does not provide real-time protection for DDoS attack. It just helps detect DDoS attack only.

Stealthwatch aggregates observed network activity and performs behavioral and policy driven analytics against what it sees in order to surface problematic activities. While we don't position our self as a DDOS solution, we're going to leverage our analytical capabilities to identify a DDoS attack against an internal host using the WebUI.

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2016/pdf/LTRSEC-8421-LG.pdf>

338. How does Protocol Independent Multicast function?

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

Correct Answer: C

Explanation: Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the reverse path forwarding (RPF) check function instead of building up a completely independent multicast routing table. Unlike other routing protocols, PIM does not send and receive routing updates between routers.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xen-16/imc-pim-xe-16-book/imc-tech-overview.html

339. 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 traffic classification and marking conditions
- **D. under interface saturation conditions**

Correct Answer: D

340. 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

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

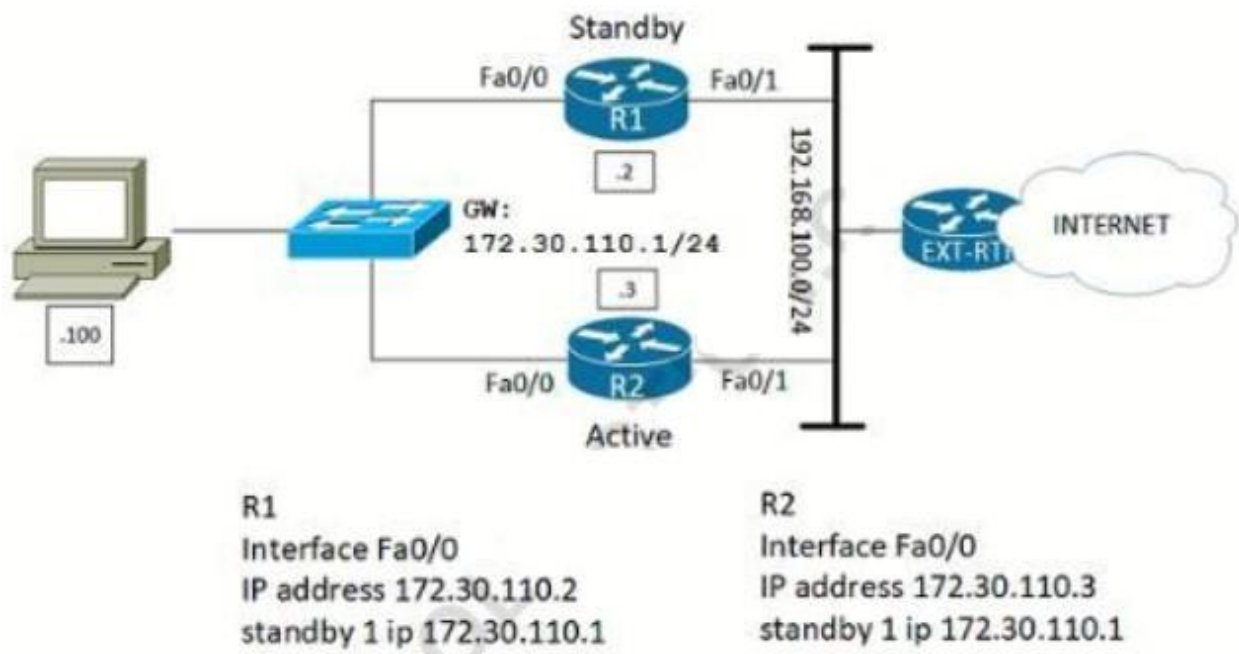
341. A company has an existing Cisco 5520 HA cluster using SSO. An engineer deploys a new single Cisco Catalyst 9800 WLC to test new features. The engineer successfully configures a mobility tunnel between the 5520 cluster and 9800 WLC. Clients connected to the corporate WLAN roam seamlessly between 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: B

342. 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?



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

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

Correct Answer: A

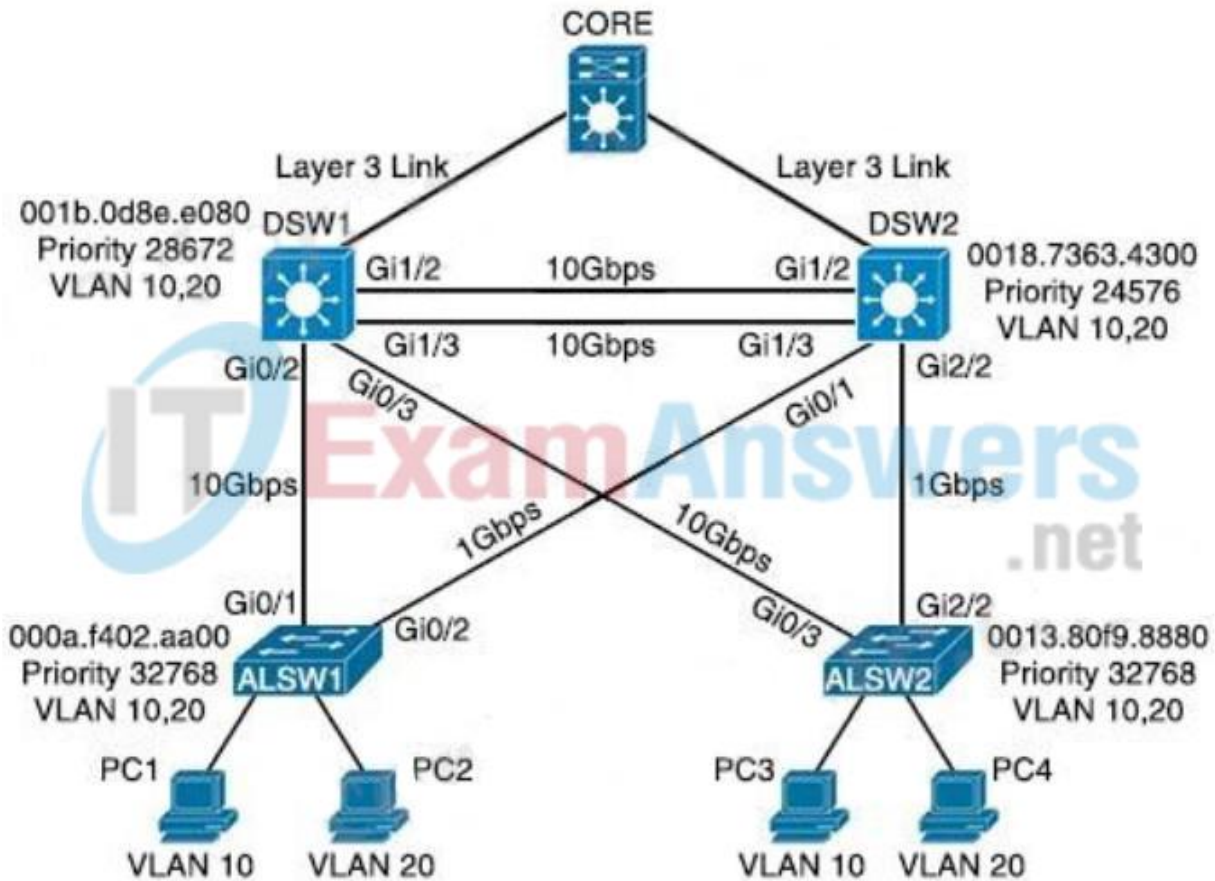
343. What are two methods of ensuring that the multicast RPF check passes without changing the unicast routing table? (Choose two.)

- **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: A C

Explanation: [Click here](#)

344. Refer to the exhibit. How to make DSW1 the primary root for VLAN 10? (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: A C

Explanation: Maybe something was wrong with this question but we still have to choose the best answers.

345. 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

346. 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.

Answer: A

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

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

Answer: B

Explanation: VXLAN adds 50 bytes to the original packet. 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. Devices in the same routing domain and Layer 2 domain should be configured with a consistent MTU size to support routing protocol adjacencies and packet forwarding without fragmentation.

348. 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

Answer: C

Explanation: Live migration refers to the process of moving a running virtual machine or application between different physical machines without disconnecting the client or application. Memory, storage, and network connectivity of the virtual machine are transferred from the original guest machine to the destination. An example of live migration tool is VMware vSphere vMotion.

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

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

Answer: C,D

Explanation: The following are restrictions for Flexible NetFlow:

+ Traditional NetFlow (TNF) accounting is not supported.
+ Flexible NetFlow v5 export format is not supported, only NetFlow v9 export format is supported.

+ Both ingress and egress NetFlow accounting is supported.

