

Vendor: Cisco

Exam Code: 350-401

Exam Name: Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)

Version: 21.041

Important Notice

Product

Our Product Manager keeps an eye for Exam updates by Vendors. Free update is available within One year after your purchase.

You can login member center and download the latest product anytime. (Product downloaded from member center is always the latest.)

PS: Ensure you can pass the exam, please check the latest product in 2-3 days before the exam again.

Feedback

We devote to promote the product quality and the grade of service to ensure customers interest.

If you have any questions about our product, please provide Exam Number, Version, Page Number, Question Number, and your Login Account to us, please contact us at support@passleader.com and our technical experts will provide support in 24 hours.

Copyright

The product of each order has its own encryption code, so you should use it independently.

If anyone who share the file we will disable the free update and account access.

Any unauthorized changes will be inflicted legal punishment. We will reserve the right of final explanation for this statement.

Order ID: **********

PayPal Name: **********

PayPal ID: **********

QUESTION 1
What is a benefit of data modeling languages like YANG?

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

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

QUESTION 2
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. Autonomous
B. Mobility express
C. SD-Access wireless
D. Local mode

Answer: B
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. A 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.

QUESTION 3
Which statement about agent-based versus agentless configuration management tools is true?

A. Agentless tools require no messaging systems between master and slaves.
B. Agentless tools use proxy nodes to interface with slave nodes.
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.

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.

QUESTION 4
On which protocol or technology is the fabric data plane based in Cisco SD-Access fabric?

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

Answer: D
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.

QUESTION 5
When using TLS for syslog, which configuration allows for secure and reliable transportation of messages to its default port?

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

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

QUESTION 6
A client device fails to see the enterprise SSID, but other devices are connected to it.
What is the cause of this issue?

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

Answer: A

QUESTION 7
Which function does a fabric edge node perform in an SD-Access deployment?

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

C. Provides reachability border nodes in the fabric underlay
D. Encapsulates end-user data traffic into LISP.

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

QUESTION 8
Which two methods are used by an AP that is typing to discover a wireless LAN controller? (Choose two.)

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

Answer: BD
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

QUESTION 9
Which statement describes the IP and MAC allocation requirements for virtual machines on types

1 hypervisors?

A. Each virtual machine requires a unique IP and MAC addresses to be able to reach to other nodes.
B. Each virtual machine requires a unique IP address but shares the MAC address with the physical server
C. Each virtual machines requires a unique IP address but shares the MAC address with the address of the physical server.
D. Each virtual machine requires a unique MAC address but shares the IP address with the physical server.

Answer: A
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. A big advantage of Type 2 hypervisors is that management console software is not required.

QUESTION 10
Which LISP infrastructure device provides connectivity between non-sites and LISP sites by receiving non-LISP traffic with a LISP site destination?

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

Answer: B
Explanation:
Proxy ingress tunnel router (PITR): A 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.
Reference: https://www.ciscopress.com/articles/article.asp?p=2992605

QUESTION 11
IS OSPF, which LAS type is responsible for pointing to the ASBR router?

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

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.

QUESTION 12
An engineer configures a WLAN with fast transition enabled Some legacy clients fail to connect to this WLAN.
Which feature allows the legacy clients to connect while still allowing other clients to use fast transition based on then OLTIs?

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

Answer: B
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. Therefor 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: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/80211r-ft/b-80211r-dg.html

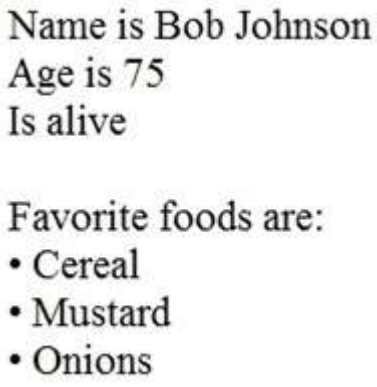
IEEE 802.11v is an amendment to the IEEE 802.11 standard which describes numerous enhancements to wireless network management. One such enhancement is Network assisted Power Savings which helps clients to improve the battery life by enabling them to sleep longer. Another enhancement is Network assisted 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: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/802-11v.pdf

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.

QUESTION 13
Refer to the exhibit. What is the JSON syntax that is formed the data?



A. Name: Bob, Johnson, Age: 75, Alive: true, Favourite Foods. [Cereal, “Mustard”, “Onions}}
B. Name”, “Bob Johnson”, “Age”, 75, “Alive”, true, “favourite Foods”, [“Cereal, “Mustard”, Onions”}}
C. Name’, ‘Bob Johnson,’ ‘Age’, 75, ‘Alive’, true, ‘favourite Foods’ ‘Cereal Mustard’, ‘Onions’}
D. Name”, “Bob Johnson”, “Age”: Seventysix, “Alive” true, “favourite Foods” ,[Cereal” “Mustard” “Onions”}}
E. {“Name”:”Bob Johnson”,”age”:75,”alive”:true,”favorite foods”:[“Cereal”,”Mustard”,”Onions”]}

Answer: E
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” ]
}
```

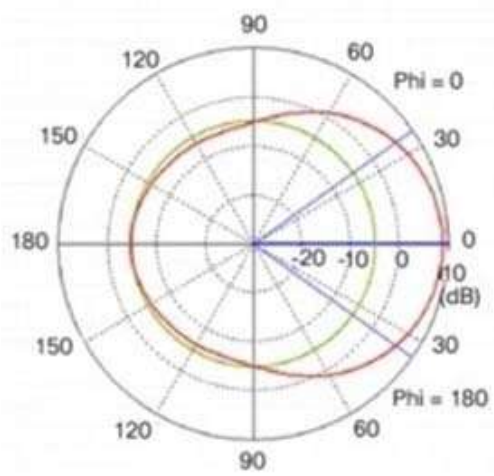
QUESTION 14
If a VRRP master router fails, which router is selected as the new master router?

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

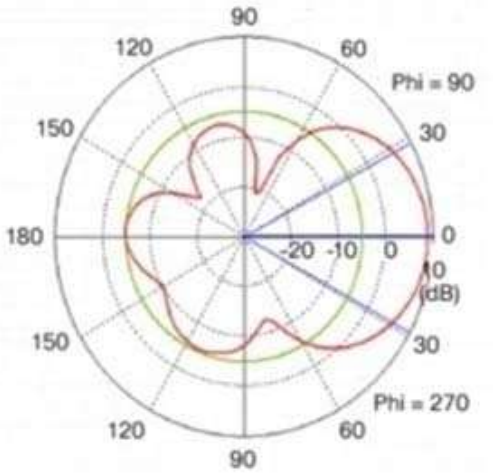
Answer: A

QUESTION 15

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



Antenna Azimuth Plane Pattern

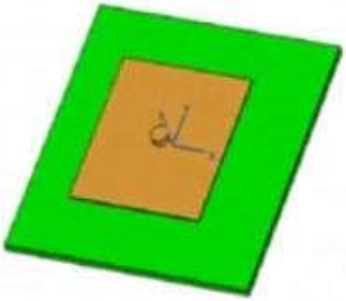


Antenna Elevation Plane Pattern

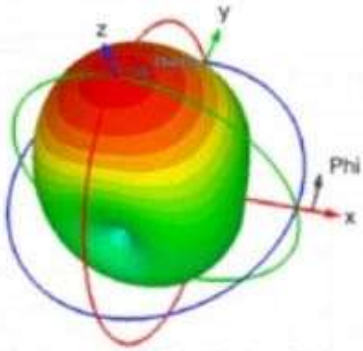
A. Patch
B. Omnidirectional
C. Yagi
D. Dipole

Answer: A
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.

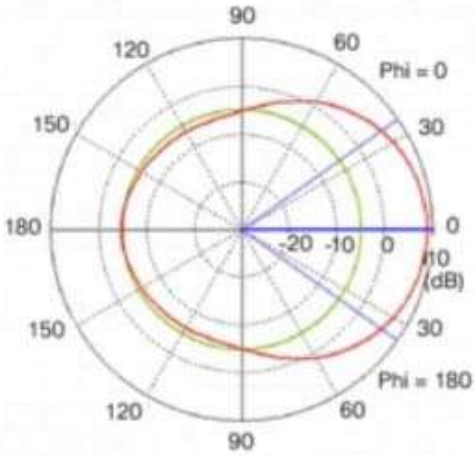
The azimuth and elevation plane patterns are derived by simply slicing through the 3D radiation pattern. In this case, the azimuth plane pattern is obtained by slicing through the x-z plane, and the elevation plane pattern is formed by slicing through the y-z plane. Note that there is one main lobe that 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.



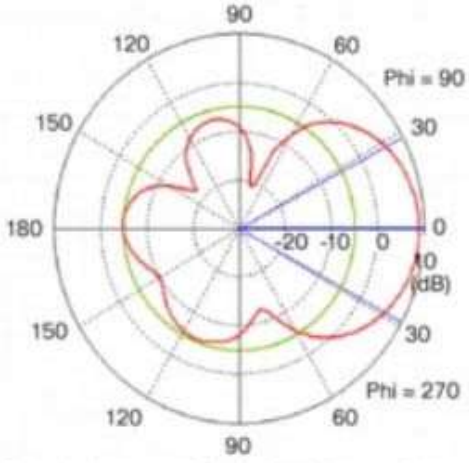
(a) Patch Antenna Model



(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. A 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

QUESTION 16
What do Cisco DNA southbound APIs provide?

A. Interface between the controller and the network devices
B. NETCONF API interface for orchestration communication
C. RESful API interface for orchestrator communication
D. Interface between the controller and the consumer

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

QUESTION 17
To increase total throughput and redundancy on the links between the wireless controller and switch, the customer enabled LAG on the wireless controller.

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

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

Answer: C
Explanation:
Restrictions for Link Aggregation:
You can bundle all eight ports on a Cisco 5508 Controller into a single link.
Terminating on two different modules within a single Catalyst 6500 series switch provides redundancy and ensures that connectivity between the switch and the controller is maintained when one module fails. The controller's port 1 is connected to Gigabit interface 3/1, and the controller's port 2 is connected to Gigabit interface 2/1 on the Catalyst 6500 series switch. Both switch ports are assigned to the same channel group.
LAG requires the EtherChannel to be configured for 'mode on' on both the controller and the Catalyst switch.
Once the EtherChannel is configured as on at both ends of the link, the Catalyst switch should not be configured for either Link Aggregation Control Protocol (LACP) or Cisco proprietary Port Aggregation Protocol (PAgP) but be set unconditionally to LAG. Because no channel negotiation is done between the controller and the switch, the controller does not answer to negotiation frames and the LAG is not formed if a dynamic form of LAG is set on the switch. Additionally, LACP and PAgP are not supported on the controller.
If the recommended load-balancing method cannot be configured on the Catalyst switch, then configure the LAG connection as a single member link or disable LAG on the controller.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-5/configuration-guide/b_cg75/b_cg75_chapter_0100010.html

QUESTION 18
Which description of an SD-Access wireless network infrastructure deployment is true?

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.

Answer: C
Explanation:
Access Points
+ AP is directly connected to FE (or to an extended node switch)
+ AP is part of Fabric overlay
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKEWN-2020.pdf

QUESTION 19
Which method displays text directly into the active console with a synchronous EEM applet policy?

A. event manager applet boom
event syslog pattern 'UP'
action 1.0 gets 'logging directly to console'
B. event manager applet boom

event syslog pattern 'UP'
action 1.0 syslog priority direct msg 'log directly to console'

C. event manager applet boom
event syslog pattern 'UP'
action 1.0 puts 'logging directly to console'

D. event manager applet boom
event syslog pattern 'UP'
action 1.0 string 'logging directly to console'

Answer: C
Explanation:
To enable the action of printing data directly to the local tty when an Embedded Event Manager (EEM) applet is triggered, use the action puts command in applet configuration mode.

The following example shows how to print data directly to the local tty:

```
Router(config-applet)# event manager applet puts
Router(config-applet)# event none
Router(config-applet)# action 1 regexp "(.*) (.*) (.*)" "one two three" _match _sub1
Router(config-applet)# action 2 puts "match is $_match"
Router(config-applet)# action 3 puts "submatch 1 is $_sub1"
Router# event manager run puts
match is one two three
submatch 1 is one
Router#
```

The action puts command applies to synchronous events. The output of this command for a synchronous applet is directly displayed to the tty, bypassing the syslog.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/command/eem-cr-book/eem-cr-a1.html

QUESTION 20
What is the difference between a RIB and a FIB?

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

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

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

QUESTION 21
Which PAgP mode combination prevents an Etherchannel from forming?

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

Answer: A
Explanation:
There are two PAgP modes:

Auto	Responds to PAgP messages but does not aggressively negotiate a PAgP EtherChannel. A 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. A 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**

QUESTION 22
In which part of the HTTP message is the content type specified?

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

Answer: C

QUESTION 23
What is the correct EBGP path attribute list, ordered from most preferred to the least preferred, that the BGP best-path algorithm uses?

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

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

QUESTION 24

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.

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:
https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

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.

QUESTION 25
What the role of a fusion in an SD-Access solution?

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

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

QUESTION 26
Which statement about VXLAN is true?

A. VXLAN uses TCP 35 the transport protocol over the physical data cento network
B. VXLAN extends the Layer 2 Segment ID field to 24-bits. which allows up to 4094 unique Layer 2 segments over the same network.
C. VXLAN encapsulates a Layer 2 frame in an IP-UDP header, which allows Layer 2 adjacency across router boundaries.
D. VXLAN uses the Spanning Tree Protocol for loop prevention.

Answer: C
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 B 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.
Reference: https://www.cisco.com/c/en/us/support/docs/lan-switching/vlan/212682-virtual-extensible-lan-and-ethernet-virt.html

QUESTION 27
Refer to the exhibit. 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?

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

SwitchC#show vlan brief

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

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

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

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

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

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

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

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.

QUESTION 28
Which HHTP 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

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: A 4xx code indicates a “client error” while a 5xx code indicates a “server error”.

Reference: https://restfulapi.net/http-status-codes/

QUESTION 29
When configuration WPA2 Enterprise on a WLAN, which additional security component configuration is required?

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

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: https://www.securew2.com/solutions/wpa2-enterprise-and-802-1x-simplified/

QUESTION 30
A response code of 404 is received while using the REST API on Cisco UNA Center to POST to this URI.

```
/dna/intent/api/v1 /template-programmer/project
```

What does the code mean?

A. The client made a request a resource that does not exist.
B. The server has not implemented the functionality that is needed to fulfill the request.

C. The request accepted for processing, but the processing was not completed.
D. The POST/PUT request was fulfilled and a new resource was created, Information about the resource is in the response body.

Answer: A
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.

Reference: https://restfulapi.net/http-status-codes/

QUESTION 31
Which behavior can be expected when the HSRP versions is changed from 1 to 2?

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

Answer: A
Explanation:
When you change the HSRP version, Cisco NX-OS reinitializes the group because it now has a new virtual MAC address. HSRP version 1 uses the MAC address range 0000.0C07.ACxx while HSRP version 2 uses the MAC address range address range 0000.0C9F.F0xx.

QUESTION 32
A client with IP address 209.165.201.25 must access a web server on port 80 at 209.165.200.225.
To allow this traffic, an engineer must add a statement to an access control list that is applied in the inbound direction on the port connecting to the web server.
Which statement allows this traffic?

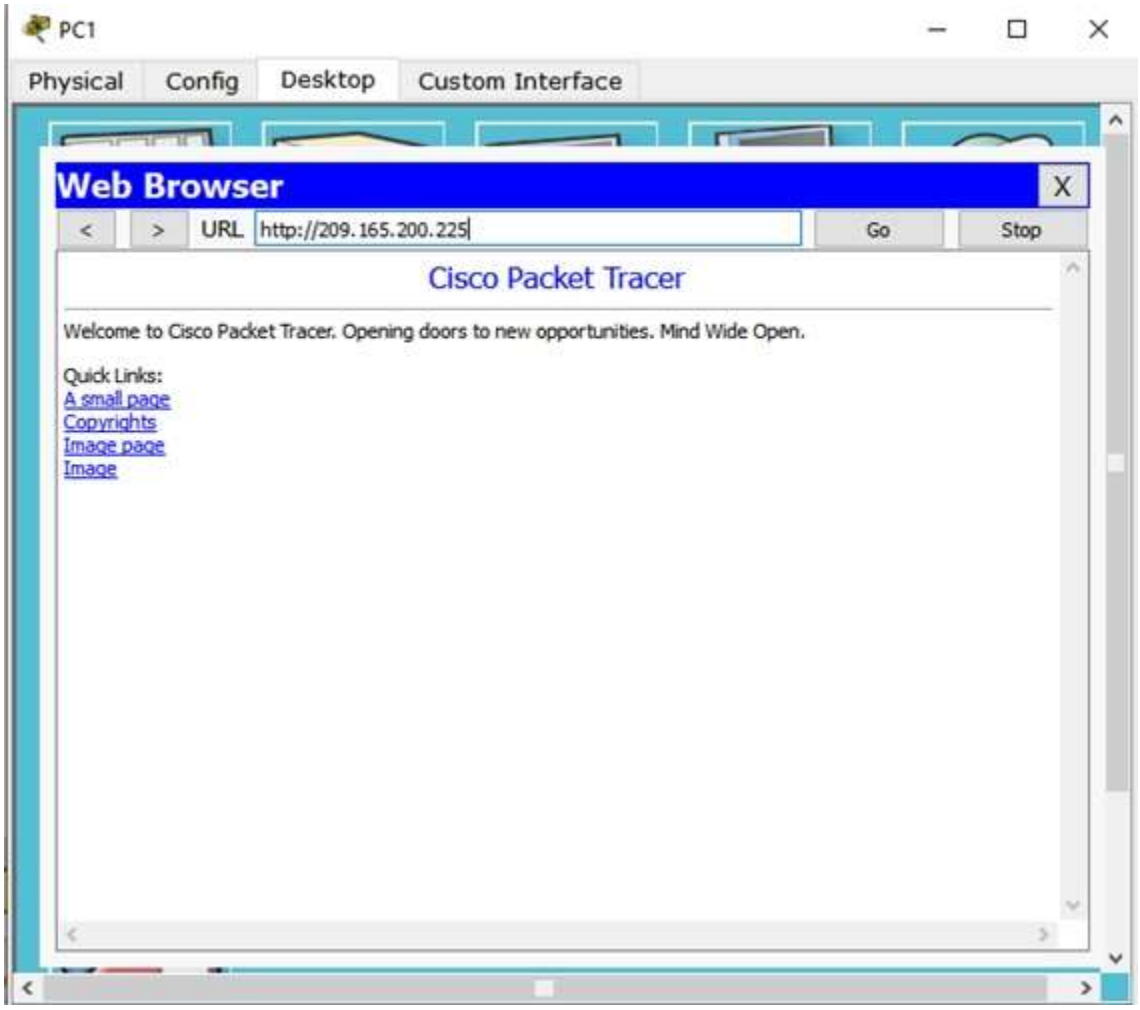
A. permit tcp host 209.165.200.225 eq 80 host 209.165.201.25
B. permit tcp host 209.165.201.25 host 209.165.200.225 eq 80
C. permit tcp host 209.165.200.225 It 80 host 209.165.201.25
D. permit tcp host 209.165.200.225 host 209.165.201.25 eq 80

Answer: A
Explanation:
Example:



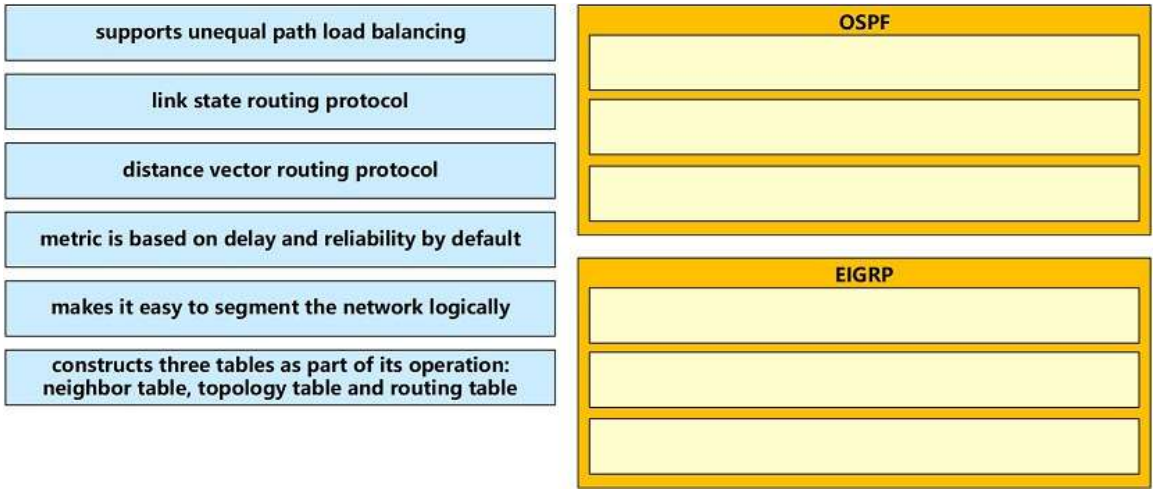