+ Microflow policing feature shares the NetFlow hardware resource with FNF.

+ Only one flow monitor per interface and per direction is supported.

When configuring NetFlow, follow these guidelines and restrictions:

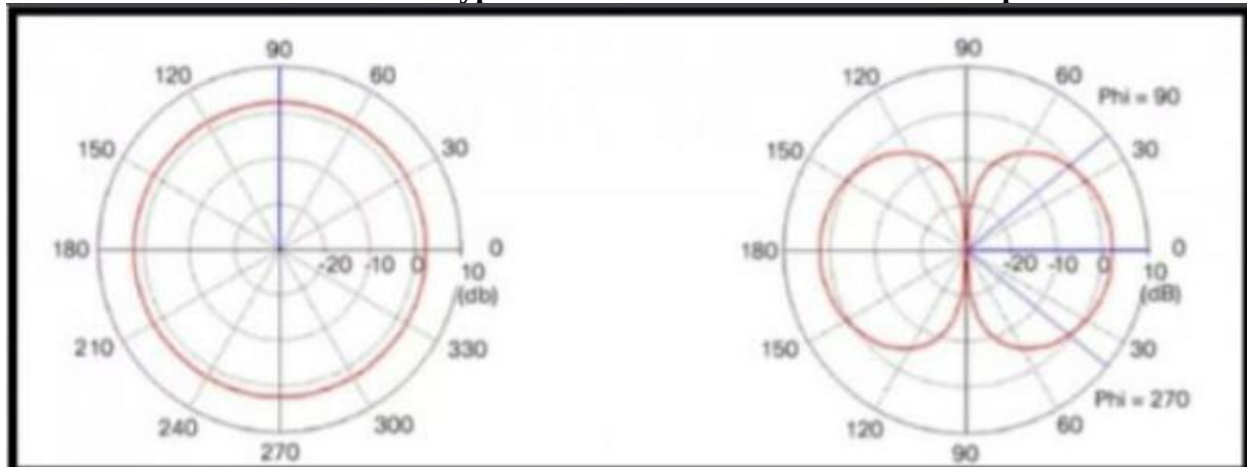
+ Except in PFC3A mode, NetFlow supports bridged IP traffic. PFC3A mode does not support NetFlow bridged IP traffic.

+ NetFlow supports multicast IP traffic.

The Flexible NetFlow – MPLS Egress NetFlow feature allows you to capture IP flow information for packets that arrive on a router as Multiprotocol Label Switching (MPLS) packets and are transmitted as IP packets.

This feature allows you to capture the MPLS VPN IP flows that are traveling through the service provider backbone from one site of a VPN to another site of the same VPN.

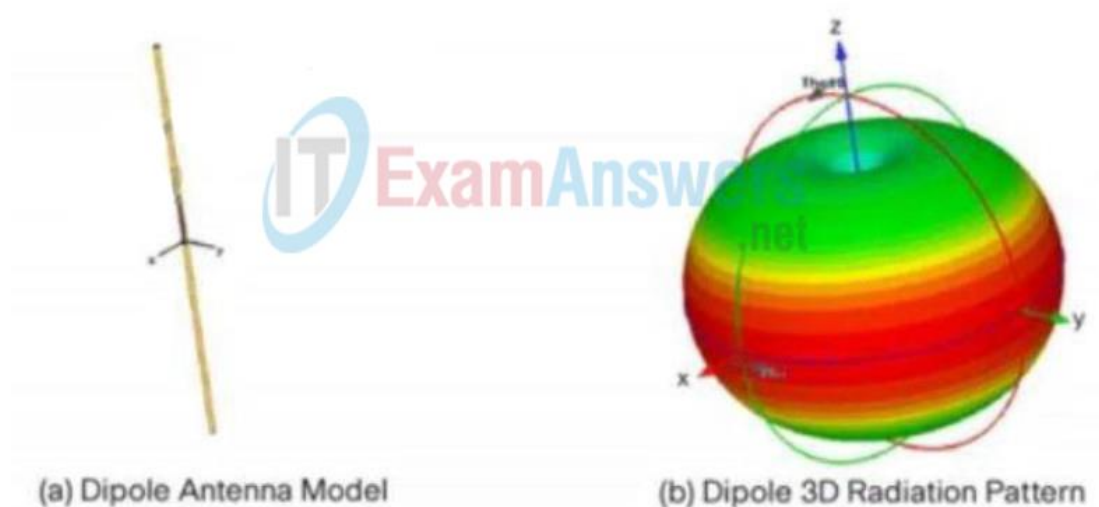
350. Refer to the exhibit. Which type of antenna is show on the radiation patterns?



- **A. Dipole**
- B. Yagi
- C. Patch
- D. Omnidirectional

Answer: A

Explanation: A dipole antenna most commonly refers to a half-wavelength ($\lambda/2$) dipole. The physical antenna (not the package that it is in) is constructed of conductive elements whose combined length is about half of a wavelength at its intended frequency of operation. This is a simple antenna that radiates its energy out toward the horizon (perpendicular to the antenna). The patterns shown are those resulting from a perfect dipole formed with two thin wires oriented vertically along the z axis.



351. What is the wireless received signal strength indicator?

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

Answer: D

Explanation: RSSI, or “Received Signal Strength Indicator,” is a measurement of how well your device can hear a signal from an access point or router. It’s a value that is useful for determining if you have enough signal to get a good wireless connection.

This value is measured in decibels (dBm) from 0 (zero) to -120 (minus 120). The closer to 0 (zero) the stronger the signal is which means it’s better, typically voice networks require a -65db or better signal level while a data network needs -80db or better.

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

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

Answer: A

353. Which protocol is implemented to establish secure control plane adjacencies between Cisco SD-WAN nodes?

- A. IKE
- **B. DTLS**
- C. IPsec
- D. ESP

Answer: B

Explanation: The Cisco SD-WAN control plane has been designed with network and device security in mind. 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.

Reference:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/securitybook/security-overvi>

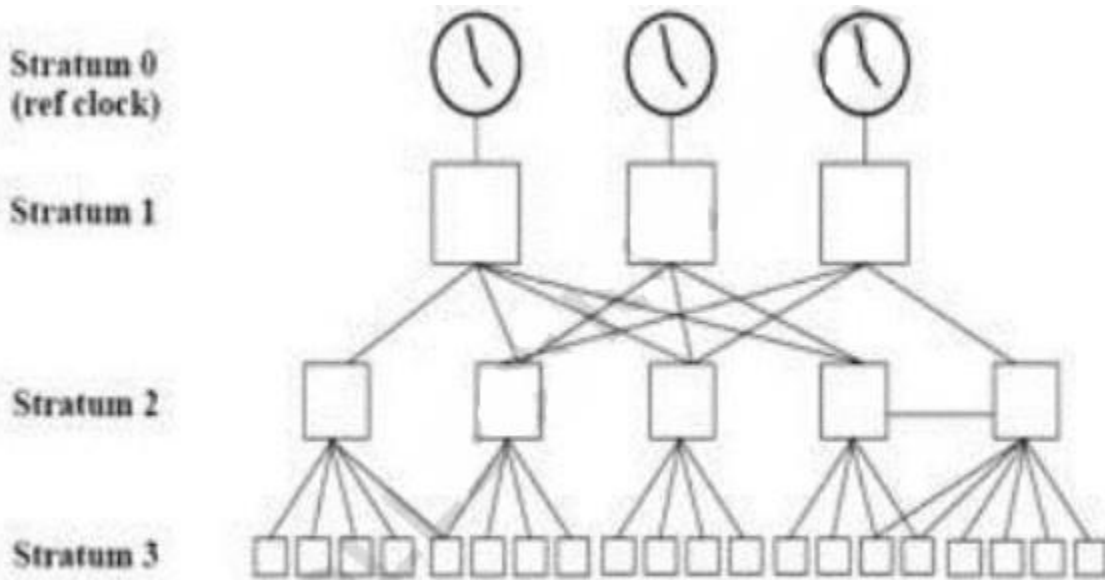
354. What does the number in an NTP stratum level represent?

- A. The number of hops it takes to reach the master time server.
- **B. The number of hops it takes to reach the authoritative time source.**
- C. The amount of offset between the device clock and true time.
- D. The amount of drift between the device clock and true time.

Answer: B

Explanation: NTP uses the concept of a stratum to describe how many hops (routers) away a machine is from an authoritative time source, usually a reference clock. A reference clock is a stratum 0 device that is assumed to be accurate and has little or no delay associated with it. Stratum 0 servers cannot be used on the network but they are directly connected to computers which then operate as stratum-1 servers. A stratum 1 time server acts as a primary network time

standard.



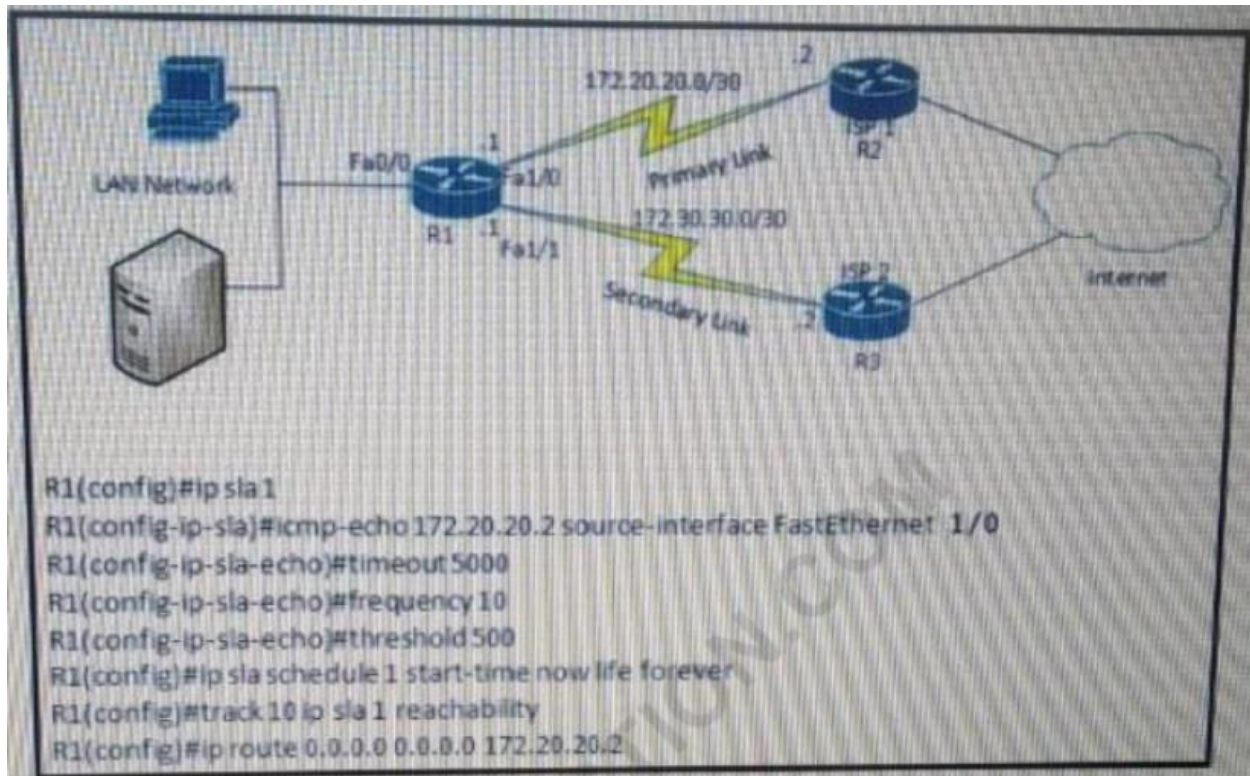
355. Refer to the exhibit. What is the effect of introducing the sampler feature into the Flexible NetFlow configuration on the router?

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

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

Answer: C

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



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

Answer: C

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

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

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

Answer: A

Explanation: vbond-as-stun-server:

Enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the vEdge router is located behind a NAT (on vEdge routers only).

When you configure this command, vEdge routers can exchange their public IP addresses and port numbers over private TLOCs.

With this configuration, the vEdge router uses the vBond orchestrator as a STUN server, so the router can determine its public IP address and public port number. (With this configuration, the router cannot learn the type of NAT that it is behind.)

No overlay network control traffic is sent and no keys are exchanged over tunnel interface configured to the vBond orchestrator as a STUN server. However, BFD does come up on the tunnel, and data traffic can be sent on it.

Answer: A

358. 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

Answer: C

Explanation: A stack master retains its role unless one of these events occurs:

The switch stack is reset.*

The stack master is removed from the switch stack.

The stack master is reset or powered off.

The stack master fails.

The switch stack membership is increased by adding powered-on standalone switches or switch stacks.*

In the events marked by an asterisk (*), the current stack master might be re-elected based on the listed factors.

When you power on or reset an entire switch stack, some stack members might not participate in the stack master election. Stack members that are powered on within the same 20-second time frame participate in the stack master election and have a chance to become the stack master.

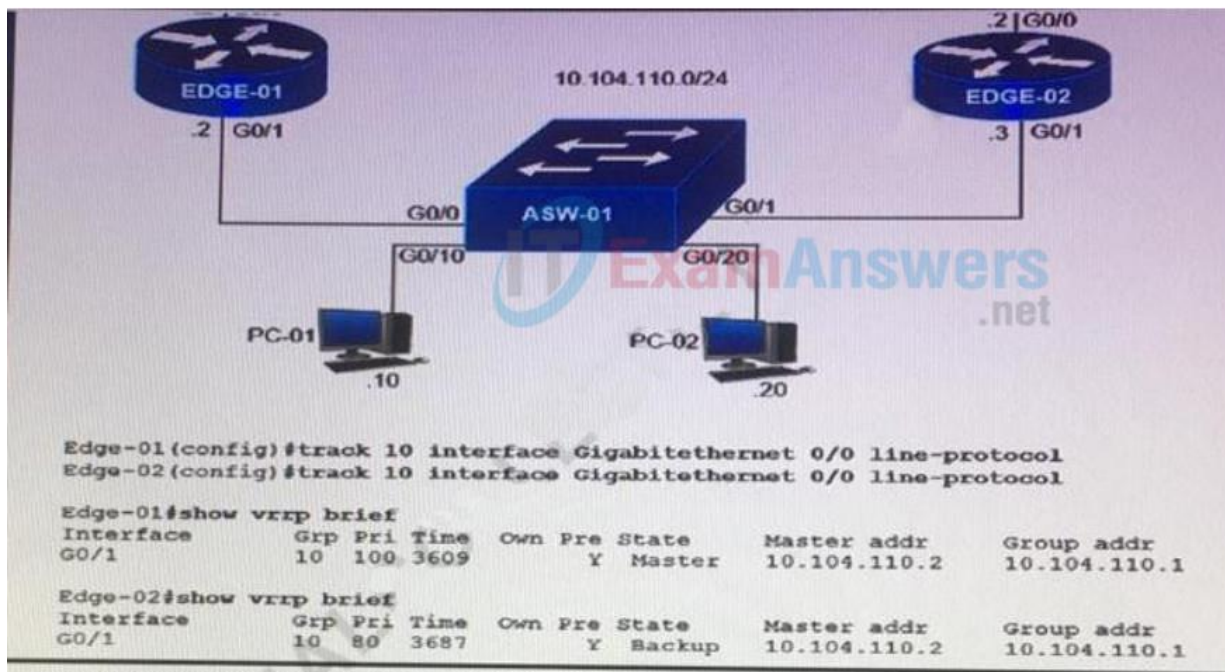
Stack members that are powered on after the 20-second time frame do not participate in this initial election and become stack members. All stack members participate in re-elections. For all powering considerations that affect stack-master elections, see the “Switch Installation” chapter in the hardware installation guide.

The new stack master becomes available after a few seconds. In the meantime, the switch stack uses the forwarding tables in memory to minimize network disruption. The physical interfaces on

the other available stack members are not affected during a new stack master election and reset. After a new stack master is elected and the previous stack master becomes available, the previous stack master does not resume its role as stack master. As described in the hardware installation guide, you can use the Master LED on the switch to see if the switch is the stack master.