```
Router#sh run
```

```
!
interface GigabitEthernet0/0
ip address 209.165.201.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 209.165.200.1 255.255.255.0
ip access-group ENCOR in
duplex auto
speed auto
!
ip access-list extended ENCOR
permit tcp host 209.165.200.225 eq www host 209.165.201.25
!
End
```

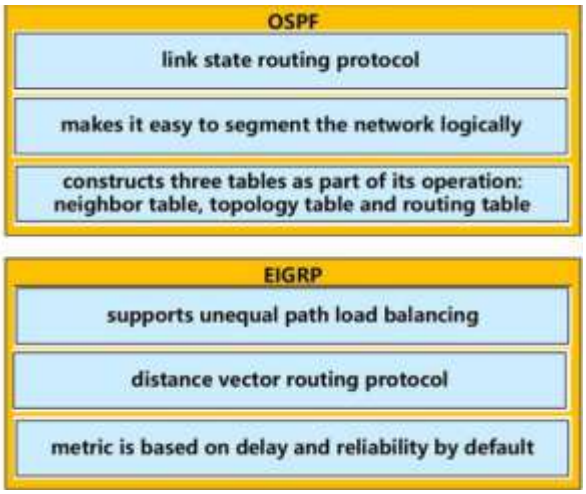


QUESTION 33
Drag and Drop Question

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



Answer:



QUESTION 34
Refer to the exhibit. Which IP address becomes the next 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. 192.168.101.18
B. 192.168.101.6
C. 192.168.101.10
D. 192.168.101.14

Answer: A
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. A path without LOCAL_PREF (LocPrf column) means it has the default value of 100. Therefore we can find the two next best paths with the next hop of 192.168.101.18 and 192.168.101.10.

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

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

QUESTION 35
Which two protocols are used with YANG data models? (Choose two.)

A. HTTPS
B. SSH
C. RESTCONF
D. TLS
E. NFTCONF

Answer: CE
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.

QUESTION 36
Which protocol does REST API rely on to secure the communication channel?

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

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

Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/rest_cfg/2_1_x/b_Cisco_APIC_REST_API_Configuration_Guide/b_Cisco_APIC_REST_API_Configuration_Guide_chapter_01.html

QUESTION 37
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”]}}

Answer: C
Explanation:
This JSON can be written as follows:

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

QUESTION 38
Which two descriptions of FlexConnect mode for Cisco APs are true? (Choose two.)

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

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.

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html

QUESTION 39
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 nonewline "Do you wish to continue [Y/N]"
   action 1.2 gets response
   action 1.3 string toupper "$response"
   action 1.4 string match "$_string_result" "Y"
   action 2.0 if $_string_result eq 1
   action 2.1 cli command "enable"
   action 2.2 cli command "show running-config"
   action 2.3 puts $_cli_result
   action 2.4 cli command "exit"
   action 2.9 end
```

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

Answer: AD
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.

Reference: https://blog.ipspace.net/2011/01/eem-event-cli-command-options-and.html

QUESTION 40
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. Python
C. Bash script
D. NETCONF
E. REST

Answer: E

QUESTION 41
Which data modeling language is commonly used by NETCONF?

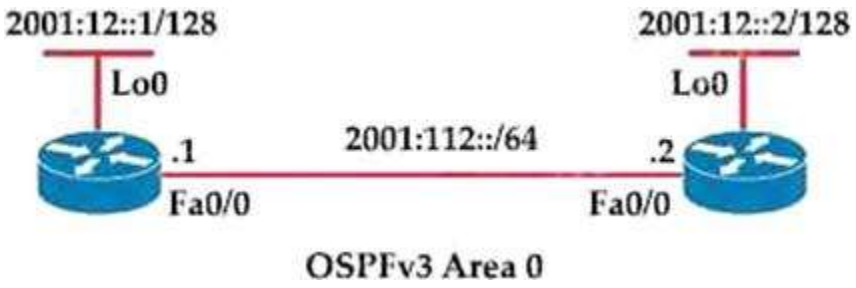
A. HTML
B. XML
C. YANG
D. REST

Answer: C
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.

Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-5/configuration_guide/prog/b_165_prog_9500_cg/data_models.pdf

Note: Although NETCONF also uses XML but XML is not a data modeling language.

QUESTION 42
Refer to the exhibit. Which IPv6 OSPF network type is applied to interface Fa0/0 of R2 by default?



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

Answer: A
Explanation:
The Broadcast network type is the default for an OSPF enabled ethernet interface (while Point-to-Point is the default OSPF network type for Serial interface with HDLC and PPP encapsulation).
Reference: https://www.oreilly.com/library/view/cisco-ios-cookbook/0596527225/ch08s15.html

QUESTION 43
A network is being migrated from IPV4 to IPV6 using a dual-stack approach. Network management is already 100% IPV6 enabled. In a dual-stack network with two dual-stack NetFlow collections, how many flow exporters are needed per network device in the flexible NetFlow configuration?

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

Answer: B

QUESTION 44
What is the structure of a JSON web token?

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

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://jwt.io/introduction/

QUESTION 45
Which feature is supported by EIGRP but is not supported by OSPF?

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

Answer: C
Explanation:
EIGRP support unequal-cost load balancing via the “variance …” while OSPF only supports equal-cost load balancing.

QUESTION 46
Which method creates an EEM applet policy that is registered with EEM and runs on demand or manually?

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

Answer: C
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. A script is a form of policy that is written in Tool Command Language (Tcl).

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.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/xe-3s/eem-xe-3s-book/eem-policy-cli.html

QUESTION 47
Which IP SLA operation requires the IP SLA responder to be configured on the remote end?

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

Answer: B
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/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806bfb52.html

The IP SLAs responder is a component embedded in the destination Cisco device that allows the system to anticipate and respond to IP SLAs request packets. The responder provides accurate measurements without the need for dedicated probes.

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

UDP Jitter measures the delay, delay variation(jitter), corruption, misorderingand packet lossby generating periodic UDP traffic. This operation always requires IP SLA responder.

Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2017/pdf/BRKNMS-3043.pdf

QUESTION 48
An engineer is configuring local web authentication on a WLAN. The engineer chooses the Authentication radio button under the Layer 3 Security options for Web Policy.
Which device presents the web authentication for the WLAN?

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

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

“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.

QUESTION 49
Refer to 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 pruning
B. SW3(config)#vtp mode transparent
C. SW2(config)=vtp pruning
D. SW1(config)>vtp mode transparent

Answer: A
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.

QUESTION 50
Which NGFW mode block flows crossing the firewall?

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

Answer: D
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

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200924-configuring-firepower-threat-defense-int.html

QUESTION 51
What are two common sources of interference for Wi-Fi networks? (Choose two.)

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

Answer: AC
Explanation:

https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Common_Sources_of_Wireless_Interference

QUESTION 52
A network administrator is Implementing a routing configuration change and enables routing debugs to track routing behavior during the change. The logging output on the terminal is interrupting the command typing process. Which two actions can the network administrator take to minimize the possibility of typing commands incorrectly? (Choose two.)

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

Answer: CD
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book/cf_l1.html
logging synchronous
To synchronize unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty, use the logging synchronous command in line configuration mode. To disable synchronization of unsolicited messages and debug output, use the no form of this command.
logging synchronous [level severity-level | all] [limit number-of-lines]

QUESTION 53
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 02050D480809

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

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

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

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

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

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

D.
```
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#
```

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 C is correct. Although the “password 7 0202039485748” line under “line vty 0 4” is not necessary.

If you want to learn more about AAA configuration, please read our AAA TACACS+ and RADIUS Tutorial – Part 2.

For your information, answer D would be correct if we add the following command under vty line (“line vty 0 4”): “login authentication telnet” (“telnet” is the name of the AAA list above)

QUESTION 54
Which QoS component alters a packet to change the way that traffic is treated in the network?

A. Marking
B. Classification
C. Shaping
D. Policing

Answer: A
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).
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_mqc/configuration/xe-16/qos-mqc-xe-16-book/qos-mrkg.html

QUESTION 55
Which marking field is used only as an internal marking within a router?

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

Answer: A
Explanation:
Cisco routers allow you to mark two internal values (qos-group and discard-class) that travel with the packet within the router but do not modify the packet’s contents.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_mqc/configuration/xe-16-6/qos-mqc-xe-16-6-book/qos-mrkg.html

QUESTION 56
Which statement about a Cisco APIC controller versus a more traditional SDN controller is true?

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

Answer: A
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).

QUESTION 57
Which QoS mechanism will prevent a decrease in TCP performance?

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

Answer: C
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:

1. 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.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conavd/configuration/15-mt/qos-conavd-15-mt-book/qos-conavd-cfg-wred.html

WRED is only useful when the bulk of the traffic is TCP/IP traffic. With TCP, dropped packets indicate congestion, so the packet source will reduce its transmission rate. With other protocols, packet sources may not respond or may resend dropped packets at the same rate. Thus, dropping packets does not decrease congestion.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conavd/configuration/xe-16/qos-conavd-xe-16-book/qos-conavd-oview.html

QUESTION 58
Which statement explains why Type 1 hypervisor is considered more efficient than Type 2 hypervisor?

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

Answer: A
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.

QUESTION 59
What are two benefit of virtualizing the server with the use of VMs in data center environment? (Choose two.)

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

Answer: BD
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.

Reference: https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/net_implementation_white_paper0900aecd806a9c05.html

QUESTION 60
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”
]
}
```

Answer: D

QUESTION 61
Which TCP setting is tuned to minimize the risk of fragmentation on a GRE/IP tunnel?

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

Answer: D
Explanation:

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

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

Reference: http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html (there is some examples of how TCP MSS avoids IP Fragmentation in this link but it is too long so if you want to read please visit this link)

Note: IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later.

QUESTION 62
Which statement about an RSPAN session configuration is true?

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

Answer: C
Explanation:
The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches -> This VLAN can be considered a special VLAN type -> Answer C is correct.

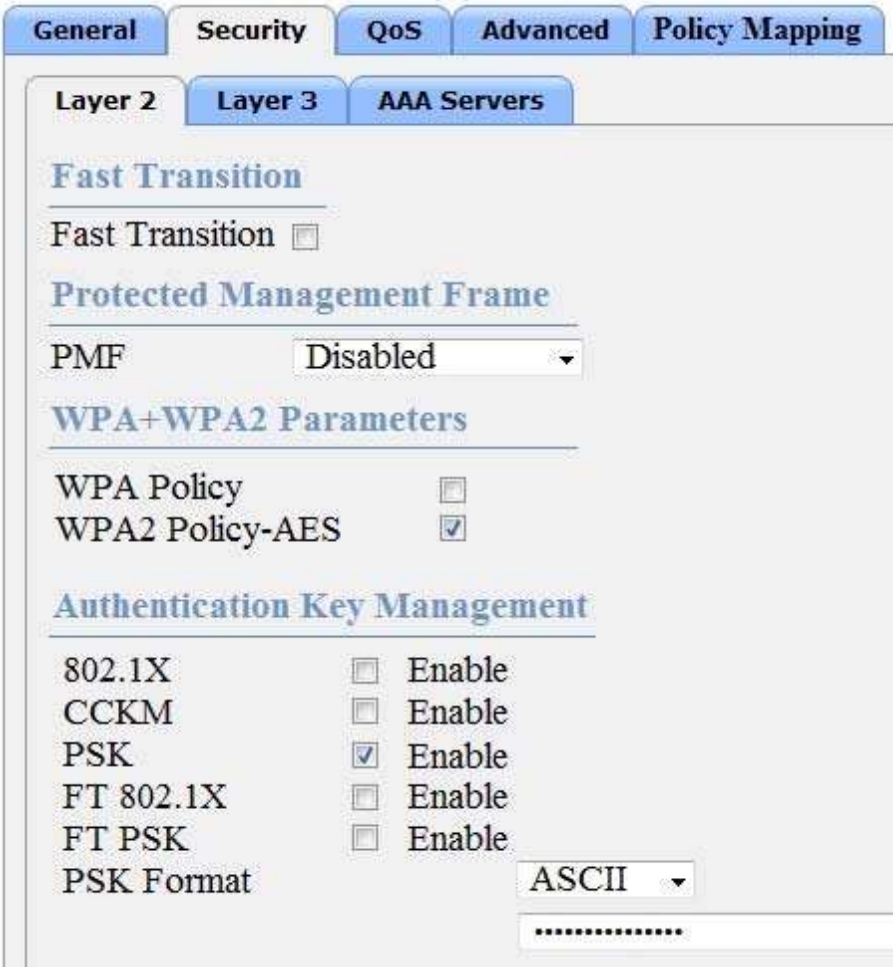
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swspan.html

We can configure multiple RSPAN sessions on a switch at a time, then continue configuring multiple RSPAN sessions on the other switch without any problem -> Answer B is not correct.

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

QUESTION 63
Refer to the exhibit. Based on the configuration in this WLAN security setting. Which method can a client use to authenticate to the network?



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

Answer: A

QUESTION 64
Which two pieces of information are necessary to compute SNR? (Choose two.)

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

Answer: BD
Explanation:
Signal to Noise Ratio (SNR) is defined as the ratio of the transmitted power from the AP to the ambient (noise floor) energy present. To calculate the SNR value, we add the Signal Value to the Noise Value to get the SNR ratio. A positive value of the SNR ratio is always better.

Here is an example to tie together this information to come up with a very simple RF plan calculator for a single AP and a single client.
+ Access Point Power = 20 dBm
+ 50 foot antenna cable = – 3.35 dB Loss
+ Signal attenuation due to glass wall with metal frame = -6 dB
+ External Access Point Antenna = + 5.5 dBi gain
+ RSSI at WLAN Client = -75 dBm at 100ft from the AP
+ Noise level detected by WLAN Client = -85 dBm at 100ft from the AP

Based on the above, we can calculate the following information.
+ EIRP of the AP at source = 20 – 3.35 + 5.5 = 22.15 dBm
+ Transmit power as signal passes through glass wall = 22.15 – 6 = 16.15 dBm
+ SNR at Client = -75 + -85 = 10 dBm (difference between Signal and Noise)

Reference:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/CMX/CMX_RFFund.html

Receive Signal Strength Indicator (RSSI) 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.

EIRP tells you what's the actual transmit power of the antenna in milliwatts.

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

QUESTION 65
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:0G:07:bd	AP Address	3c:ce:73:1b:33:39
IP Address	192.100.101.100	AP Name	172.22.253.20
Client Type	Regular	AP Type	Mobile
User Name		WLAN Profile	Staff
Port Number	29	Status	Associated
Interface	Staff	Association ID	0
VLAN ID	3602	802.11 Authentication	Open System
CCX Version	Not Supported	Reason Code	1
E2E Version	Not Supported	Status Code	0
Mobility Role	Anchor	CF Pollable	Not Implemented
Mobility Peer IP Address	172.22.253.20.	CF Poll Request	Not Implemented
Policy Manager State	RUN	Short Preamble	Implemented
Management Frame Protection	No	PBCC	Not Implemented
UpTime (Sec)	3710	Channel Agility	Not Implemented
Power Save Mode	OFF	Timeout	0
Current TxRateSet		WEP State	WEP Enable
Data RateSet	5.5,11.0,6.0,9.0,12.0,19.0,24.0,36.0,40.0,54.0		

A. Indirect
B. Layer 3 intercontroller
C. Layer 2 intercontroller
D. Intercontroller

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.

QUESTION 66
What is the difference between the enable password and the enable secret password when password encryption is enable on an IOS device?

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

Answer: D
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.

QUESTION 67
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

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 that the MTU set on the neighboring router, the neighboring router ignores the packet.

QUESTION 68

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

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

Answer: BE
Explanation:
In VRF-Lite, Route distinguisher (RD) identifies the customer routing table and allows customers to be assigned overlapping addresses. Therefore it can support multiple customers with overlapping addresses -> Answer E is correct.
VRFs are commonly used for MPLS deployments, when we use VRFs without MPLS then we call it VRF lite -> Answer C is not correct.
VRF-Lite supports most populr routing protocols: BGP, OSPF, EIGRP, RIP, and static routing -> Answer B is correct.

QUESTION 69
Which statement about the default QoS configuration on a Cisco switch is true?

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

Answer: C

QUESTION 70
Which IPv6 migration method relies on dynamic tunnels that use the 2002::/16 reserved address space?

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

Answer: B
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.

QUESTION 71
How are the Cisco Express Forwarding table and the FIB related to each other?

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

Answer: D

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.
Reference: https://www.cisco.com/c/en/us/support/docs/routers/12000-series-routers/47321-ciscoef.html

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

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

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

QUESTION 73
What is a benefit of deploying an on-premises infrastructure versus a cloud infrastructure deployment?

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

Answer: B
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.

QUESTION 74
How does Cisco Trustsec enable more access controls for dynamic networking environments and data centers?

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

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

Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Apr2016/User-to-DC_Access_Control_Using_TrustSec_Deployment_April2016.pdf

QUESTION 75
Which method does the enable secret password option use to encrypt device passwords?

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

Answer: D

QUESTION 76
Refer to the exhibit. Which privilege level is assigned to VTY users?

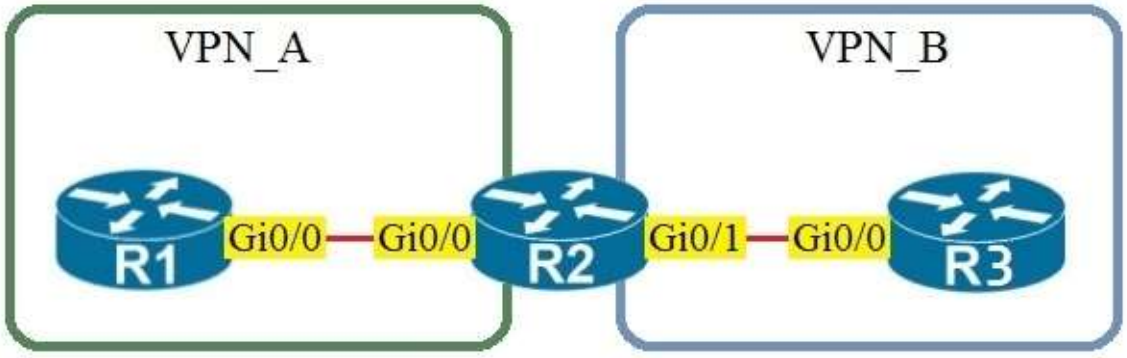
```
R1# sh run | begin line con
line con o
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux o
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  password 7 045802150C2E
  login
line vty 5 15
  password 7 045802150C2E
  login
!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