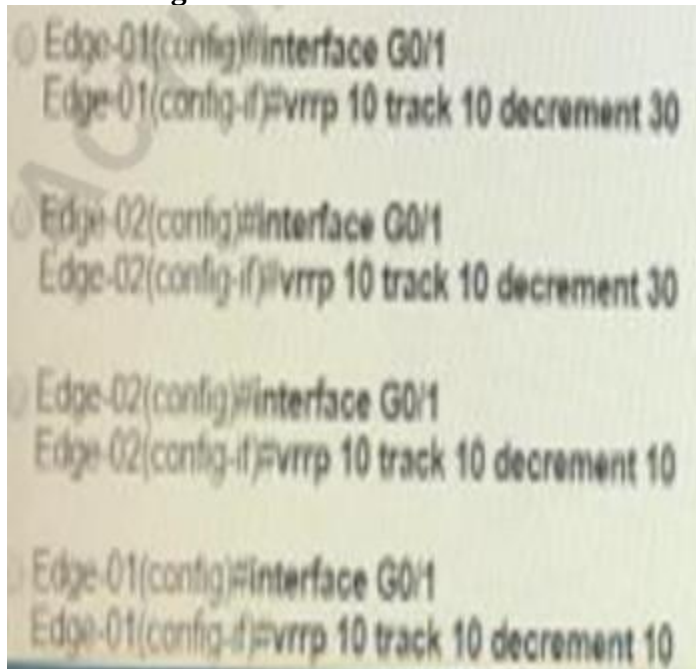
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swstack.html

359. 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. Option A**
- B. Option B
- C. Option C
- D. Option D

Answer: A

360. What is the calculation that is used to measure the radiated power of a signal after it has gone through the radio, antenna cable, and antenna?

- **A. EIRP**
- B. mW
- C. dBm
- D. dBi

Answer: A

Explanation: Once you know the complete combination of transmitter power level, the length of cable, and the antenna gain, you can figure out the actual power level that will be radiated from the antenna. This is known as the effective isotropic radiated power (EIRP), measured in dBm. EIRP is a very important parameter because it is regulated by governmental agencies in most countries. In those cases, a system cannot radiate signals higher than a maximum allowable EIRP. To find the EIRP of a system, simply add the transmitter power level to the antenna gain and subtract the cable loss.

Suppose a transmitter is configured for a power level of 10 dBm (10 mW). A cable with 5-dB loss connects the transmitter to an antenna with an 8-dBi gain. The resulting EIRP of the system

is 10 dBm – 5 dB + 8 dBi, or 13 dBm.

You might notice that the EIRP is made up of decibel-milliwatt (dBm), dB relative to an isotropic antenna (dBi), and decibel (dB) values. Even though the units appear to be different, you can safely combine them because they are all in the dB “domain”.

361. 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

Answer: C

Explanation: Cisco IOS IP SLA Responder is a Cisco IOS Software component whose functionality is to respond to Cisco IOS IP SLA request packets. The IP SLA source sends control packets before the operation starts to establish a connection to the responder. Once the control packet is acknowledged, test packets are sent to the responder. The responder inserts a time-stamp when it receives a packet and factors out the destination processing time and adds time-stamps to the sent packets. This feature allows the calculation of unidirectional packet loss, latency, and jitter measurements with the kind of accuracy that is not possible with ping or other dedicated probe testing.

Reference:

UDP Jitter measures the delay, delay variation (jitter), corruption, misordering and packet loss by generating periodic UDP traffic. This operation always requires IP SLA responder. The command to enable UDP Jitter Operation is “ip sla responder udp-echo {destination-ip-address} [destination-port]

362. 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.

Answer: A

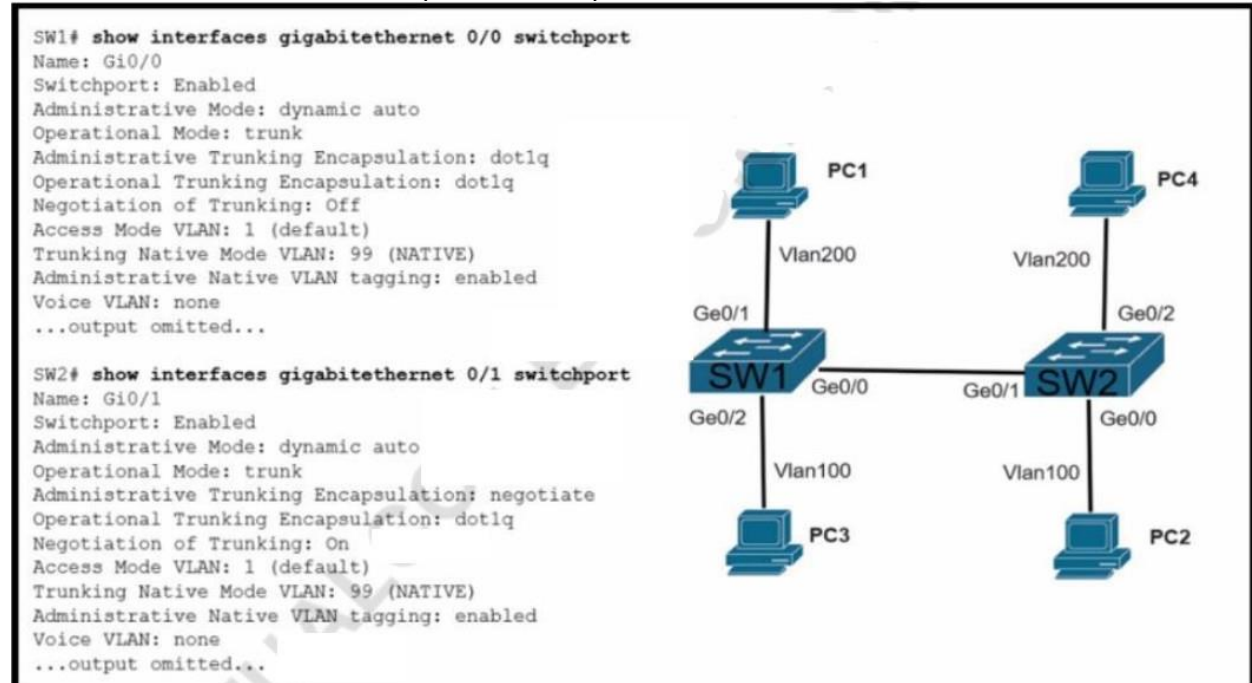
363. Which of the following statements regarding BFD are correct? (Select 2 choices.)

- **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.

Answer: A, B

364. Refer to the exhibit. 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: C E

365. How do cloud deployments differ from on-premises 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

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

```
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
```

- 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

367. 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

Explanation: We only have one AP in each store so we can only use “Presence”, which is the most basic form of location tracking.

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2016/pdf/BRKEWN-2012.pdf>

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

resolves this issue?

```
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)
```

- 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

Explanation: In this case, we are using your EtherChannel without a negotiation protocol on Switch2. As a result, if the opposite switch is not also configured for EtherChannel operation on the respective ports, there is a danger of a switching loop. The EtherChannel Misconfiguration Guard tries to prevent that loop from occurring by disabling all the ports bundled in the EtherChannel.

369. Refer to the exhibit. 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?

```
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
```

- ☐ R1(config)#ip access-list extended 100
R1(config-ext-nacl)#5 permit ip any any
- ☐ R1(config)#no access-list 100 seq 10
R1(config)#access-list 100 seq 40 deny ip any any
- ☐ R1(config)#no access-list 100 deny ip any any
- ☒ R1(config)#ip access-list extended 100
R1(config-ext-nacl)#no 10

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

Correct Answer: D

Explanation: The first ACL statement of “10 deny ip any any” will match and drop all traffic so we have to remove this statement.

370. An engineer runs the sample code, and the terminal returns this output. Which change to the sample code corrects this issue?

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'
```

- **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

Explanation:

- `json.load()` method (without "s" in "load") used to **read JSON encoded data from a file** and convert it into a Python dictionary.
- `json.loads()` method, which is used to **parse valid JSON string** into Python dictionary.

371. 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

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

associate with the master controller on the same subnet.

Reference:

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

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

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

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

Correct Answer: A

373. 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 DM2. 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

Explanation: In order to keep the mobility network stable without any manual intervention and in the event of failure or switchover, the back-and-forth concept of Mobility MAC has been introduced.

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/7-5/High_Availability_DG.html

374. 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

375. Which function is handled by vManage in the Cisco SD-WAN fabric?

- A. Establishes BFD sessions to test liveliness 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

Explanation: We can remote upgrades WAN Edge, vSmart and vBond in vManage.

[https://sdwan-](https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.4/Maintenance/Software_Upgrade)

[docs.cisco.com/Product_Documentation/vManage_Help/Release_18.4/Maintenance/Software_Upgrade](https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.4/Maintenance/Software_Upgrade)

376. Refer to the exhibit. A network administrator configured RSPAN to troubleshoot an issue between switch1 and switch2. The switches are connected using interface GigabitEthernet 1/1 An external packet capture device is connected to switch2 interface GigabitEthernet1/2 Which two commands must be added to complete this configuration? (Choose two)