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

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

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

QUESTION 77
Refer to the exhibit. Assuming that R is a CE router, which VRF is assigned to Gi0/0 on R1?



A. VRF VPN_B
B. Default VRF
C. Management VRF
D. VRF VPN_A

Answer: B
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.

QUESTION 78
Which technology provides a secure communication channel for all traffic at Layer 2 of the OSI model?

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

Answer: A
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.

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: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-9/configuration_guide/sec/b_169_sec_9300_cg/macsec_encryption.html

Note: Cisco Trustsec is the solution which includes MACsec.

QUESTION 79
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": "04/06/2017",
    "kick_file_name": "bootflash:///nxos.7.0.3.I7.4.bin",
    "kick_cmpl_time", "6/14/1970 2:00:00",
    "kick_tmstmp": "06/14/1970 09:49:04",
    "chassis_id": "Nexus9000 93180YC-EX chassis",
    "cpu_name": "Intel(R) Xeon(R) CPU @ 1.80GHz",
    "memory": 24633488,
    "mem_type": "kB",
    "rr_usecs": 134703,
    "rr_crime": "Sun Mar 10 15:41:46 2019",
    "rr_reason": "Reset Requested by CLI command reload",
    "rr_sys_ver": "7.0(3)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)

Answer: D
Explanation:
+ If you want to run the full code in this question in Python (with a real HTTP JSON response), you must first install “requests” package before “import requests”.
+ The error “NameError: name ‘json’ is not defined” is only shown if we forgot the line “import json” in Python code -> Answer A is not correct.
+ We only see the “KeyError” message if we try to print out an unknown attribute (key).

QUESTION 80
Which two statements about EIGRP load balancing are true? (Choose two.)

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

Answer: AB
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

metric < variance * 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.

QUESTION 81
Which statement about LISP encapsulation in an EIGRP OTP implementation is true?

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

Answer: B
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 A 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 D 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.

QUESTION 82
Which EIGRP feature allows the use of leak maps?

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

Answer: D
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 R4_L0opback0_LEAKMAP
```

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

QUESTION 83
Which statements are used for error handling in Python?

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

Answer: B
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!!!"
```

QUESTION 84
Which feature must be configured to allow packet capture over Layer 3 infrastructure'?

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

Answer: D
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.

QUESTION 85
Which statement about Cisco Express Forwarding is true?

A. It uses a fast cache that is maintained in a router data plane.

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

Answer: B
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.
The adjacency table is tasked with maintaining the layer 2 next-hop information for the FIB.
Note: A fast cache is only used when fast switching is enabled while CEF is disabled.

QUESTION 86
Which statement about route targets is true when using VRF-Lite?

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

Answer: B
Explanation:
Answer C and answer D are not correct as only route distinguisher (RD) identifies the customer routing table and "allows customers to be assigned overlapping addresses".
Answer A is not correct as "When BGP is configured, route targets are transmitted as BGP extended communities"

QUESTION 87
Which two GRE features are configured to prevent fragmentation? (Choose two.)

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

Answer: BF
Explanation:
The IP protocol was designed for use on a wide variety of transmission links. Although the maximum length of an IP datagram is 65535, most transmission links enforce a smaller maximum packet length limit, called an MTU. The value of the MTU depends on the type of the transmission link. The design of IP accommodates MTU differences since it allows routers to fragment IP datagrams as necessary. The receiving station is responsible for the reassembly of the fragments back into the original full size IP datagram.

Fragmentation and Path Maximum Transmission Unit Discovery (PMTUD) is a standardized technique to determine the maximum transmission unit (MTU) size on the network path between

two hosts, usually with the goal of avoiding IP fragmentation. PMTUD was originally intended for routers in IPv4. However, all modern operating systems use it on endpoints.

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.

Reference: http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html (there is some examples of how TCP MSS avoids IP Fragmentation in this link but it is too long so if you want to read please visit this link)

Note: IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later.

If the DF bit is set to clear, routers can fragment packets regardless of the original DF bit setting -> Answer D is not correct.

QUESTION 88
Refer to the exhibit. 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 GigabitEthernetO/O 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?

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

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

B. Only standard access control lists can block traffic from a source IP address.
C. After an access control list is applied to an interface, that interface must be shut and no shut for the access control list to take effect.
D. The access control list must contain an explicit deny to block traffic from the router

Answer: A

QUESTION 89
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

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.

QUESTION 90
Which LISP device is responsible for publishing EID-to-RLOC mappings for a site?

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

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/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.html

QUESTION 91
Which access controls list allows only TCP traffic with a destination port range of 22-433, 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

Answer: C
Explanation:
Although the statement “permit tcp any any gt … lt …” seems to be correct but in fact it is not. Each ACL statement only supports either “gt” or “lt” but not both.

QUESTION 92
Which feature does Cisco TrustSec use to provide scalable, secure communication throughout a network?

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

Answer: B
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 A and answer C are not correct as they say “assigned … on a switch” only. Answer D is not correct either as it says “assigned to each router”).

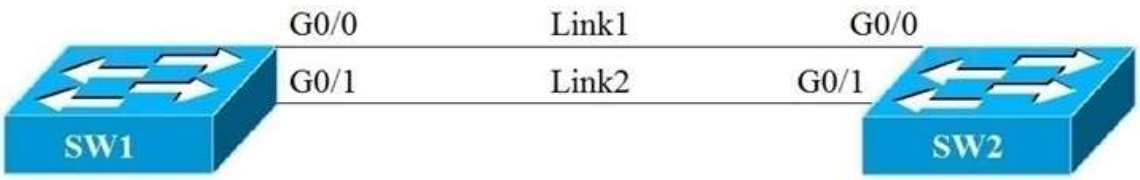
QUESTION 93
Which action is the vSmart controller responsible for in an SD-WAN deployment?

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

Answer: B
Explanation:
The major components of the vSmart controller are:
+ Control plane connections - Each vSmart controller establishes and maintains a control plane connection with each vEdge router in the overlay network. (In a network with multiple vSmart controllers, a single vSmart controller may have connections only to a subset of the vEdge routers, for load-balancing purposes.) Each connection, which runs as a DTLS tunnel, is established after device authentication succeeds, and it carries the encrypted payload between the vSmart controller and the vEdge router. This payload consists of route information necessary for the vSmart controller to determine the network topology, and then to calculate the best routes to network destinations and distribute this route information to the vEdge routers. The DTLS connection between a vSmart controller and a vEdge router is a permanent connection. The vSmart controller has no direct peering relationships with any devices that a vEdge router is connected to on the service side (so answer C is not correct as vSmart only manages vEdge routers only, not the whole nodes within SD-WAN fabric).

+ OMP (Overlay Management Protocol) - The OMP protocol is a routing protocol similar to BGP that manages the Cisco SD-WAN overlay network. OMP runs inside DTLS control plane connections and carries the routes, next hops, keys, and policy information needed to establish and maintain the overlay network. OMP runs between the vSmart controller and the vEdge routers and carries only control plane information. The vSmart controller processes the routes and advertises reachability information learned from these routes to other vEdge routers in the overlay network.
+ Authentication - The vSmart controller has pre-installed credentials that allow it to authenticate every new vEdge router that comes online (-> Answer A is correct). These credentials ensure that only authenticated devices are allowed access to the network.
+ Key reflection and rekeying - The vSmart controller receives data plane keys from a vEdge router and reflects them to other relevant vEdge routers that need to send data plane traffic.
+ Policy engine - The vSmart controller provides rich inbound and outbound policy constructs to manipulate routing information, access control, segmentation, extranets, and other network needs.
+ Netconf and CLI - Netconf is a standards-based protocol used by the vManage NMS to provision a vSmart controller. In addition, each vSmart controller provides local CLI access and AAA.
Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html

QUESTION 94
Refer to the exhibit. 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 GO/1 on SW2. but the port remains blocked.
Which command should be entered on the ports that are connected to Lmk2 to resolve the issue?




```
SW2#show spanning-tree

 VLAN0001

   Spanning tree enabled protocol ieee

   Root ID     Priority    32769
               Address     5000.0005.0000
               Cost        4
               Port        1 (GigabitEthernet0/0)
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

   Bridge ID   Priority    32769 (priority 32768 sys-id-ext 1)
               Address     5000.0006.0000
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
               Aging Time  300 sec

Interface           Role  Sts  Cost  Prio.Nbr   Type
---------------     ----  ---  ----  --------  -------------------

Gi0/0               Root  FWD   4    128.1      P2p
Gi0/1               Altn  BLK   4    32.2       P2p
```

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

Answer: A
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. A BPDU is superior than another if it has:
1. A lower Root Bridge ID
2. A lower path cost to the Root
3. A lower Sending Bridge ID
4. A 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.

QUESTION 95
Which requirement for an Ansible-managed node is true?

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

Answer: B
Explanation:
While it is true Ansible cannot be installed on Windows machine, it cannot also be installed on Cisco device.
However for all Ansible managed host i.e cisco device, windows device, etc, SSH must be running to manage them.

QUESTION 96
Refer to this output. What is the logging severity level?

```
R1#Feb 14 37:15:12:429: %LINEPROTO-5-UPDOWN Line protocol on interface
GigabitEthernet0/1. Change state to up
```

A. Notification
B. Alert
C. Critical
D. Emergency

Answer: A
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 “5” in “%LINEPROTO-5- UPDOWN” is the severity level of this message so in this case it is “notification”.

QUESTION 97

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

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

Answer: D
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 CISCO-CAPWAP-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: https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107606-dns-wlc-config.html

QUESTION 98
At which Layer does Cisco DNA Center support REST controls?

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

Answer: D

QUESTION 99
Which two statements about IP SLA are true? (Choose two)

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

Answer: BC
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: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book/sla_overview.html

QUESTION 100
Which two statements about Cisco Express Forwarding load balancing are true?

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

Answer: DE
Explanation:
Cisco IOS software basically supports two modes of CEF load balancing: On per-destination or per-packet basis.
For per destination load balancing a hash is computed out of the source and destination IP address (-> Answer E is correct). This hash points to exactly one of the adjacency entries in the adjacency table (-> Answer D 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 non-load 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 A is not correct.
Reference:
https://www.cisco.com/en/US/products/hw/modules/ps2033/prod_technical_reference09186a00800afeb7.html

QUESTION 101
What is the main function of VRF-lite?

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

Answer: B

QUESTION 102
Which two steps are required for a complete Cisco DNA Center upgrade? (Choose two.)

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

E. system update

Answer: DE

QUESTION 103
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. Full on both routers
B. not established
C. 2WAY/DROTHER on both routers
D. FULL/BDR on R1 and FULL/BDR on R2

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

QUESTION 104
Which statement about TLS is true when using RESTCONF to write configurations on network devices?

A. It is provided using NGINX acting as a proxy web server.
B. It is no supported on Cisco devices.
C. It required certificates for authentication.
D. It is used for HTTP and HTTPs requests.

Answer: A
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.

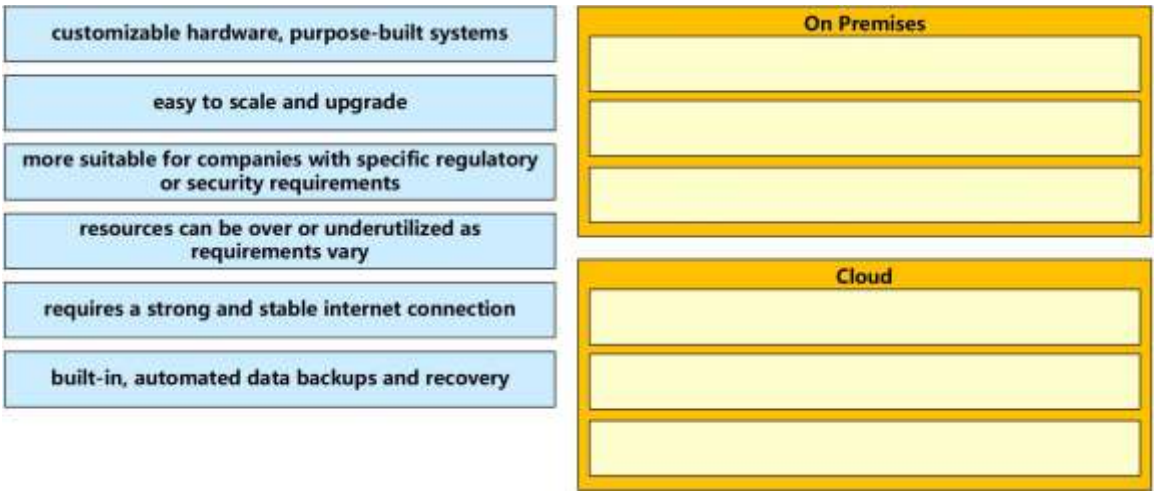
QUESTION 105
Which controller is the single plane of management for Cisco SD-WAN?

A. vBond
B. vEdge
C. vSmart
D. vManange

Answer: D
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

QUESTION 106
Drag and Drop Question

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

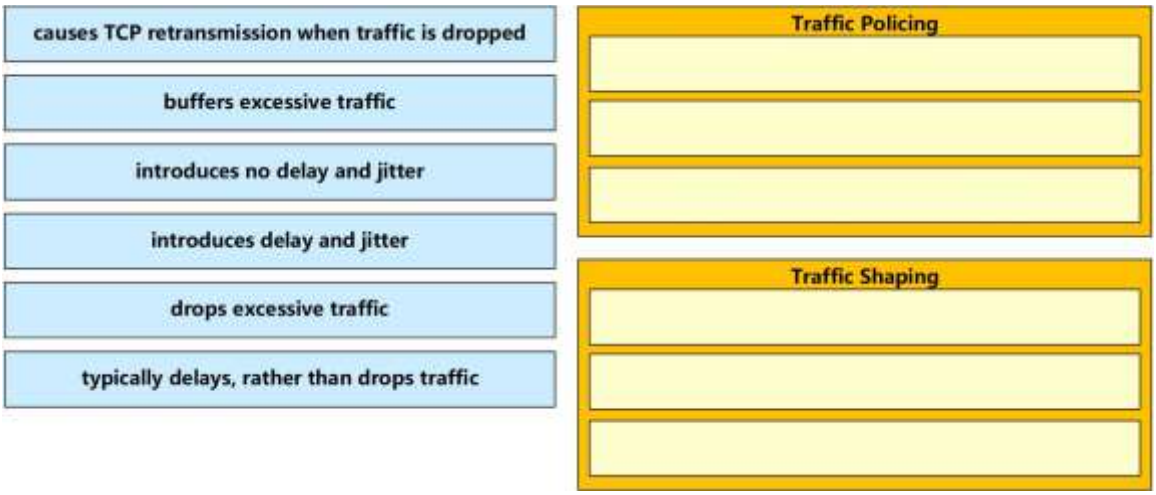


Answer:



QUESTION 107
Drag and Drop Question

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



Answer:



Explanation:
The following diagram illustrates the key difference between traffic policing and traffic shaping. 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. In contrast to policing, 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.
Note: Committed information rate (CIR): The minimum guaranteed data transfer rate agreed to by the routing device.

QUESTION 108
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. It issues email when the value is greater than 75% for five polling cycles.
B. It reads an SNMP variable, and when the value exceeds 75%, it triggers an action GO.
C. It presents a SNMP variable that can be interrogated.

D. Upon the value reaching 75%, a SNMP event is generated and sent to the trap server.

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 entry-value [exit-comb {or | and}] [exit-op operator] [exit-val exit-value] [exit-time exit-time-value] 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)

Reference: https://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtioseem.html

QUESTION 109
What are three valid HSRP states? (Choose three)

A. listen
B. learning
C. full
D. established
E. speak
F. IN IT

Answer: ABE
Explanation:
HSRP consists of 6 states:

State	Description
Initial	This is the beginning state. It indicates HSRP is not running. It happens when the configuration changes or the interface is first turned on
Learn	The router has not determined the virtual IP address and has not yet seen an authenticated hello message from the active router. In this state, the router still waits to hear from the active router.
Listen	The router knows both IP and MAC address of the virtual router but it is not the active or standby router. For example, if there are 3 routers in HSRP group, the router which is not in active or standby state will remain in listen state.
Speak	The router sends periodic HSRP hellos and participates in the election of the active or standby router.
Standby	In this state, the router monitors hellos from the active router and it will take the active state when the current active router fails (no packets heard from active router)
Active	The router forwards packets that are sent to the HSRP group. The router also sends periodic hello messages

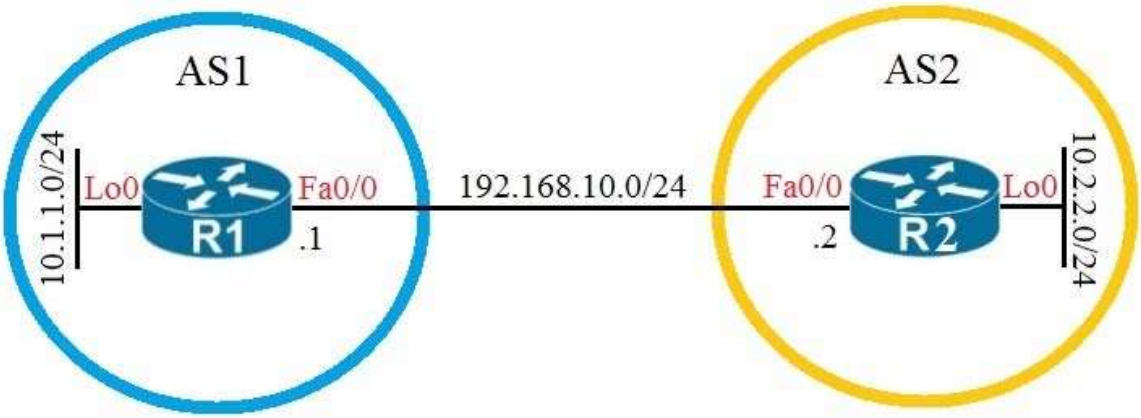
Please notice that not all routers in a HSRP group go through all states above. In a HSRP group, only one router reaches active state and one router reaches standby state. Other routers will stop at listen state.

QUESTION 110
Which two statements about HSRP are true? (Choose two.)

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

Answer: AD
Explanation:
When you change the HSRP version, Cisco NX-OS reinitializes the group because it now has a new virtual MAC address. HSRP version 1 uses the MAC address range 0000.0C07.ACxx while HSRP version 2 uses the MAC address range 0000.0C9F.F0xx.
HSRP supports interface tracking which allows to specify another interface on the router for the HSRP process to monitor in order to alter the HSRP priority for a given group.

QUESTION 111
Refer to the exhibit. Which configuration establishes EBGP neighborship between these two directly connected neighbors and exchanges the loopback network of the two routers through BGP?



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

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

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

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

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

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

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

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

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 ebgp-multihop 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.
+ A route to the neighbor loopback interface. For example: "ip route 10.2.2.0 255.255.255.0 192.168.10.2" on R1 and "ip route 10.1.1.0 255.255.255.0 192.168.10.1" on R2

QUESTION 112
Which two mechanisms are available to secure NTP? (Choose two.)

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

Answer: DE
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/en/us/support/docs/availability/high-availability/19643-ntpm.html

QUESTION 113
Which standard access control entry permits from odd-numbered hosts in the 10.0.0.0/24 subnet?

A. Permit 10.0.0.0.0.0.0.1
B. Permit 10.0.0.1.0.0.0.0
C. Permit 10.0.0.1.0.0.0.254
D. Permit 10.0.0.0.255.255.255.254

Answer: C
Explanation:
Remember, for the wildcard mask, 1′s are I DON'T CARE, and 0′s 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 172.23.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: 0001111 = 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 odd-numbered hosts in the 10.0.0.0/24 subnet.

QUESTION 114
Refer to the exhibit. What are two effect 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. Inside source addresses are translated to the 209.165.201.0/27 subnet.
B. It establishes a one-to-one NAT translation.
C. The 10.1.1.0/27 subnet is assigned as the inside global address range.
D. The 209.165.201.0/27 subnet is assigned as the outside local address range.
E. The 10.1.1.0/27 subnet is assigned as the inside local addresses.

Answer: AE
Explanation:
In this question, the inside local addresses of the 10.1.1.0/27 subnet are translated into 209.165.201.0/27 subnet. This is one-to-one NAT translation as the keyword "overload" is missing so in fact answer B is also correct.

QUESTION 115
Which statement about a fabric access point is true?

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

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/sda-sdg-2019oct.html

QUESTION 116
A local router shows an EBGP neighbor in the Active state. Which statement is true about the local router?

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

Answer: C
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 OpenSent 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 OpenSent state.
4 - OpenSent: the BGP speaker is waiting to receive an OPEN message from the remote BGP speaker
5 - OpenConfirm: 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.

QUESTION 117
Which OSPF networks types are compatible and allow communication through the two peering devices?

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

Answer: A
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.

QUESTION 118
Which statement about Cisco EAP-FAST is true?

A. It does not require a RADIUS server certificate
B. It requires a client certificate

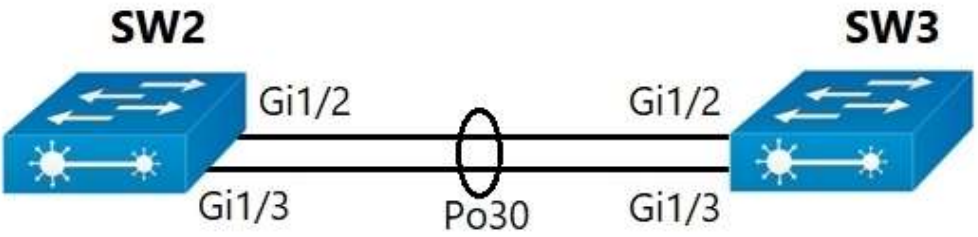
C. It is an IETF standard.
D. It operates in transparent mode

Answer: A
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-mobility/wireless-fixed/72788-CSSC-Deployment-Guide.html

QUESTION 119
Refer to the exhibit. A port channel is configured between SW2 and SW3. SW2 is not running a Cisco operating system. When all physical connections are mode, the port channel does not establish. Based on the configuration excerpt of SW3, what is the cause of the problem?




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

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

QUESTION 120
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 all OSPF messages which router R1 has sent to received on interface Fa0/1.
B. The output displays all OSPF messages which router R1 has sent or received on all interfaces.
C. The output displays OSPF hello messages which router R1 has sent received on interface Fa0/1.
D. The output displays OSPF hello and LSACK messages which router R1 has sent or received.

Answer: C
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
```

QUESTION 121
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 GigabitEthemet 0/1.

```
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
```

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

A. config t
ip access-list extended EGRESS
permit ip 10.1.10.0 255.255.255.0 10.1.2.0 255.255.255.0
B. config t
ip access-list extended EGRESS
5 permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
C. config t
ip access-list extended EGRESS2
permit ip 10.1.10.0 0.0.0.295 10.1.2.0 0.0.0.299
permit ip 10.1.100.0 0.0.0.299 10.1.2.0 0.0.0.299
deny ip any any
!
interface g0/1
no ip access-group EGRESS out
ip access-group EGRESS2 out
D. 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

Answer: B

QUESTION 122
Which two statements about VRRP are true? (Choose two.)

A. It is assigned multicast address 224.0.0.18.
B. The TTL for VRRP packets must be 255.
C. It is assigned multicast address 224.0.0.9.
D. Its IP protocol number is 115.
E. Three versions of the VRRP protocol have been defined.
F. It supports both MD5 and SHA1 authentication.

Answer: AB

QUESTION 123
Which variable in an EEM applet is set when you use the sync yes option?

A. $_cli_result
B. $_result
C. $_string_result
D. $_exit_status

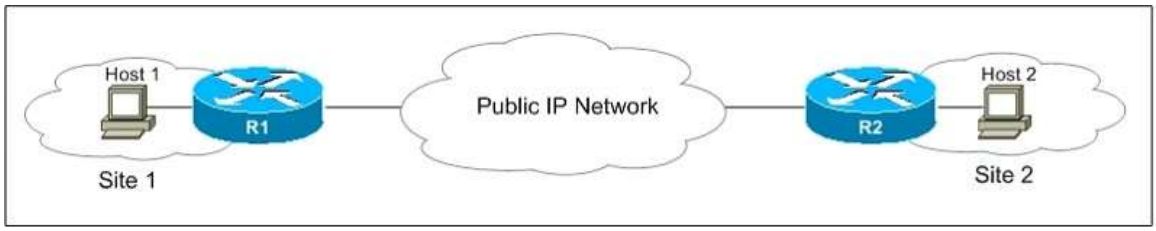
Answer: D
Explanation:
With Synchronous (sync yes), the CLI command in question is not executed until the policy exits. Whether or not the command runs depends on the value for the variable _exit_status. If _exit_status is 1, the command runs, if it is 0, the command is skipped.

QUESTION 124
Into which two pieces of information does the LISP protocol split the device identity? (Choose two.)

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

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

QUESTION 125
Refer to the exhibit. Which LISP component do routers in the public IP network use to forward traffic between the two networks?



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

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

QUESTION 126
Which statement about VRRP is true?

A. It supports load balancing.
B. It can be configured with HSRP on a switch or switch stack.
C. It supports IPv4 and IPv6.
D. It supports encrypted authentication.

Answer: B

QUESTION 127
Refer to the exhibit. 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.)