```
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.

```
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: B,E

Explanation: Switch2 is not allowing VLAN 70 which is used on Switch1 for RSPAN so we must allow it -> Option B is correct (although it would not allow VLAN 81 to 90 to go through).

“An external packet capture device is connected to switch2 interface GigabitEthernet1/2” so we must configure Gi1/2 as the destination port.

For your information, this is how to configure Remote SPAN (RSPAN) feature on two switches. Traffic on FastEthernet0/1 of Switch 1 will be sent to Fa0/10 of Switch2 via VLAN 40.

+ Configure on both switches

Switch1,2(config)#vlan 40

Switch1,2(config-vlan)#remote-span

+ Configure on Switch1

Switch1(config)# monitor session 1 source interface FastEthernet 0/1

Switch1(config)# monitor session 1 destination remote vlan 40

+ Configure on Switch2

Switch2(config)#monitor session 5 source remote vlan 40

Switch2(config)# monitor session 5 destination interface FastEthernet 0/10

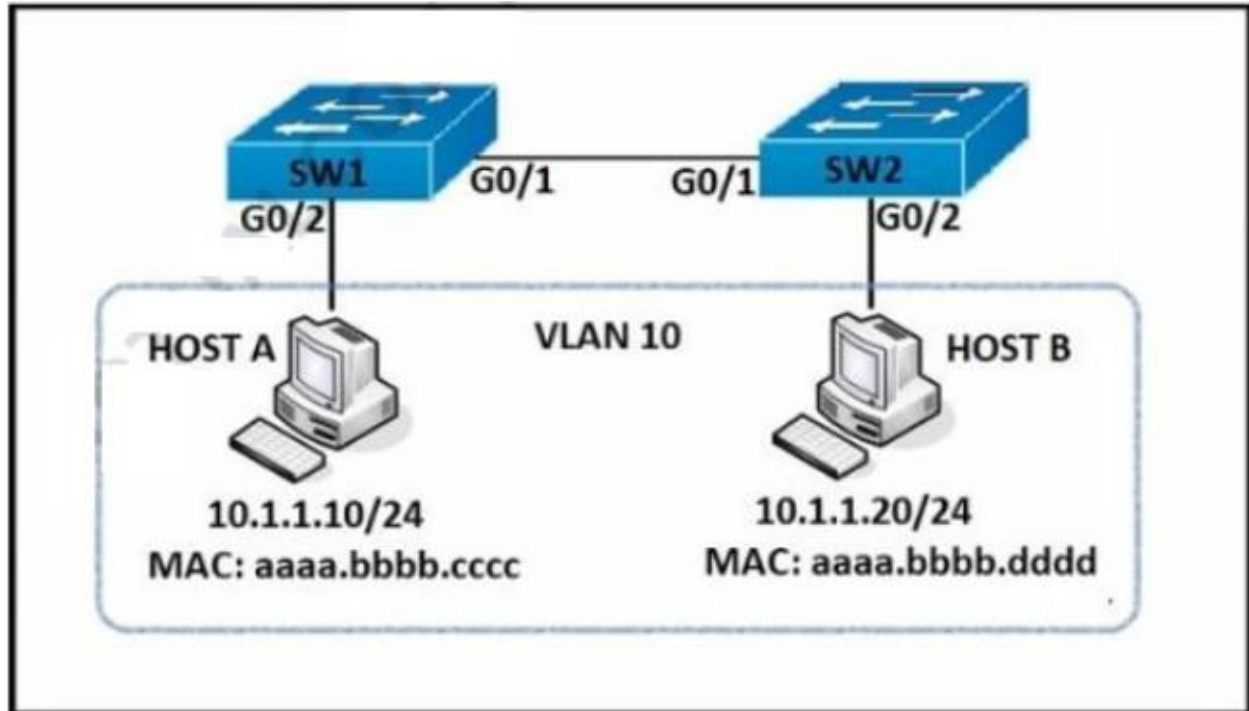
377. Refer to the exhibit. An engineer must create a script that appends the output of the show process cpu sorted command to a file. Which action completes the configuration?

```
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"
```

- 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

378. Refer to the exhibit. An engineer must deny HTTP traffic from host A to host B while allowing all other communication between the hosts. Which command set accomplishes this task?



- SW1(config)# **ip access-list extended DENY-HTTP**
SW1(config-ext-nacl)# **permit tcp host 10.1.1.10 host 10.1.1.20 eq www**

SW1(config)# **ip access-list extended MATCH_ALL**
SW1(config-ext-nacl)# **permit ip any any**

SW1(config)# **vlan access-map HOST-A-B 10**
SW1(config-access-map)# **match ip address DENY-HTTP**
SW1(config-access-map)# **action drop**
SW1(config)# **vlan access-map HOST-A-B 20**
SW1(config-access-map)# **match ip address MATCH_ALL**
SW1(config-access-map)# **action forward**

SW1(config)# **vlan filter HOST-A-B vlan 10**

- SW1(config)# **mac access-list extended HOST-A-B**
SW1(config-ext-macl)# **permit host aaaa.bbbb.cccc aaaa.bbbb.dddd**

SW1(config)# **ip access-list extended DENY-HTTP**
SW1(config-ext-nacl)# **deny tcp host 10.1.1.10 host 10.1.1.20 eq www**

SW1(config)# **vlan access-map DROP-MAC 10**
SW1(config-access-map)# **match mac address HOST-A-B**
SW1(config-access-map)# **action drop**
SW1(config)# **vlan access-map HOST-A-B 20**
SW1(config-access-map)# **match ip address DENY-HTTP**
SW1(config-access-map)# **action drop**

```

SW1(config)# mac access-list extended HOST-A-B
SW1(config-ext-macl)# permit host aaaa.bbbb.cccc aaaa.bbbb.dddd

SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)# permit tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# vlan access-map DROP-MAC 10
SW1(config-access-map)# match mac address HOST-A-B
SW1(config-access-map)# action forward
SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# action drop

SW1(config)# vlan filter HOST-A-B vlan 10

SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)# 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

```

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

Correct Answer: A

Explanation: In this case we need to configure a VLAN access-map to deny HTTP traffic and apply it to VLAN 10. To do it, first create an access-list, by which interesting traffic will be matched. The principle of VLAN access-map config is similar to the route-map principle. After this we'll create a vlan access-map, which has two main parameters: action and match. Match: by this parameter the interesting traffic is matched and here RACL or MAC ACL can be applied as well. Action: what to do with matched traffic. Two main parameters exist: Drop and Forward. In case of Drop, matched traffic will be dropped, and in case of forward, matched traffic will be allowed. A good reference and example can be found at <https://www.networkstraining.com/vlan-access-mapexample-configuration/>

379. Refer to the exhibit. Which Python code snippet prints the descriptions of disabled interfaces only?

```
>>> 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'
```

- ☐ for interface in netconf_data["GigabitEthernet"]:
 print(interface["enabled"])
 print(interface["description"])
- ☐ for interface in netconf_data["GigabitEthernet"]:
 if interface["disabled"] != 'true':
 print(interface["description"])
- ☐ for interface in netconf_data["GigabitEthernet"]:
 if interface["enabled"] != 'true':
 print(interface["description"])
- ☐ for interface in netconf_data["GigabitEthernet"]:
 if interface["enabled"] != 'false':
 print(interface["description"])

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

Correct Answer: C

380. 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

381. 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

382. 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?

The screenshot shows the Cisco SD-WAN configuration interface with the following settings:

- General:** Allow AAA Override (Disabled), Coverage Hole Detection (Enabled), Enable Session Timeout (Disabled), Aironet IE (Disabled), Diagnostic Channel (Enabled), Override Interface ACL (IPv4: None, IPv6: None), Layer2 Ad (None), URL ACL (None), P2P Blocking Action (Disabled), Client Exclusion (Enabled), Maximum Allowed Clients (0), Static IP Tunneling (Enabled), Wi-Fi Direct Clients Policy (Disabled), Maximum Allowed Clients Per AP Radio (200).
- Security:** DHCP (DHCP Server: Override, DHCP Addr. Assignment: Required), OEAP (Split Tunnel: Enabled), Management Frame Protection (MFP) (MFP Client Protection: Optional, DTIM Period (in beacon intervals): 802.11a/n (1 - 255): 1, 802.11b/g/n (1 - 255): 1), NAC (NAC State: None).

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

Correct Answer: D

Explanation: Reference: [Click here](#)

383. What is an advantage of using BFD?

- A. It local 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

Explanation: Bidirectional Forwarding Detection provides a method for network administrators to configure sub-second Layer 2 failure detection between adjacent network nodes. Furthermore, they can configure their routing protocols to respond to BFD notifications, and begin Layer 3 route convergence almost immediately.

https://www.cisco.com/en/US/technologies/tk648/tk365/tk207/technologies_white_paper0900aecd80243fe7.html

384. 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

385. 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

Explanation: WLC

- WLC is connected outside Fabric (optionally directly to Border)
- WLC needs to reside in global routing table – to talk to CP!
- No need for inter-VRF leaking for AP to join the WLC
- WLC can only belong to one FD. WLC talks to one CP (two for HA)

Access Points

- AP is directly connected to FE (or to an extended node switch)

- AP is part of Fabric overlay
- AP belongs to the INFRA_VN which is mapped to the global routing table (new in DNAC 1.1)
- AP joins the WLC in Local mode

386. Which unit is used to express the signal-to-noise ratio?

- A. mW
- **B. db**
- C. amp
- D. dbm

Correct Answer: B

387. 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 statemets does the engineer use to explain these values to the customer? (Choose two)

- A. The signl 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: D E

388. 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

389. 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)
```