```
*May20 12:16: 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
*May20 12:16: BGP(4):10.1.1.2 rcvd 999:999:192.168.1.99/32,label 29--DENIED due to:extended community not supported
```

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

Answer: DE
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 Filteringfeature 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.

QUESTION 128
A GRE tunnel is down with the error message %TUN-5-RECURDOWN:

Tunnel0 temporarily disabled due to recursive routing error.

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

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

Answer: CE
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/enhanced-interior-gateway-routingprotocol-eigrp/22327-gre-flap.html

QUESTION 129
Which two statements about AAA authentication are true? (Choose two)

A. RADIUS authentication queries the router's local username database.
B. TACASCS+ 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: DE

QUESTION 130
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

Answer: D

QUESTION 131
Refer to the exhibit. What is the result when a technician adds the monitor session 1 destination remote vlan 223 command?

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

Answer: A

QUESTION 132
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.

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".

QUESTION 133
Which configuration restricts the amount of SSH traffic that a router accepts to 100 kbps?

A.
```
class-map match-all CoPP_SSH
match access-group name CoPP_SSH
 !
 Policy-map CoPP_SSH
 class CoPP_SSH
police cir 100000
exceed-action drop
! ! !
Interface GigabitEthernet0/1
ip address 209.165.200.225 255.255.255.0
 ip access-group 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
deny tcp any any eq 22
!
```

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

Answer: D

QUESTION 134
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.

Answer: BC
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.

QUESTION 135

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

A. Not all of the controllers in the mobility group are using the same mobility group name.
B. Not all of the controllers within he 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.

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

QUESTION 136
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 WLS that resolves the domain name

Answer: D

QUESTION 137
Which two namespaces does the LISP network architecture and protocol use? (Choose two.)

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

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/xe-3s/irl-xe-3s-book/irl-overview.html

QUESTION 138
Which method of account authentication does OAuth 2.0 use within REST APIs?

A. username/role combination

B. access tokens
C. cookie authentication
D. basic signature workflow

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.

QUESTION 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

Answer: A

QUESTION 140
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

Answer: A

QUESTION 141
Which protocol infers that a YANG data model is being used?

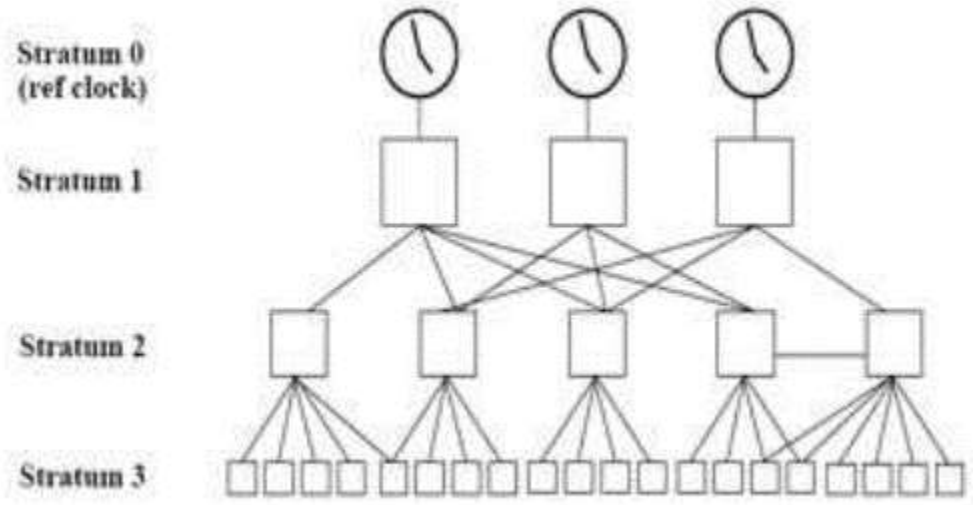
A. SNMP
B. NX-API
C. REST
D. RESTCONF

Answer: D
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.

QUESTION 142
What NTP Stratum level is a server that is connected directly to an authoritative time source?

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

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

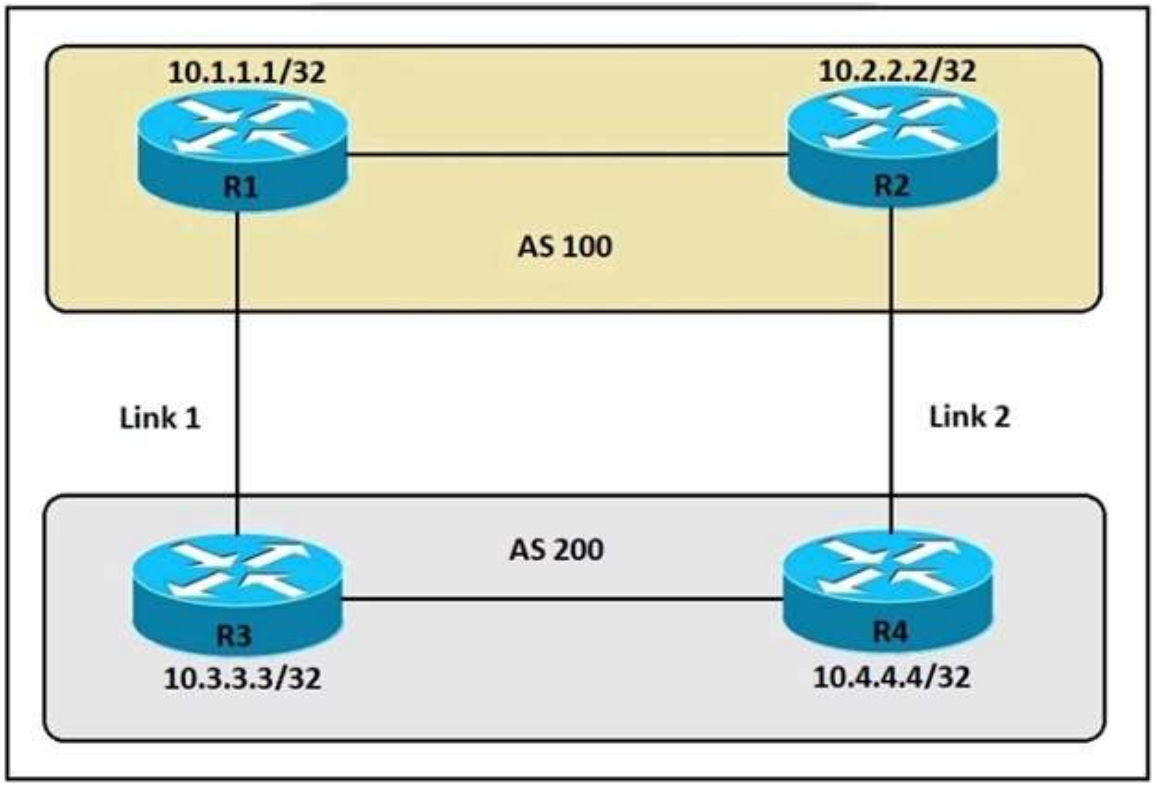
QUESTION 143
Which tool is used in Cisco DNA Center to build generic configurations that are able to be applied on device with similar network settings?

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

Answer: B

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.
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3/user_guide/b_cisco_dna_center_ug_1_3/b_cisco_dna_center_ug_1_3_chapter_0111.html

QUESTION 144
Refer to the exhibit. An engineer must ensure that all traffic leaving AS 200 will choose Link 2 as the exit point. Assuming that all BGP neighbor relationships have been formed and that the attributes have not been changed on any of the routers, which configuration accomplish task?



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

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.

QUESTION 145
Which access point mode allows a supported AP to function like a WLAN client would, associating and identifying client connectivity issues?

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

Answer: C
Explanation:
Using a sensor, a device can function like a WLAN client, associating and identifying client connectivity issues in the network in real time without requiring an onsite IT technician.

QUESTION 146
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

Answer: A

QUESTION 147
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

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

QUESTION 148
Which component of the Cisco Cyber Threat Defense solution provides user and flow context analysis?

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

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
Reference: 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

QUESTION 149
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

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.

QUESTION 150
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

Answer: B
Explanation:
ISE is mandatory component of SDA fabric, so answer is not just any RADIUS, but ISE.

QUESTION 151
What is the role of the RP in PIM sparse mode?

A. The RP responds to the PIM join messes 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.

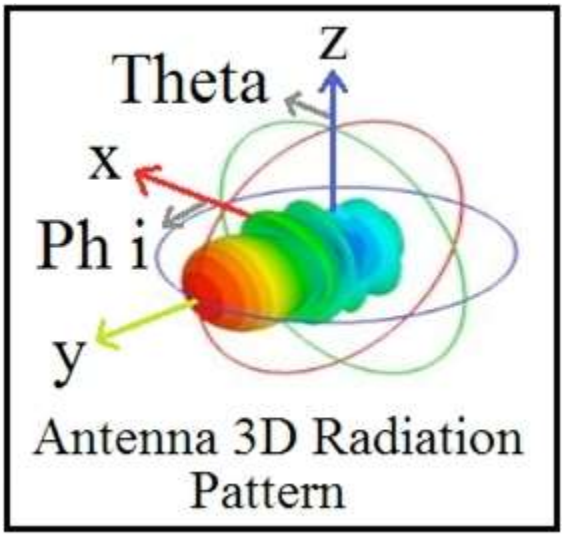
Answer: A

QUESTION 152
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.

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

QUESTION 153
Refer to the exhibit. Which type of antenna does the radiation pattern represent?



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

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.



Reference: https://www.cisco.com/c/en/us/products/collateral/wireless/aironetantennas-accessories/prod_white_paper0900aecd806a1a3e.htm

QUESTION 154
Refer to the exhibit. The inside and outside interfaces in the NAT configuration of this device have been correctly identified.

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

What is the effect of this configuration?

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

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-toone) by using different ports so it is called Port Address Translation (PAT).

QUESTION 155
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

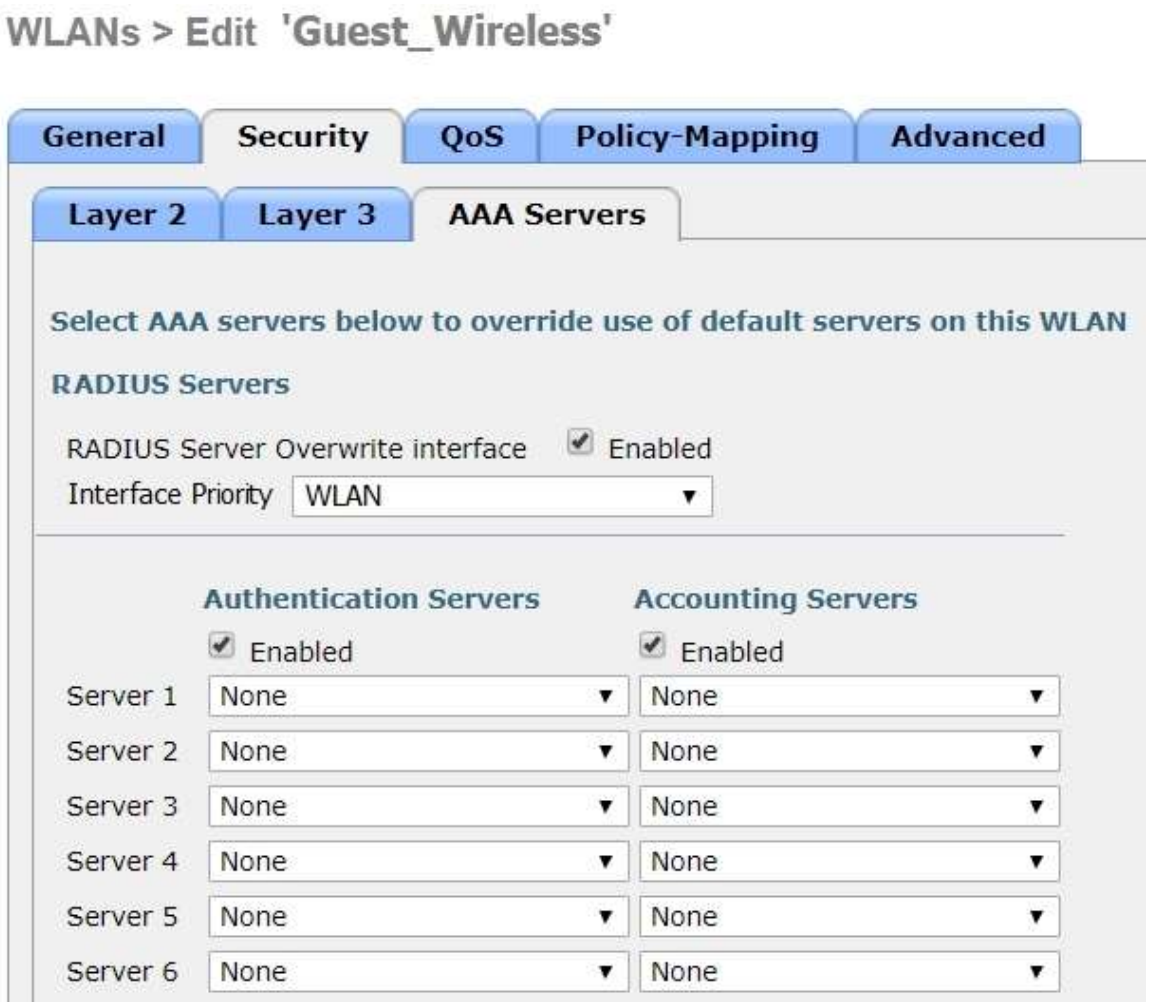
Answer: C
Explanation:
The Cisco DNA Center open platform for intent-based networking provides 360- degree extensibility across multiple components, including:
+ Intent-based APIs leverage the controller to enable business and IT applications to deliver intent to the network and to reap network analytics 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.
Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systemsmanagement/dna-center/nb-06-dna-cent-plat-sol-over-cte-en.html

QUESTION 156
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.

Answer: B

QUESTION 157
Refer to the exhibit. Assuming the WLC's interfaces are not in the same subnet as the RADIUS server, which interface would the WLC use as the source for all RADIUS-related traffic?



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

Answer: A

QUESTION 158
An engineer must protect their company against ransom ware attacks. Which solution allows the engineer to block the execution stage and prevent file encryption?

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

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/ampfor-endpoints/white-paper-c11-740980.pdf

QUESTION 159
Wireless users report frequent disconnections from the wireless network. While troubleshooting a network engineer finds that after the user a disconnect, the connection re-establishes automatically without any input required. The engineer also notices these message logs .

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

Which action reduces the user impact?

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

Answer: D
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.

QUESTION 160
Which algorithms are used to secure REST API from brute attacks and minimize the impact?

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

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

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

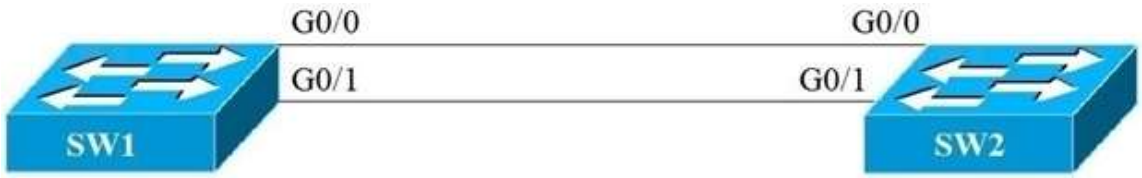
QUESTION 161
Company policy restricts VLAN 10 to be allowed only on SW1 and SW2. All other VLANs can be on all three switches. An administrator has noticed that VLAN 10 has propagated to SW3.
Which configuration corrects the issue?



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

Answer: C

QUESTION 162
Refer to the exhibit. An engineer reconfigures the pot-channel between SW1 and SW2 from an access port to a trunk and immediately notices this error in SW1's log.



Which command set resolves this error?

A. SW1(config-if)#**interface G0/0**
SW1(config-if)#**no spanning-tree bpdufilter**
SW1(config-if)#**shut**
SW1(config-if)#**no shut**
B. SW1(config-if)#**interface G0/0**
SW1(config-if)#**no spanning-tree bpduguard enable**
SW1(config-if)#**shut**
SW1(config-if)#**no shut**

C. SW1(config-if)#**interface G0/0**
SW1(config-if)#**spanning-tree bpduguard enable**
SW1(config-if)#**shut**
SW1(config-if)#**no shut**
D. SW1(config-if)#**interface G0/1**
SW1(config-if)#**spanning-tree bpduguard enable**
SW1(config-if)#**shut**
SW1(config-if)#**no shut**

Answer: B

QUESTION 163
A company plans to implement intent-based networking in its campus infrastructure. Which design facilities a migrate from a traditional campus design to a programmer fabric designer?

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

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).

QUESTION 164
Which two entities are Type 1 hypervisors? (Choose two.)

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

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)

QUESTION 165
A network administrator applies the following configuration to an IOS device:

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

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

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

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).

QUESTION 166
Which devices does Cisco Center configure when deploying an IP-based access control policy?

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

Answer: A
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: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automationand-management/dna-center/1-3-1-0/user_guide/b_cisco_dna_center_ug_1_3_1_0/b_cisco_dna_center_ug_1_3_1_0_chapter_01011.html

QUESTION 167
A network administrator is preparing a Python scrip 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 he in client manager prevent colleague making changes to the device while the scrip is running?

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

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.

QUESTION 168
Which component handles the orchestration plane of the Cisco SD-WAN?

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

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.

QUESTION 169
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

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.

QUESTION 170

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

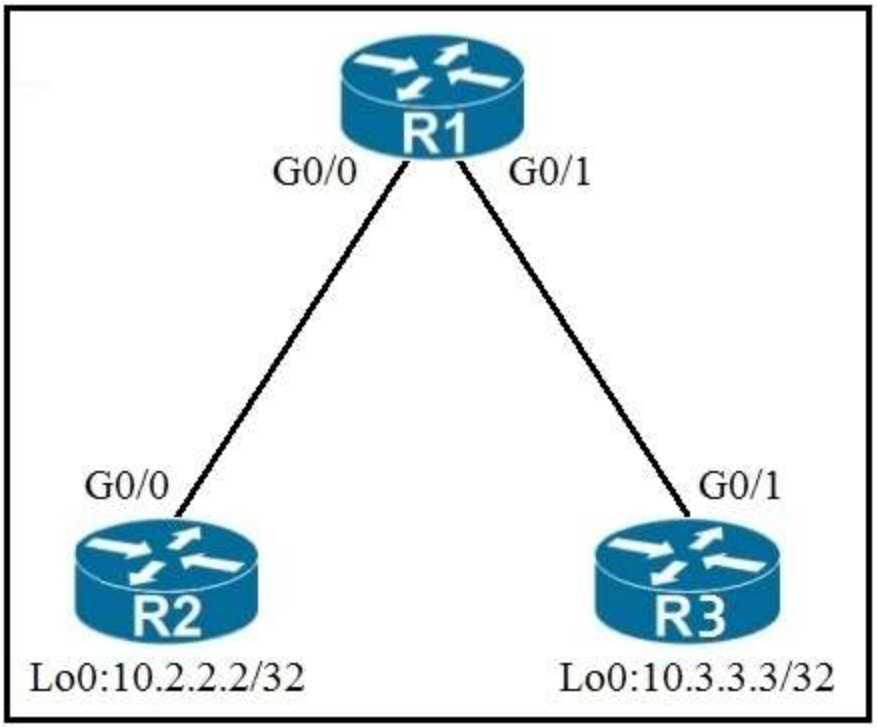
Answer: D
Explanation:
Intra-Controller Roaming: Each controller supports same-controller client roaming across access points managed by the same controller. This roaming is transparent to the client as the session is sustained, and the client continues using the same DHCP-assigned or client-assigned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

QUESTION 171
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

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. 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.

QUESTION 172
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 G0/1**
R3(config-if)#**ip access-group 150 out**

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

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

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

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

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

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

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

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

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

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

QUESTION 173
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?




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

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

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**

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.

QUESTION 174
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.

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.

QUESTION 175
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.

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 spare 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.

QUESTION 176
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

Answer: DE

QUESTION 177
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

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.

QUESTION 178
In a Cisco SD-WAN solution, how is the health of a data plane tunnel monitored?

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

Answer: C

QUESTION 179
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

Answer: AC

QUESTION 180
In an SD-WAN deployment, which action in the vSmart controller responsible for?

A. handle, maintain, and gather configuration and status for nodes within the SD-WAN fabric
B. distribute policies that govern data forwarding performed within the SD-WAN fabric

C. gather telemetry data from vEdge routers
D. onboard vEdge nodes into the SD-WAN fabric

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.

QUESTION 181
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

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.

QUESTION 182
Which protocol is responsible for data plane forwarding in a Cisco SD-Access deployment?

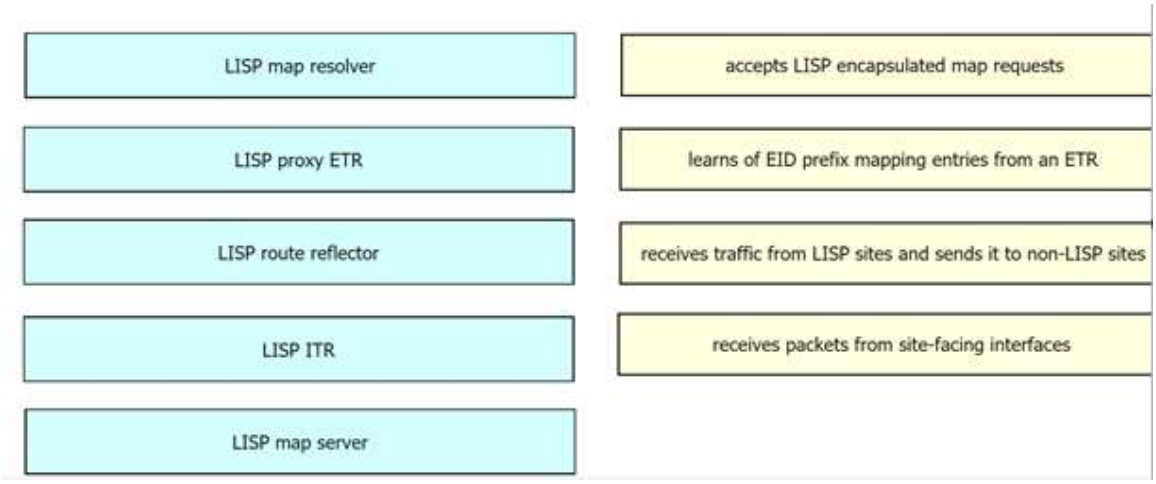
A. VXLAN
B. IS-IS
C. OSPF
D. LISP

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.

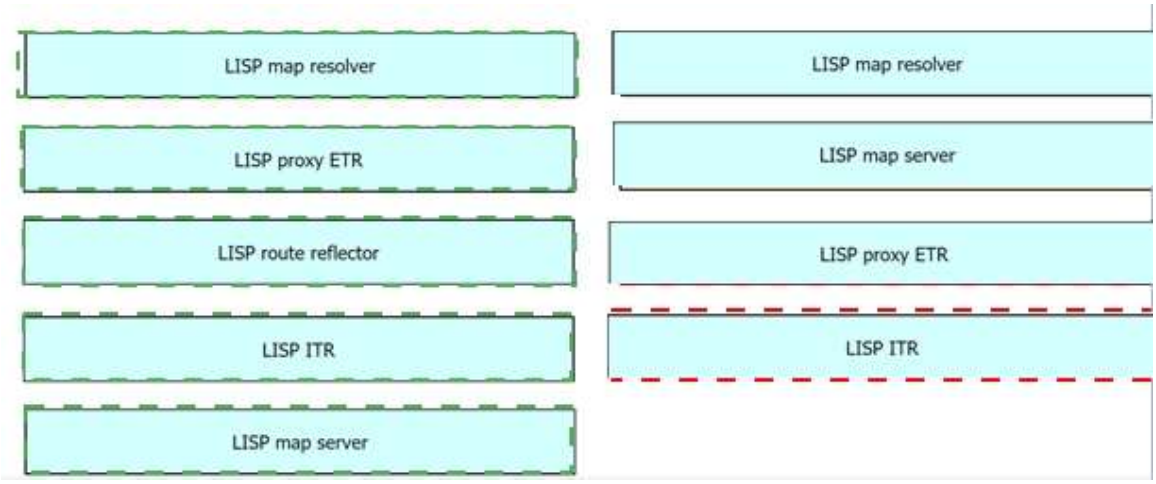
QUESTION 183
Drag and Drop Question

Drag and drop the LISP components from the left onto the function they perform on the right. Not

all options are used.

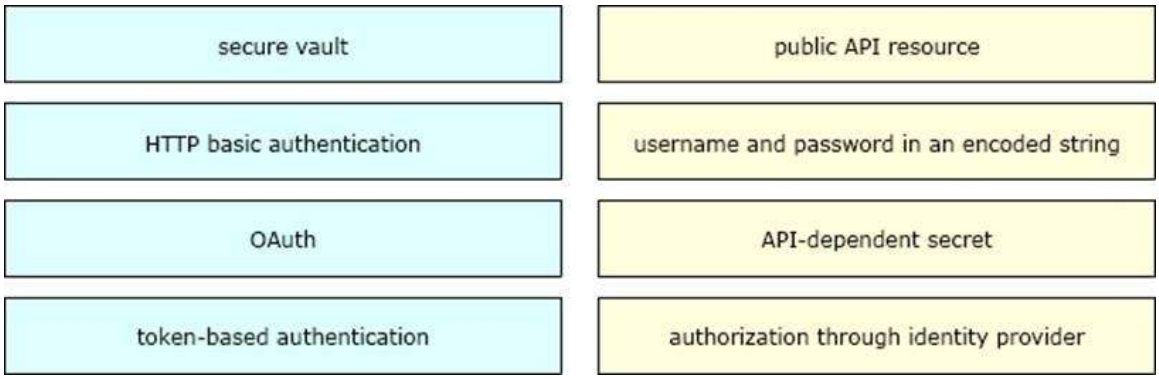


Answer:

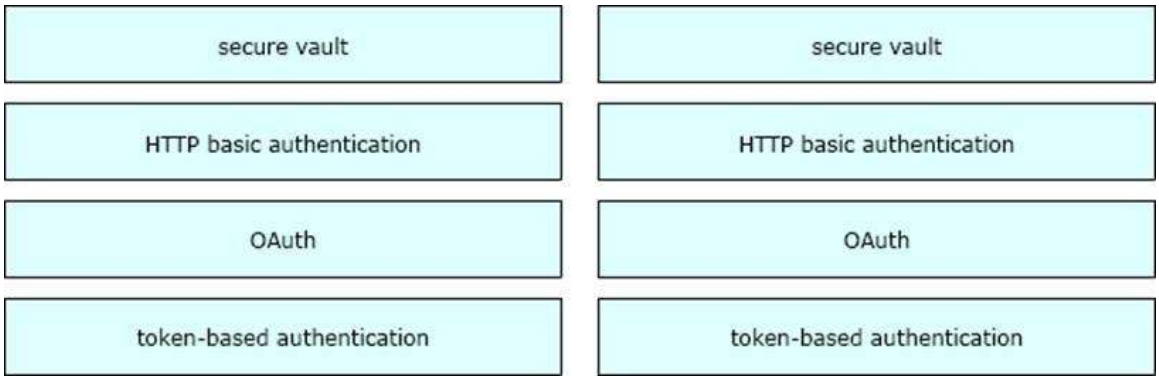


QUESTION 184
Drag and Drop Question

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



Answer:



QUESTION 185
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

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).

QUESTION 186
Which characteristic distinguishes Ansible from Chef?

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

Answer: C

QUESTION 187
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

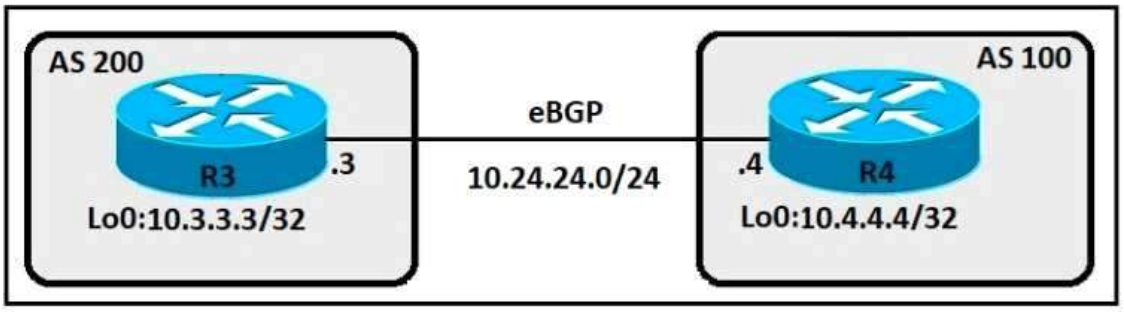
Answer: C
Explanation:
The established keyword is only applicable to TCP access list entries to match TCP segments that have the ACK and/or RST control bit set (regardless of the source and destination ports), which assumes that a TCP connection has already been established in one direction only. Let's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

QUESTION 188
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

Answer: C

QUESTION 189
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?



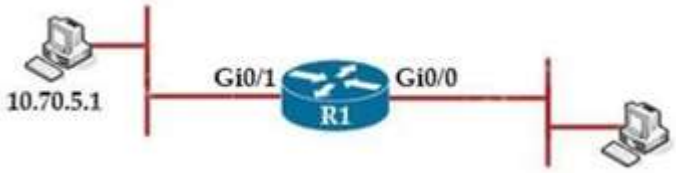
A. R3(config)#router bgp 200
R3(config-router)#neighbor 10.24.24.4 remote-as 100
R3(config-router)#bgp router-id 10.3.3.3
R4(config)#router bgp 100
R4(config-router)#neighbor 10.24.24.3 remote-as 200
R4(config-router)#bgp router-id 10.4.4.4
B. R3(config)#router bgp 200

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

Answer: A

QUESTION 190
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 pat outside
R1(config)#interface GigabitEthernet0/1
R1(config)#ip pat inside

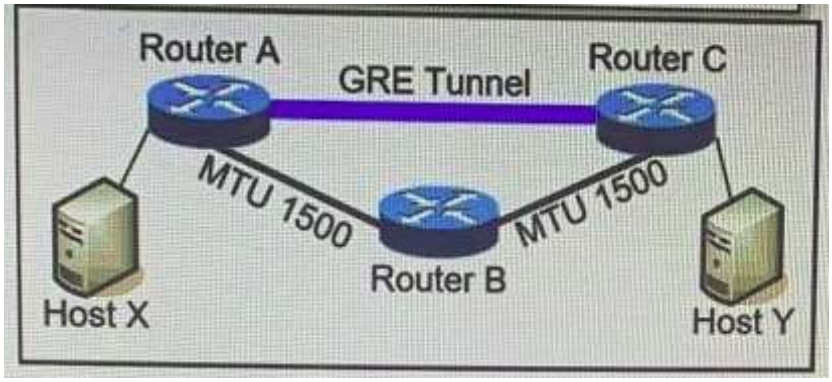
B. R1(config)#interface GigabitEthernet0/0
R1(config)#ip nat outside
R1(config)#interface GigabitEthernet0/1
R1(config)#ip nat inside

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

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

Answer: B

QUESTION 191
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-bye IPv4 packet traverses the GRE tunnel from host X to host Y, assuming the DF bit is cleared?



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

Answer: D
Explanation:

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

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

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

QUESTION 192
What is used to measure the total output energy of a Wi-Fi device?

A. dBi
B. EIRP
C. mW
D. dBm

Answer: C
Explanation:
Output power is measured in mW (milliwatts). answer 'dBi' milliwatt is equal to one thousandth (10−3) of a watt.

QUESTION 193
Drag and Drop Question

Drag and drop the Qos mechanisms from the left to the correct descriptions on the right.

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

Answer:

service policy	shaping
shaping	policy map
DSCP	DSCP
policy map	service policy
policing	policing
CoS	CoS

QUESTION 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

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: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-5/user_guide/b_dnac_ug_1_2_5/b_dnac_ug_1_2_4_chapter_0110.html

QUESTION 195
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

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

QUESTION 196
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.

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:
http://www.cisco.com/web/about/security/intelligence/acl-logging.html

QUESTION 197
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: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa1/0/7
 with BPDU Guard enabled. Disabling port.
*Mar  3 07:29:24.854: %PM-4-ERR_DISABLE: bpduguard error detected on Fa1/0/7, put
 ting Fa1/0/7 in err-disable state
*Mar  3 07:29:24.879: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa1/0/7
 with BPDU Guard enabled. Disabling port.
*Mar  3 07:29:25.869: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtherne
 t1/0/7, changed state to down
*Mar  3 07:29:26.884: %LINK-3-UPDOWN: Interface FastEthernet1/0/7, changed state
 to down
```

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

Answer: A
Explanation:

Seems someone maybe trying to insert a switch into that port which sends bpdu 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 bpdu's is still active on the port.

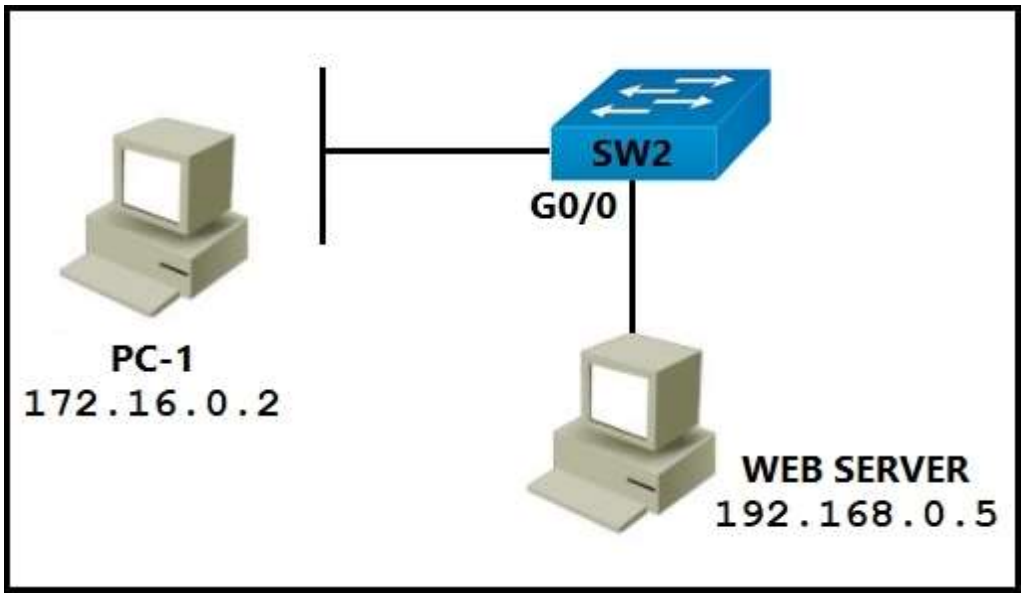
QUESTION 198
How does the RIB differ from the FIB?

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.

Answer: A
Explanation:
RIB is derived from the control plane,
FIB is used for forwarding,

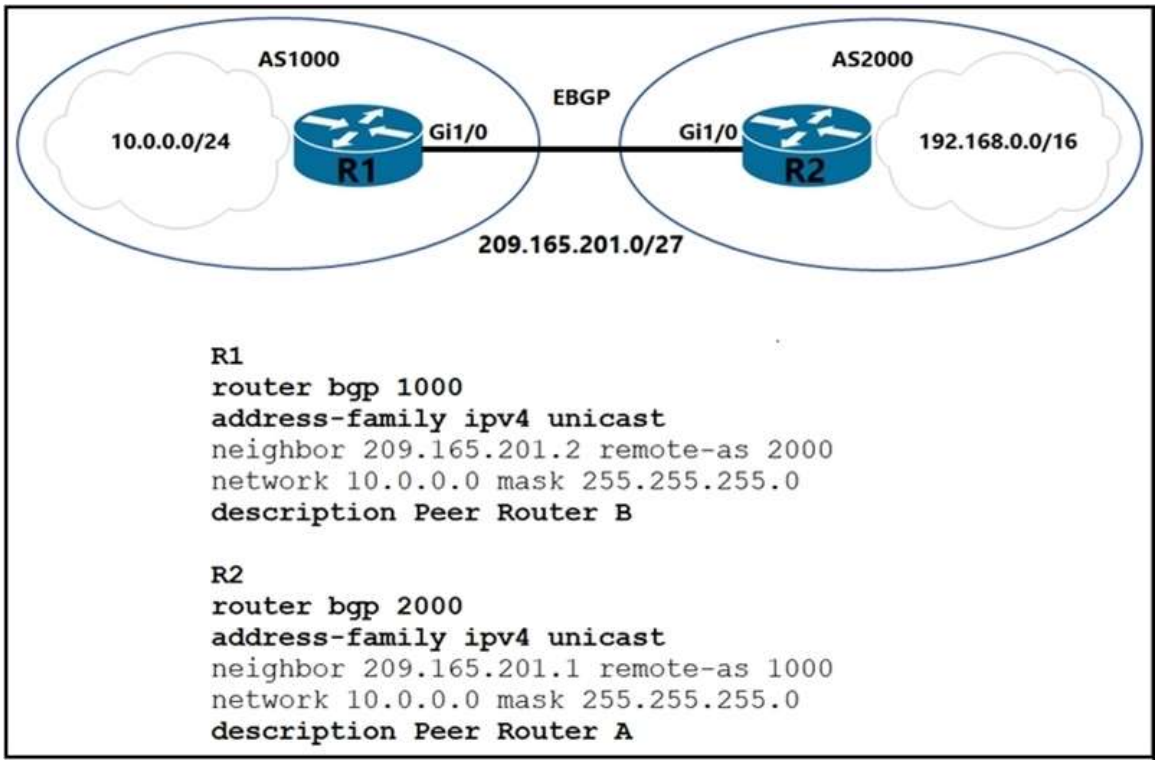
QUESTION 199
Refer to the exhibit. PC-1 must access the web server on port 8080. To allow this traffic, which statement must be added to an access control list that is applied on SW2 port G0/0 in the inbound direction?



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

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

QUESTION 200
Refer to the exhibit. Which two commands are needed to allow for full reachability between AS 1000 and AS 2000? (Choose two)




```
R1
router bgp 1000
address-family ipv4 unicast
neighbor 209.165.201.2 remote-as 2000
network 10.0.0.0 mask 255.255.255.0
description Peer Router B

R2
router bgp 2000
address-family ipv4 unicast
neighbor 209.165.201.1 remote-as 1000
network 10.0.0.0 mask 255.255.255.0
description Peer Router A
```

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 19.168.0.0 mask 255.255.0.0
D. R2#network 209.165.201.0 mask 255.255.192.0
E. R1#no network 10.0.0.0 255.255.255.0

Answer: BC

QUESTION 201
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.

Answer: A
Explanation:

3. Missing Data Model RPC Error Reply Message

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

Tip: Use the NETCONF capabilities functionality to determine whicl

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

QUESTION 202
Witch 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.

Answer: BD

QUESTION 203
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-day)
    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.

Answer: A

QUESTION 204
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

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).

QUESTION 205
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.

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.

QUESTION 206
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=GigabitEthernet2</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

Answer: C
Explanation:

External RESTful services return common HTTP response codes as described in the tables below. In addition to the status codes returned in the response header, each response may have additional content (in JSON format) according to the nature of the request.

This response can have several causes, and here are some common ones:

- The content-type header is missing
- Content-type does not match the submitted body data
- Submitted body data does not respect the JSON or XML format

QUESTION 207
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.

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

Which command set resolves this issue?