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

Correct Answer: A

390. 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>

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

Correct Answer: B

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

- A. DDoS
- **B. ransomware**
- C. Microsoft Word macro attack
- D. SQL injection
- **E. email phishing**

Correct Answer: B,E

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

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

Correct Answer: A,C

393. 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)#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
- B. ☐ 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
- C. ☐ 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
- D. ☐ Router(config)#access-list 100 permit ip host 172.20.10.1 any log
Router(config)#interface GigabitEthernet0/1
Router(config-if)#access-group 100 in

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

Correct Answer: D

394. “HTTP/1.1 204 content” is returned when `curl -I -x DELETE` command is issued. Which situation has occurred?

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

Correct Answer: B

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

GC	= 0x00000000	HotStandBy port = null
Port state	= Port-channel	
Protocol	= PAgP	
Port Security	= Disabled	

- A.  NewYork(config)#no interface po1
NewYork(config)#interface range fa0/1-2
NewYork(config-if)#channel-group 1 mode negotiate
NewYork(config-if)#end
NewYork#
- C.  NewYork(config)#no interface po1
NewYork(config)#interface range fa0/1-2
NewYork(config-if)#channel-group 1 mode on
NewYork(config-if)#end
NewYork#
- B.  NewYork(config)#no interface po1
NewYork(config)#interface range fa0/1-2
NewYork(config-if)#channel-group 1 mode auto
NewYork(config-if)#end
NewYork#
- D.  NewYork(config)#no interface po1
NewYork(config)#interface range fa0/1-2
NewYork(config-if)#channel-group 1 mode passive
NewYork(config-if)#end
NewYork#

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

Correct Answer: D

396. 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

397. What is the function of cisco DNA center in a cisco SD-access deployment?

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

Correct Answer: B

398. 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

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

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

Correct Answer: B

400. What is the function of the LISP map resolver?

- A. to send traffic to non-LISP sites when connected to a service provider that does not accept nonroutable EIDs as packet sources
- B. to connect a site to the LISP-capable part of a core network, publish the EID-to-RLOC mappings for the site and respond to map-request messages

- **C. to decapsulate map-request messages from ITRs and forward the messages to the MS**
- D. to advertise routable non-USP traffic from one address family to LISP sites in a different address family

Correct Answer: C

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

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

Correct Answer: C,D

402. 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

403. 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. A 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

404. 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?

```
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
```

- **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

405. What are two characteristics of VXLAN? (Choose two)

- **A. It uses VTEPs to encapsulate and decapsulate frames.**
- B. It has a 12-bit network identifier
- **C. It allows for up to 16 million VXLAN segments**
- D. It lacks support for host mobility
- E. It extends Layer 2 and Layer 3 overlay networks over a Layer 2 underlay.

Correct Answer: A,C

406. which entity is a Type 1 hypervisor?

- A. Oracle VM VirtualBox
- B. VMware server
- **C. Citrix XenServer**

- D. Microsoft Virtual PC

Correct Answer: C

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

```
import ncclient

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

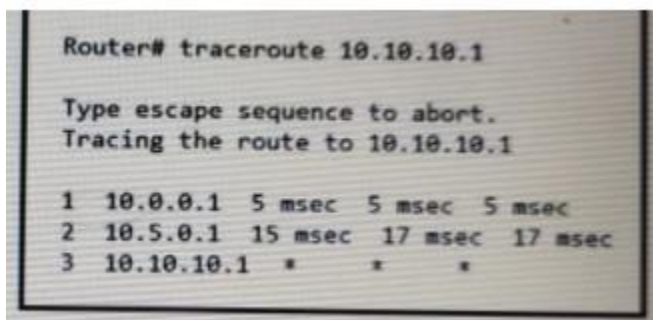
Output

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

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

Correct Answer: C

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



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

Correct Answer: D

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

! — success

* — time out

N — network unreachable

H — host unreachable

P — protocol unreachable

A — admin denied

Q — source quench received (congestion)

? — unknown (any other ICMP message)

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

! — success

* — time out

N — network unreachable

H — host unreachable

P — protocol unreachable

A — admin denied

Q — source quench received (congestion)

? — unknown (any other ICMP message)

409. 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

410. 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

411. Where is radio resource management performed in a cisco SD-access wireless solution?

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

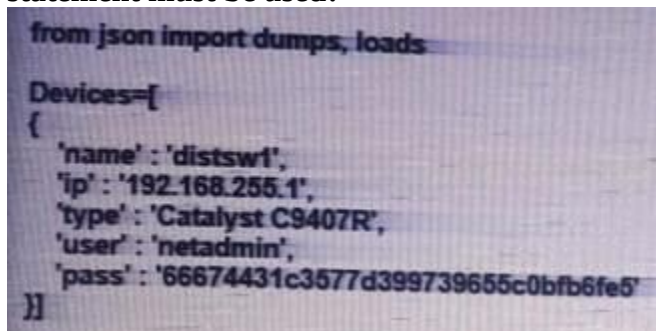
Correct Answer: C

412. Which deployment option of Cisco NQFW provides scalability?

- A. clustering
- B. Inline tap
- **C. high availability**
- D. tap

Correct Answer: C

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



```
from json import dumps, loads

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

- A. json.repr(Devices)
- **B. json.dumps(Devices)**
- C. json.prints(Devices)
- D. json.loads(Devices)

Correct Answer: B

414. 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

415. 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: C,E

416. which features does Cisco EDR use to provide threat detection and response protection?

- A. containment, threat intelligence, and machine learning
- **B. firewalling and intrusion prevention**
- C. container-based agents
- D. cloud analysis and endpoint firewall controls

Correct Answer: B

417. 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

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

the message?

```
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#
```

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

Correct Answer: A

419. In cisco SD_WAN, which protocol is used to measure link quality?

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

Correct Answer: B

420. 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

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

- A. Rouge detector
- B. Sniffer
- C. FlexConnect
- **D. Local**

- **E. Monitor**

Correct Answer: D,E

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

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

Correct Answer: D

423. Which measurement is used from a post wireless survey to depict the cell edge of the access points?

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

Correct Answer: A

424. 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

425. How is Layer 3 roaming accomplished in a unified wireless deployment?

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

Correct Answer: A

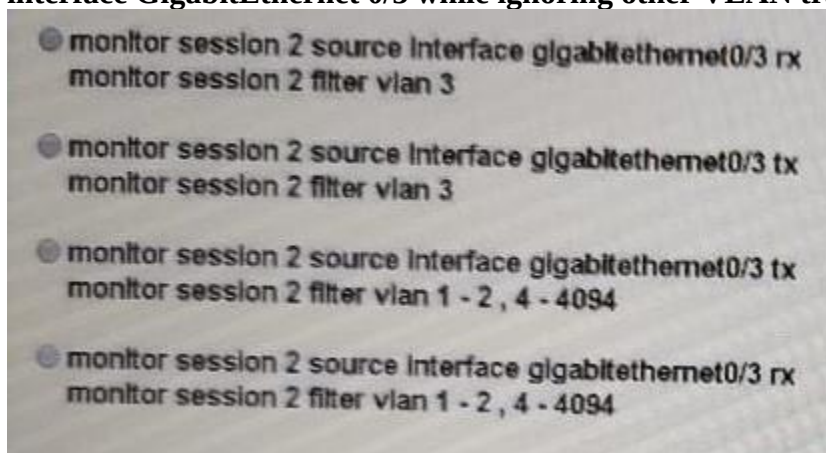
426. What is one benefit of implementing a VSS architecture?

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

Correct Answer: C

Explanation: Support Virtual Switching System (VSS) to provide resiliency, and increased operational efficiency with a single point of management;

427. Which command set configures RSPAN to capture outgoing traffic from VLAN 3 on interface GigabitEthernet 0/3 while ignoring other VLAN traffic on the same interface?