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

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
```

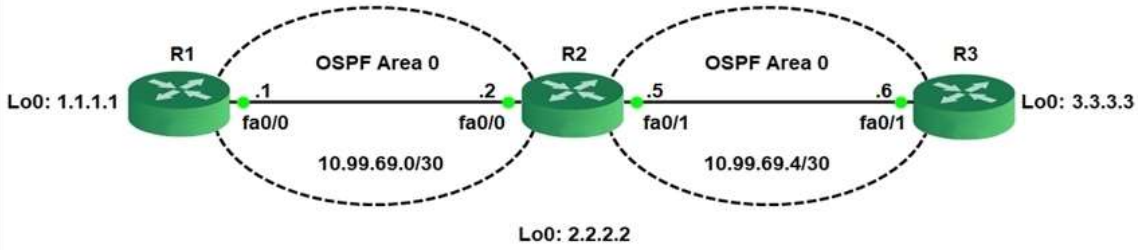
C.
```
interface Vlan10
no ip vrf forwarding Clients
ip address 192.168.1.2. 255.255.255.0
!
interface Vlan20
no ip vrf forwarding Servers
ip address 172.16.1.2 255.255.255.0
!
interface Vlan30
no ip vrf forwarding Printers
ip address 10.1.1.2 255.255.255.0
```

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

Answer: C

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

QUESTION 208
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

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.

QUESTION 209
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, white the routing protocol reconverges.
D. It enables HSRP to failover to the standby RP on the same device.

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: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-s/fhp-15-s-book/fhp-hsrp-sso.html

QUESTION 210
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

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.

QUESTION 211
An engineer configures monitoring on SW1 and enters the show command to verify operation. What does the output confirm?

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

Type                   : Remote Destination Session
Source RSPAN VLAN      : 50

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

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

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

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).

QUESTION 212
Which outbound access list, applied to the WAN interface of a router, permits all traffic except for

http traffic sourced from the workstation with IP address 10.10.10.1?

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

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

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

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

Answer: A

QUESTION 213
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

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: https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/intent-api-northbound

QUESTION 214
Refer to the exhibit. An engineer must create a configuration that executes the show run command and then terminates the session when user CCNP legs in.
Which configuration change is required?

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

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

D. Add the autocommand keyword to the aaa authentication command

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

QUESTION 215
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+

Answer: D

QUESTION 216
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

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.

QUESTION 217
Which three methods does Cisco DNA Centre use to discover devices? (Choose three)

A. CDP
B. SNMP

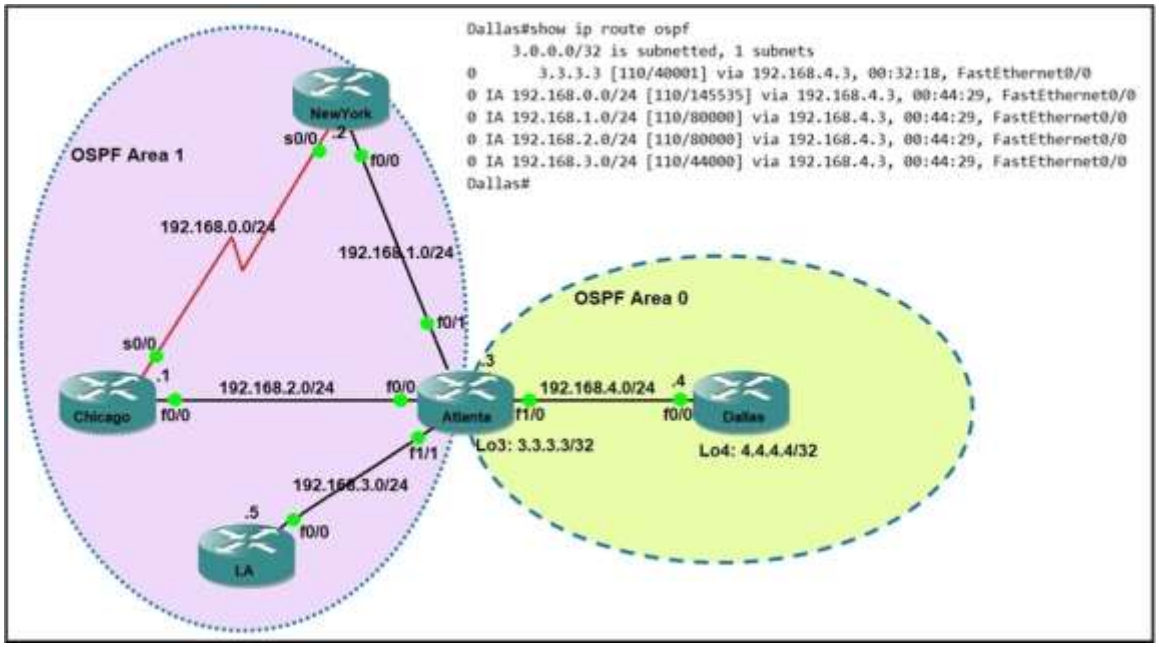
C. LLDP
D. ping
E. NETCONF
F. a specified range of IP addresses

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.

QUESTION 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?



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

Answer: C

QUESTION 219
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
Virutal 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
Virutal IP address is 192.168.0.1
Active virtual MAC address is 0000.0c07.ac0a

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

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.

QUESTION 220
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 A 38-24-044.40
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

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.

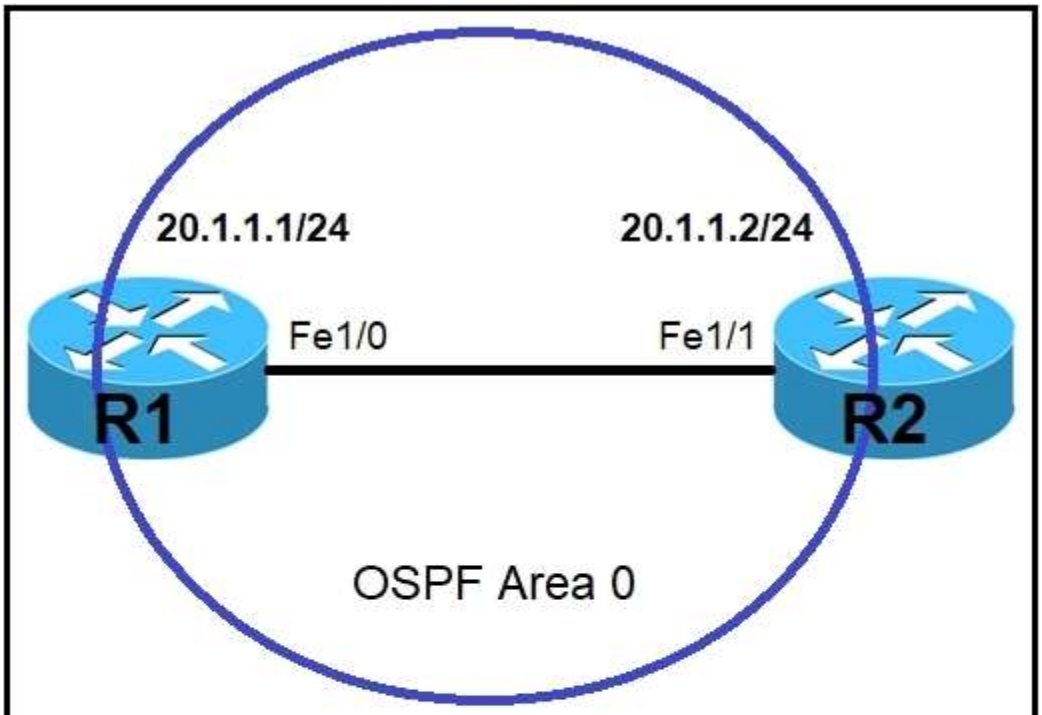
QUESTION 221
What are two reasons a company would choose a cloud deployment over an on-prem deployment? (Choose Two)

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

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

QUESTION 222
Refer to the exhibit. Which command must be applied to R2 for an OSPF neighborship to form?

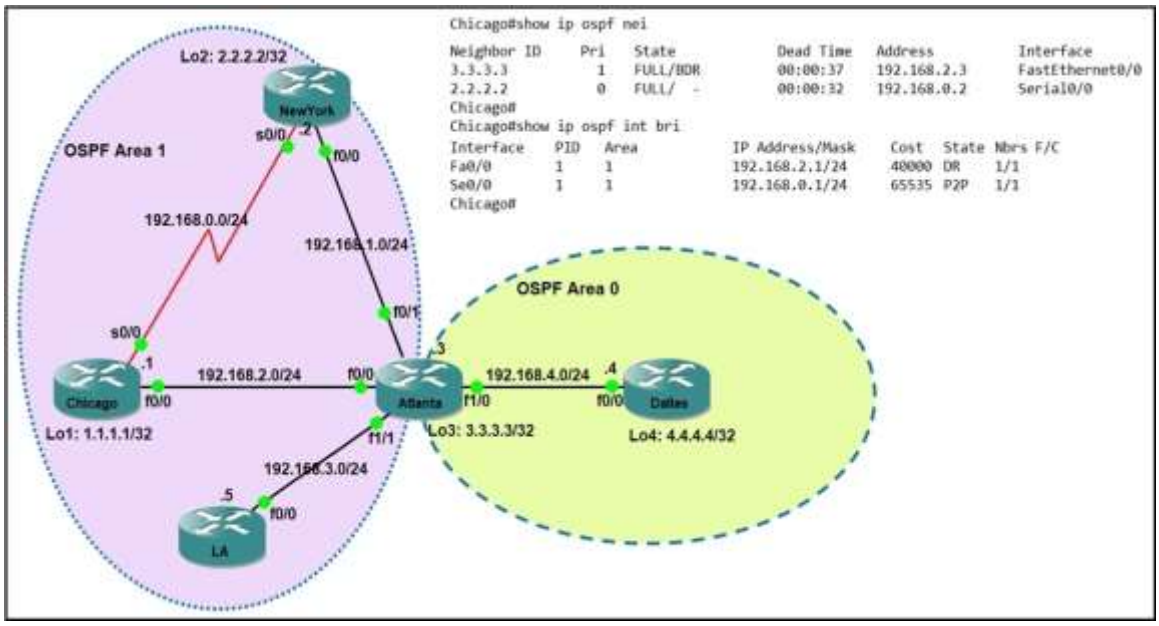



```
hostname R1
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
auto-cost reference-bandwidth 1000
!
hostname R2
router ospf 2
network 20.0.0.0 0.0.0.255 area 0
```

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

Answer: A

QUESTION 223
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

Answer: B
Explanation:
This segment has no designated router because it is a p2p network type." It is clearly seen on the output that this is a serial point to point link LOL which requires no DR/BDR. Also, a non-broadcast network type actually calls for a DR/BDR. Not sure what they were thinking.
OSPF recognizes the following network types:

Broadcast
Non-Broadcast
Point to Multipoint (Broadcast)
Point to Multipoint (Non-Broadcast)
Point to Point

Out of all of those possibilities, only Broadcast and Non-Broadcast form DRs and BDRs. The Broadcast and Non-Broadcast network types describe a multi-access network media, such as Ethernet. In this case OSPF requires that all routers on the same network segment have direct reachability both to the DR and BDR, otherwise the network will break.

QUESTION 224
Which antenna type should be used for a site-to-site wireless connection?

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

Answer: D

Explanation:

Yagi Antenna

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

QUESTION 225

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

```
DSW1#sh 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         128.9    P2p Bound (PVST)
Fa1/0/10            Desg FWD 2         128.12   P2p Bound (PVST)
Fa1/0/11            Root FWD 2         128.13   P2p
Fa1/0/12            Altn BLK 2         128.14   P2p
```

```
DSW#1sh spanning-tree mst

##### MST1    vlans mapped:   10,20
Bridge        address 001b.0d8e.e080 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
!
```

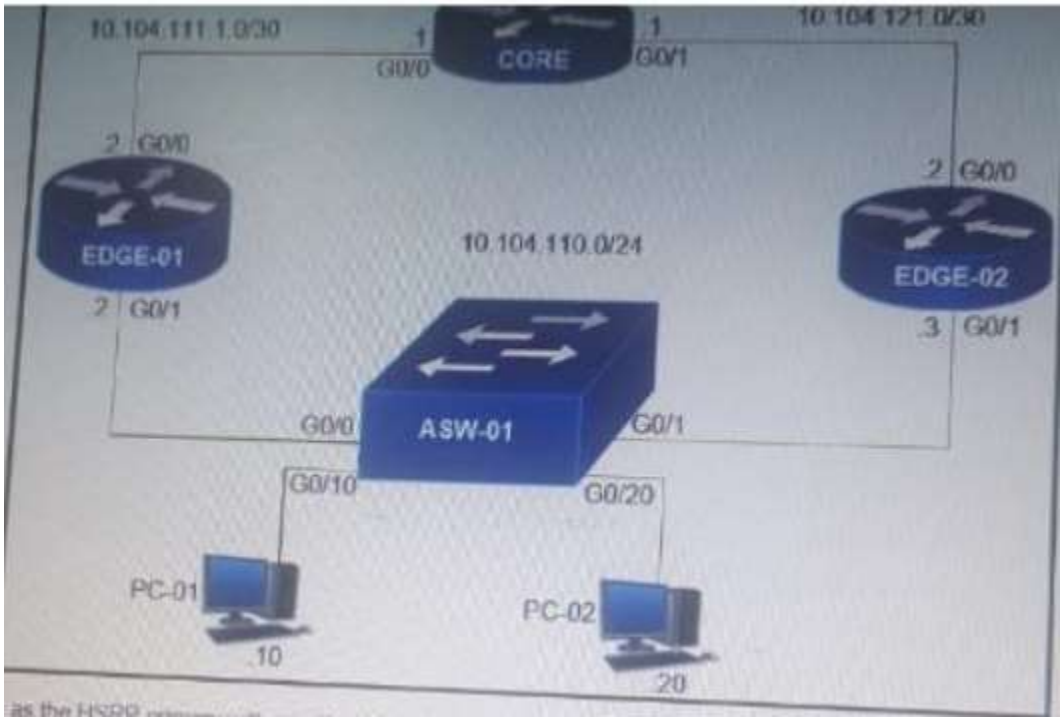
A. spanning-tree mst 1 priority 1
B. spanning-tree mst 1 root primary
C. spanning-tree mstp vlan 10,20 root primary
D. spanning-tree mst vlan 10,20 priority root
E. spanning-tree mst 1 priority 4096

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.

QUESTION 226
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

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

QUESTION 227
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.

Answer: C

QUESTION 228
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

Answer: ABD

QUESTION 229
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

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

QUESTION 230
Refer to the exhibit. A wireless client is connecting to FlexAP1 which is currently working standalone mode.

```
(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
```

The AAA authentication processis 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.

Answer: BCG
Explanation:
+ From the output of WLC show interface summary, we learned that the WLC has four VLANs: 999, 14, 15 and 16.
+ From the show ap config general FlexAP1 output, we learned that FlexConnect AP has four VLANs: 10, 11, 12 and 13. Also the WLAN of FlexConnect AP is mapped to VLAN 10 (from the line WLAN 1: ..... 10 (AP-Specific)).
From the reference at: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8- 1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide/ch7_HREA.html

QUESTION 231
Refer to the exhibit.

```
(YOUR CONNECTION IS NOT PRIVATE WARNING )
```

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

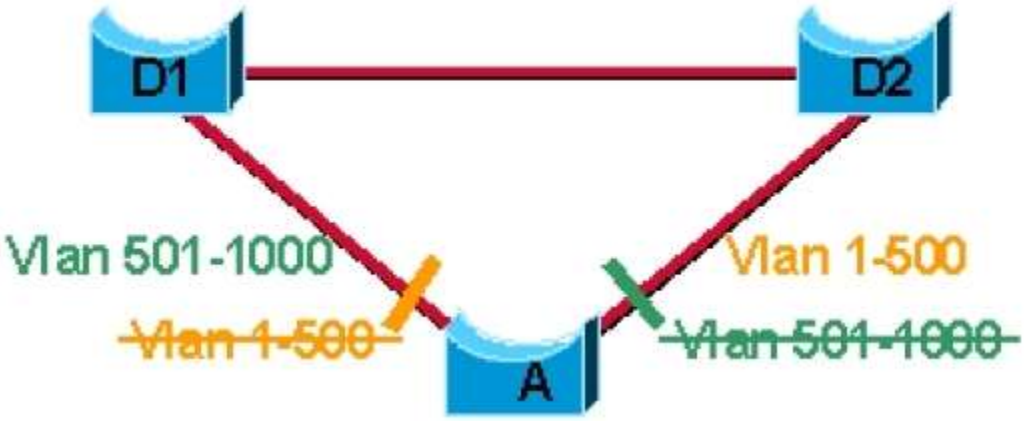
A. The server that is providing the portal has an expired certificate
B. The server that is providing the portal has a self-signed certificate
C. The connection is using an unsupported protocol
D. The connection is using an unsupported browser

Answer: B

QUESTION 232
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

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.
https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24248-147.html



QUESTION 233
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

Answer: C
Explanation:
Portfast feature should only be used on edge ports (ports directly connected to end stations). Neither edge ports or PortFast enabled ports generate topology changes when the link toggles so we cannot say Portfast reduces the STP convergence time.
PortFast causes a switch or trunk port to enter the spanning tree forwarding state immediately, bypassing the listening and learning states so answer 'It immediately puts the port into the forwarding state when the switch is reloaded ' is the best choice.

QUESTION 234
An engineer reviews a router's logs and discovers the following entry. What is the event's logging severity level?