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

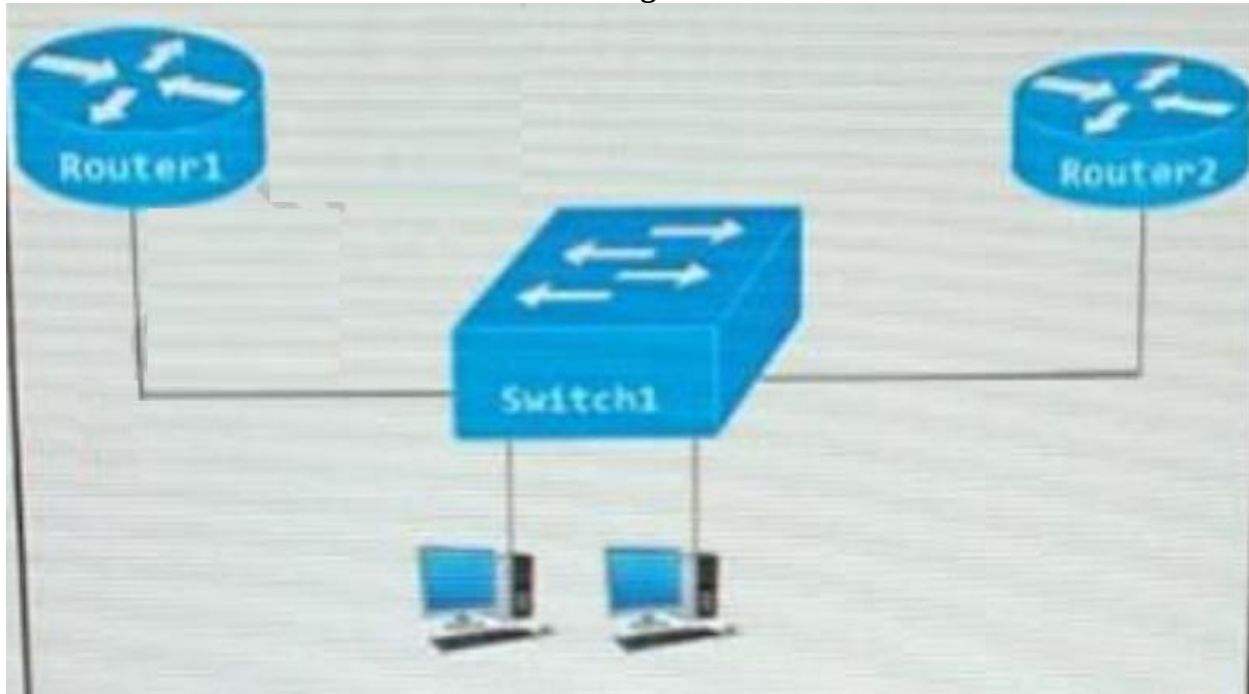
Correct Answer: B

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

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

Correct Answer: C

429. Refer to the exhibit. Router 1 is currently operating as the HSRP primary with a priority of 110 Router1 fails and Router2 take over the forwarding role. Which command on router1 causes it to take over the forwarding role when it return to service?



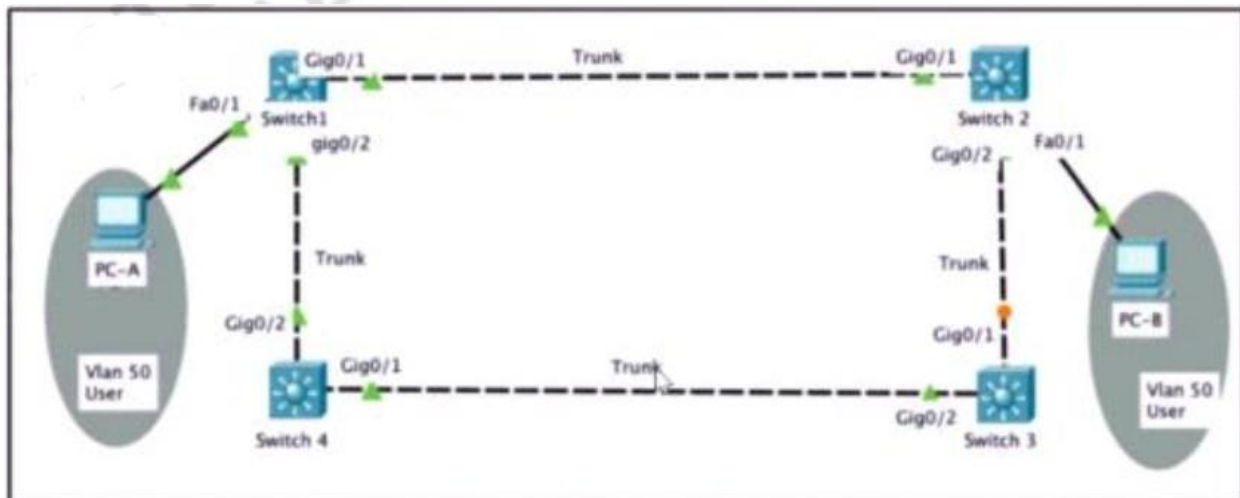
- A. standby 10 priority
- B. standby 10 timers
- C. standby 10 track
- **D. standby 10 preempt**

Correct Answer: D

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

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

- Switch1(config)# **interface f0/1**
Switch1(config-if)# **spanning-tree portfast**
- Switch1(config)# **spanning-tree portfast bpduguard default**
Switch1(config)# **interface f0/1**
Switch1(config-if)# **spanning-tree portfast**
- Switch1(config)# **spanning-tree portfast bpduguard default**
Switch1(config)# **interface f0/1**
Switch1(config-if)# **spanning-tree portfast**
- Switch1(config)# **interface f0/1**
Switch1(config-if)# **spanning-tree portfast**
Switch1(config-if)# **spanning-tree bpduguard enable**



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

Correct Answer: D

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

requirement?

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

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

Correct Answer: B

432. 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.)

- ☐ R2(config-router)#neighbor 10.10.10.1 peer-group CORP
R2(config-router)#neighbor PEER password Cisco
- ☐ R2(config-router)#neighbor 10.10.10.1 peer-group CORP
R2(config-router)#neighbor CORP password Cisco
- ☐ R1(config-router)#neighbor 10.10.10.1 peer-group CORP
R1(config-router)#neighbor CORP password Cisco
- ☐ R2(config-router)#neighbor 10.120.10.1 peer-group CORP
R2(config-router)#neighbor CORP password Cisco
- ☐ R1(config-router)#neighbor 10.120.10.1 peer-group CORP
R1(config-router)#neighbor CORP password Cisco

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

Correct Answer: B,E

433. When is an external antenna used inside a building?

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

Correct Answer: A

434. What is used to perform OoS packet classification?

- A. the Options field in the Layer 3 header
- B. the Type field in the Layer 2 frame

- C. the Flags field in the Layer 3 header
- **D. the TOS field in the Layer 3 header**

Correct Answer: D

435. 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

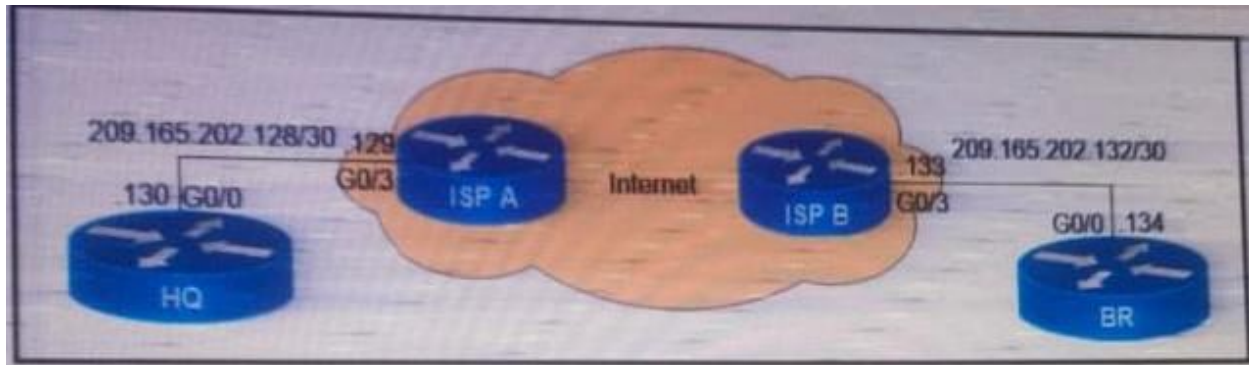
436. Which HTTP code must be returned to prevent the script from exiting?

```
def get_token () :
    device_uri = "https://192.168.1.1/dna/system/api/v1/auth/token"
    http_result = requests.post(device_uri, auth = ("test", "test398810436!"))
    if http_result.status_code != requests.codes.ok:
        print ("Call failed! Review get_token () . ")
        sys.exit ()
    return (http_result.json () ["Token"])
```

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

Correct Answer: D

437. Refer to the exhibit. What is the effect of these commands on the BR and HQ tunnel interfaces?



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

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

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

Correct Answer: B

438. Which technology is used as the basis for the cisco SD-Access data plane?

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

Correct Answer: C

439. 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: A,C,E

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

- **A. End user subnets and endpoints are part of the underlay network.**
- B. The underlay switches provide endpoint physical connectivity for users.

- C. Static routing is a requirement,
- D. It must support IPv4 and IPv6 underlay networks.

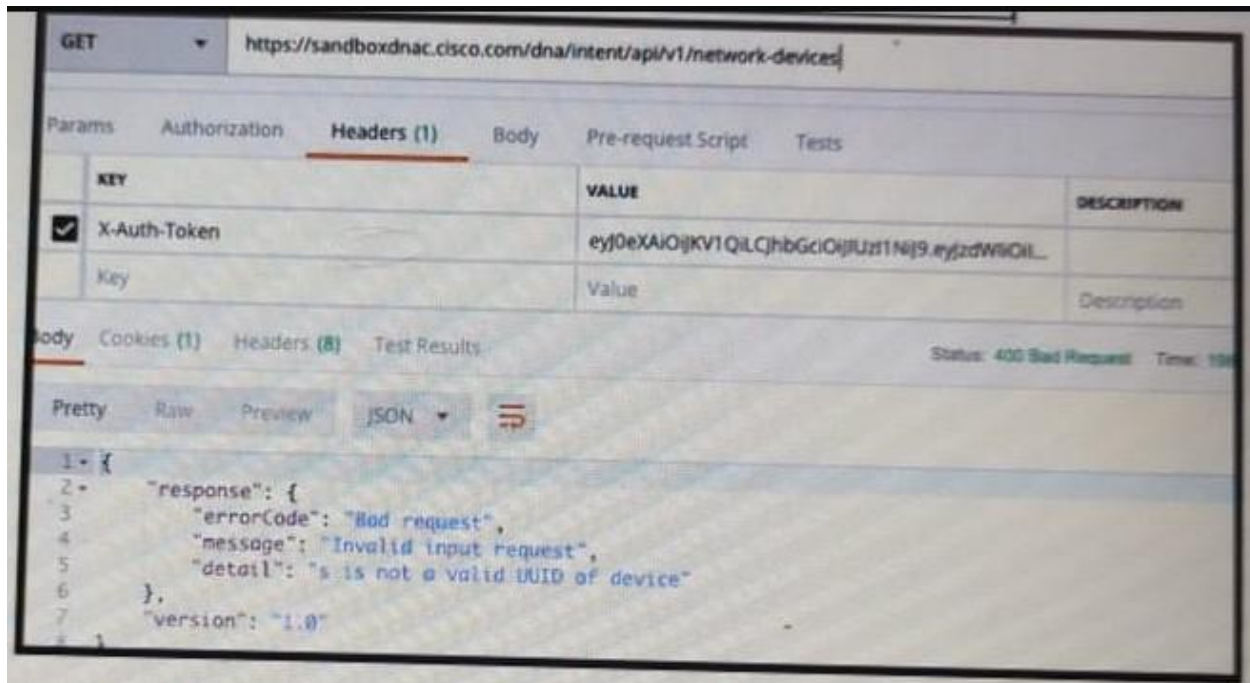
Correct Answer: A

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

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

Correct Answer: D

442. 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 UUID**

Correct Answer: D

443. What are two benefits of YANG? (Choose two.)

- A. It enables multiple leaf statements to exist within a leaf list

- **B. It collects statistical constraint analysis information.**
- C. It enforces configuration constraints.
- D. It enforces configuration semantics.
- **E. It enforces the use of a specific encoding format for NETCONF**

Correct Answer: B,E

444. 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: B

445. 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 URL string is incorrect.
- C. The Cisco DNA Center API port is incorrect
- D. The HTTP method is incorrect

Correct Answer: A

446. Which cisco DNA center application is responsible for group-based access control permissions?

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

Correct Answer: D

447. Which new enhancement was implemented in Wi-Fi 6?

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

Correct Answer: D

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

- A. Use the txml 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

449. 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: C

450. What is the output of this code?

```
def get_credentials():
    creds=('username': 'cisco', 'password': 'c3577dc8ae4e36c0bfb6fe5399079338')
    return (creds.get('username'))

print(get_credentials())
```

- A. username: cisco
- B. get_credentials
- C. username
- **D. cisco**

Correct Answer: D

451. Refer to the exhibit. The EtherChannel between SW2 and SW3 is not operational which action resolves this issue?

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 nonegotiate
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 nonegotiate
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 nonegotiate
channel-group 1 mode passive
end
```

SW3# show etherchannel summary

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

- A. Configure the channel-group mode on SW2 Gi0/0 and Gi0/1 to on.
- B. Configure the channel-group mode on SW3 Gi0/0 and Gi0/1 to active
- **C. Configure the mode on SW2 Gi0/0 to trunk**

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

Correct Answer: C

452. 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"
    }
    """
```

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

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

Correct Answer: D

453. Which device makes the decision for a wireless client to roam?

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

Correct Answer: A

454. 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 how within models

Correct Answer: C

455. 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

456. Which congestion queuing method on Cisco IOS based routers uses four static queues?

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

Correct Answer: A

457. 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

458. 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. wlcboostname.domain.com
- **B. cisco-capwap-controller.domain.com**
- C. ap-manager.domain.com
- D. primary-wlc.domain.com

Correct Answer: B

459. Refer to the exhibit. A network engineer troubleshoots an issue with the port channel between SW1 and SW2. which command resolves the issue?

- ☐ SW1(config-if)#channel-group 10 mode desirable
- ☐ SW1(config-if)#channel-group 10 mode active
- ☐ SW2(config-if)#switchport mode trunk
- ☐ SW2(config-if)#channel-group 10 mode on

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

Correct Answer: B

460. What does the Cisco DNA 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 DONA Center has the incorrect credentials for cat3000-1**

- D. Cisco DNA Center has the Incorrect credentials for RouterASR-1

Correct Answer: C

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

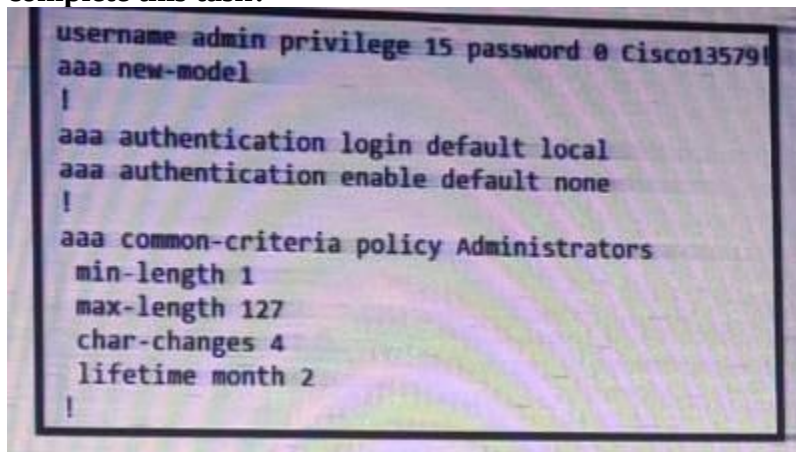
- A. Set the weight attribute to 65.535 on BR1 toward PE1.
- B. Set the local preference to 150 on PE1 toward BR1 outbound
- **C. Set the MED to 1 on PE2 toward BR2 outbound.**
- D. Set the origin to igp on BR2 toward PE2 inbound.

Correct Answer: C

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

- **15**
- 1.2
- -165
- .83

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



```

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
!

```

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

Explanation: SUMMARY STEPS

Perform this task to create a password security policy and to apply the policy to a specific user profile.

```
enable
configure terminal
aaa new-model
aaa common-criteria policy policy-name
char-changes number
max-length number
min-length number
numeric-count number
special-case number
exit
username username common-criteria-policy policy-name password password
end
```

[Previous](#) [1](#) [2](#) [3](#)[Next](#)