```
Router# *Jan 01 38:24:04.401: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up
```

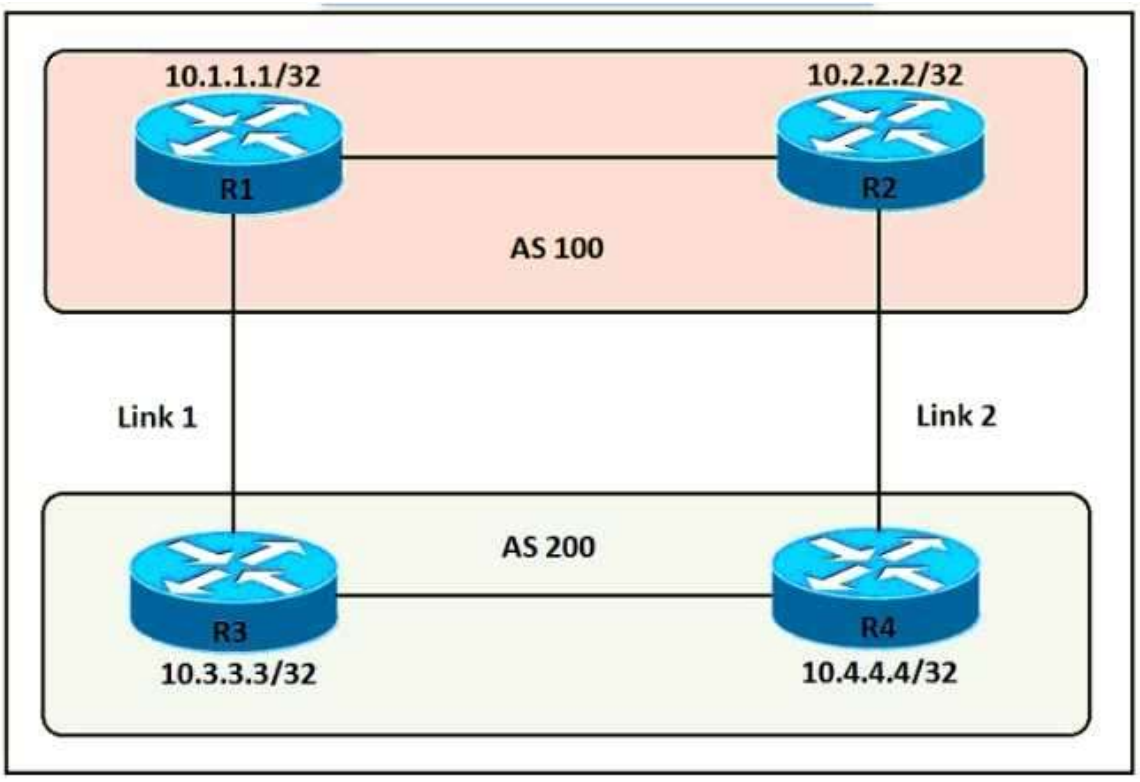
A. notification
B. error
C. informational
D. warning

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.

QUESTION 235
Refer to the exhibit. An engineer must ensure that all traffic leaving AS 200 will choose Link 2 as an entry point. Assuming that all BGP neighbor relationships have been formed and that the attributes have not been changed on any of the routers, which configuration accomplish task?



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

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

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

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

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

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

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

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

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

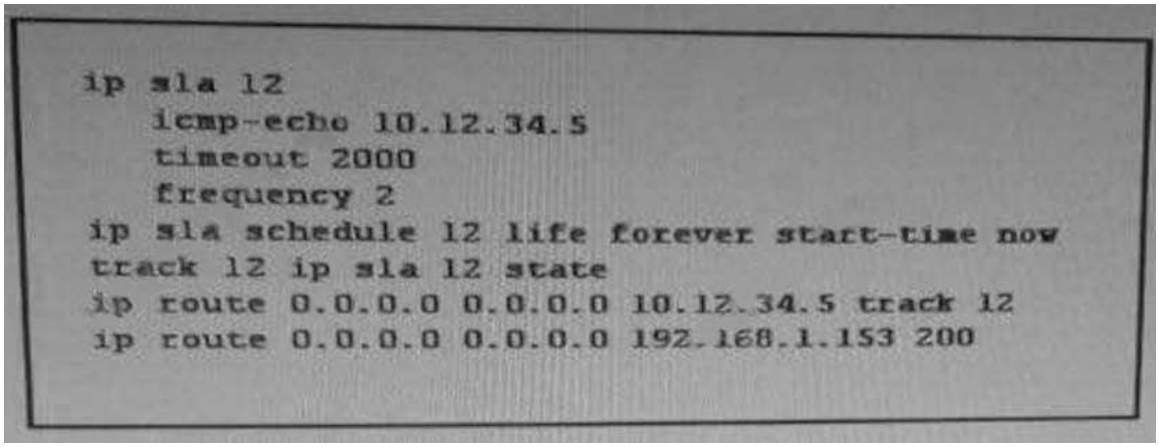
Answer: A

QUESTION 236
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

Answer: D

QUESTION 237
Refer to the exhibit. After you configure the given IP SLA on a Cisco router,you note that the device is unable to fialover to the backup route even when pings to 10.12.34.5 fail.
What action can you take to correct the problem?



A. Change the ip route 0.0.0.0 0.0.0.0 192.168.1.153 200 command to ip route 0.0.0.0 0.0.0.0 192.168.1.153 12.
B. Change the ip sla schedule 12 life forever start-time now command to ip sla schedule 12 life forever start-time 00:12:00.
C. Change the track 12 ip sla 12 state command to track 12 ip sla 12 reachability.
D. Change the frequency 2 command to frequency 12.

Answer: C

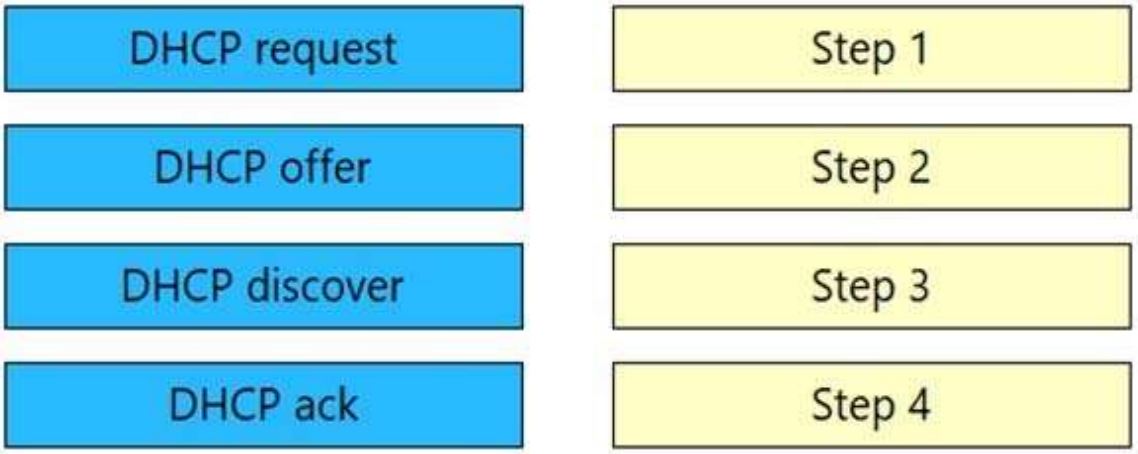
QUESTION 238
Which feature is supported by EIGRP but is not supported by OSPF?

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

Answer: C
Explanation:
EIGRP support unequal-cost load balancing via the "variance ..." while OSPF only supports equalcost load balancing.

QUESTION 239
Drag and Drop Question

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

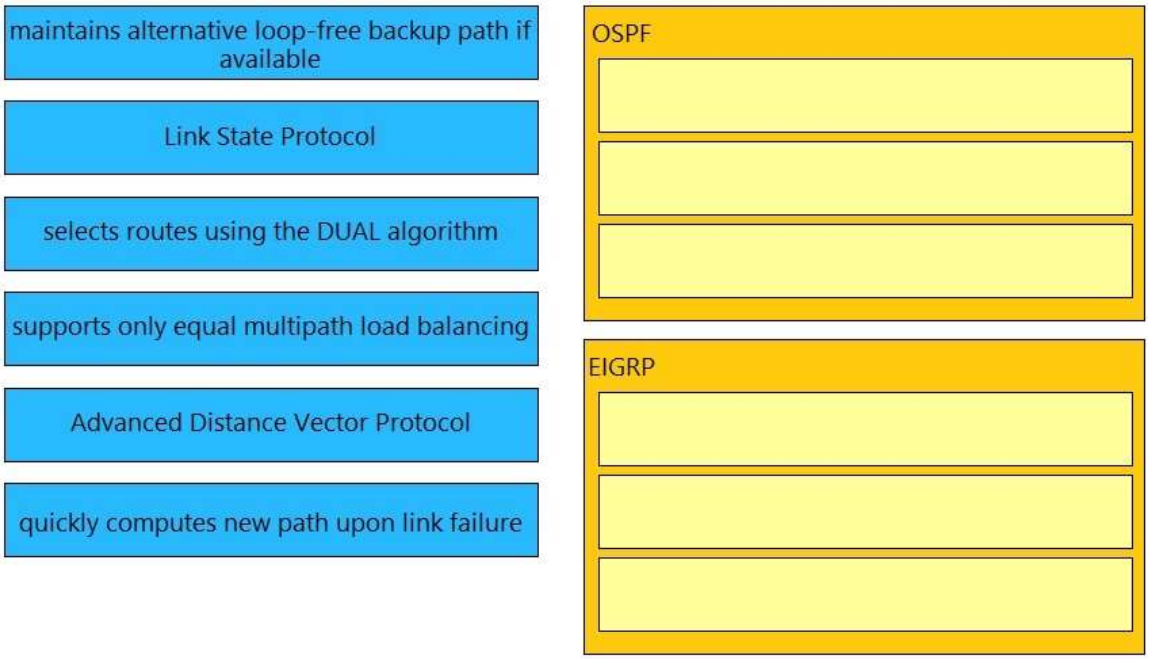


Answer:

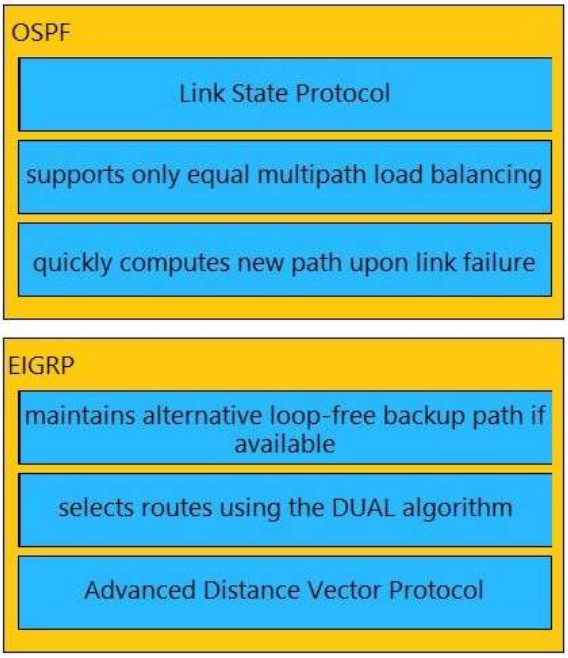


QUESTION 240
Drag and Drop Question

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



Answer:



QUESTION 241
Drag and Drop Question

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

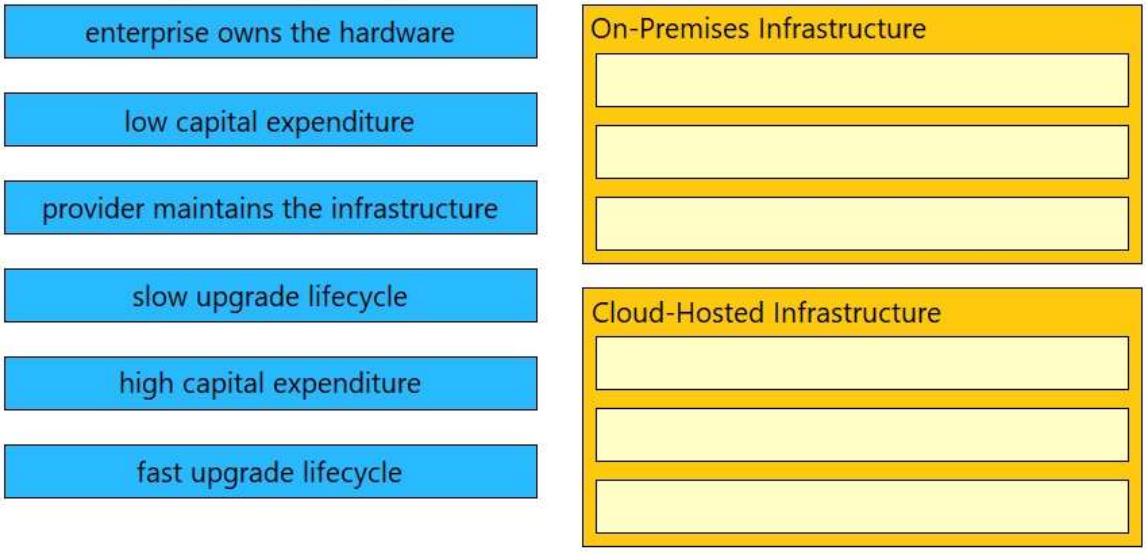
Umbrella	provides malware protection on endpoints
AMP4E	provides IPS/IDS capabilities
FTD	performs security analytics by collecting network flows
StealthWatch	protects against email threat vector
ESA	provides DNS protection

Answer:

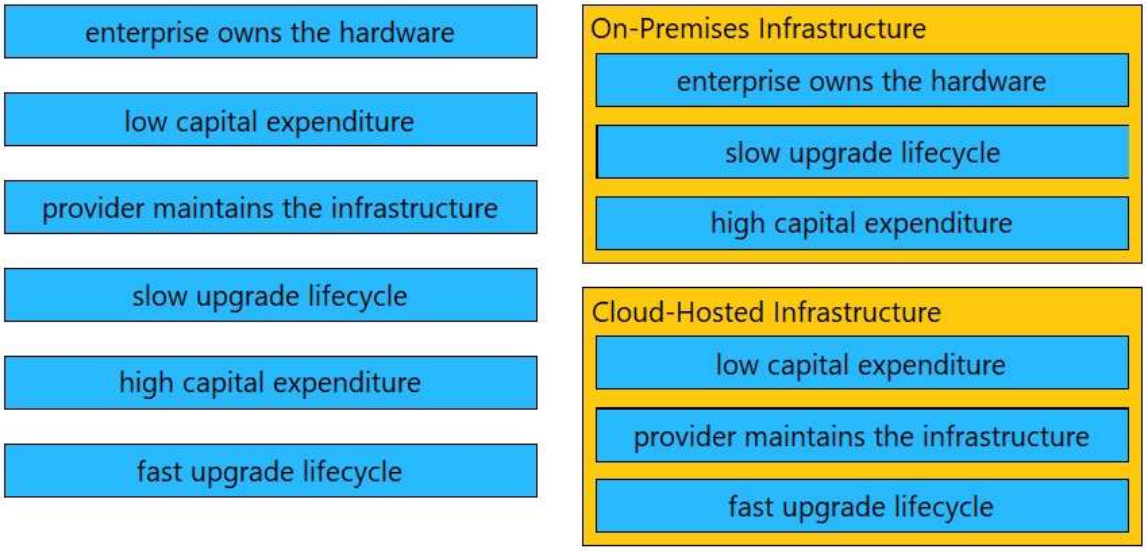
Umbrella	AMP4E
AMP4E	FTD
FTD	StealthWatch
StealthWatch	ESA
ESA	Umbrella

QUESTION 242
Drag and Drop Question

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



Answer:



QUESTION 243
Refer to the exhibit. This is the configuration of the ASBR of area 110.Which option explains why the remote ABR should not translate the type 7 LSA for the prefix 192.168.0.0/16 into a type 5 LSA?

```
router ospf 100
 router-id 4.4.4.4
 area 110 nssa
 summary-address 192.168.0.0 255.255.0.0 nssa-only
 redistribute static metric-type 1 subnets tag 704
 network 110.110.0.0 0.0.255.255 area 110
```

A. The remote ABR translates all type 7 LSA into type 5 LSA, regardless of any option configured in

the ASBR.
B. The ASBR sets the forwarding address to 0.0.0.0 which instructs the ABR not to translate the LSA into a type 5 LSA.
C. The ASBR originates a type 7 LSA with age equal to MAXAGE 3600.
D. The ABR clears the P bit in the header of the type 7 LSA for 192.168.0.0/16.

Answer: D

QUESTION 244
What is the function of an EIGRP sequence TLV packet?

A. to acknowledge a set of sequence numbers during the startup update process
B. to list the peers that should listen to the next multicast packet during the reliable multicast process
C. to list the peers that should not listen to the next multicast packet during the reliable multicast process
D. to define the initial sequence number when bringing up a new peer

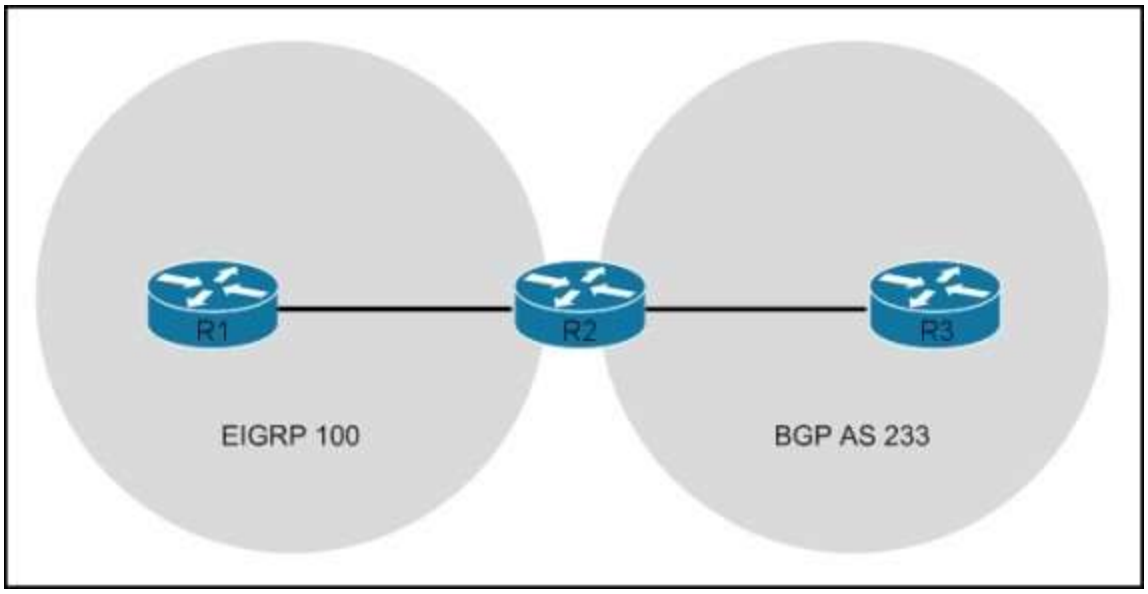
Answer: C

QUESTION 245
What are two reasons to define static peers in EIGRP? (Choose two.)

A. Security requirements do not allow dynamic learning of neighbors.
B. The link between peers requires multicast packets.
C. Back-level peers require static definition for successful connection.
D. The link between peers requires unicast packets.

Answer: AD

QUESTION 246
Refer to the exhibit. R2 is mutually redistributing between EIGRP and BGP.
Which configuration is necessary to enable R1 to see routes from R3?



A. The R3 configuration must include ebgp-multihop to the neighbor statement for R2.
B. The R2 BGP configuration must include bgp redistribute-internal.
C. R1 must be configured with next-hop-self for the neighbor going to R2.
D. The AS numbers configured on R1 and R2 must match.

Answer: B

QUESTION 247
What is the purpose of EIGRP summary leaking?

A. to allow a summary to be advertised conditionally on specific criteria
B. to allow a component of a summary to be advertised in addition to the summary
C. to allow overlapping summaries to exist on a single interface
D. to modify the metric of the summary based on which components of the summary are operational

Answer: B

QUESTION 248
Refer to the exhibit. Which statement about this IP SLA is true?

```
Entry number: 1
Owner:
Tag:
Type of operation to perform: echo
Target address/Source address: 172.16.129.9/0.0.0.0
Type of Service parameter: 0x0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Verify data: No
Vrf Name:
Schedule:
    Operation frequency (seconds): 10
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
History Statistics:
    Number of history Lives kept: 0
    Number of history Buckets kept: 15
    History Filter Type: None
Enhanced History:
```

A. The SLA must also have a schedule configured before it will start.
B. The TTL of the SLA packets is 10.
C. The SLA has a timeout of 3.6 seconds.
D. The SLA has a lifetime of 5 seconds.

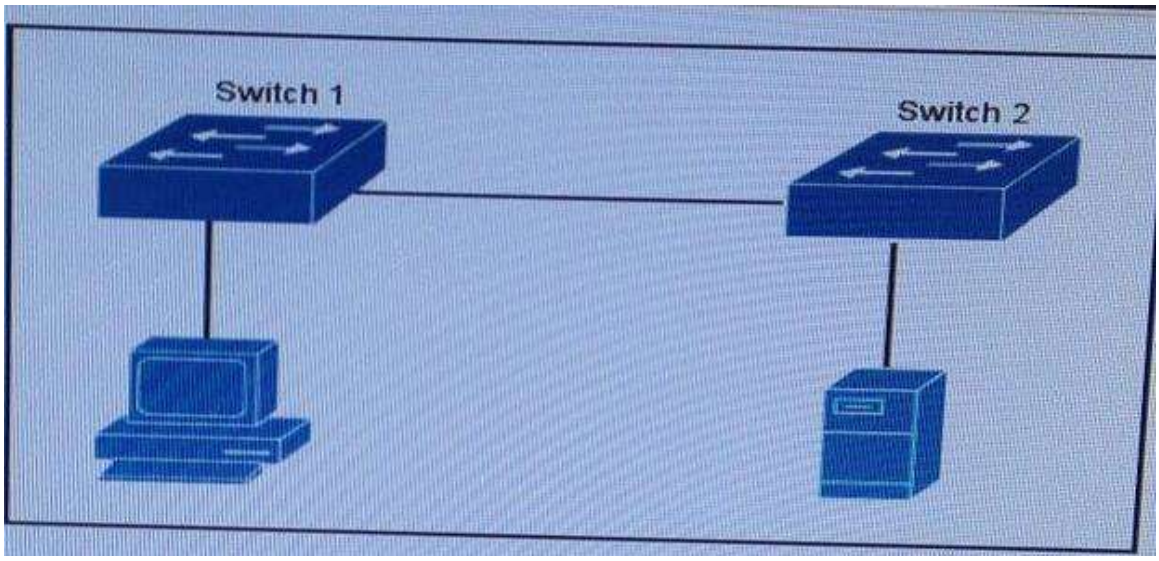
Answer: A

QUESTION 249
Which IP SLA operation type is enhanced by the use of the IP SLAs Responder?

A. DNS
B. HTTP
C. ICMP Echo
D. UDP Echo

Answer: D

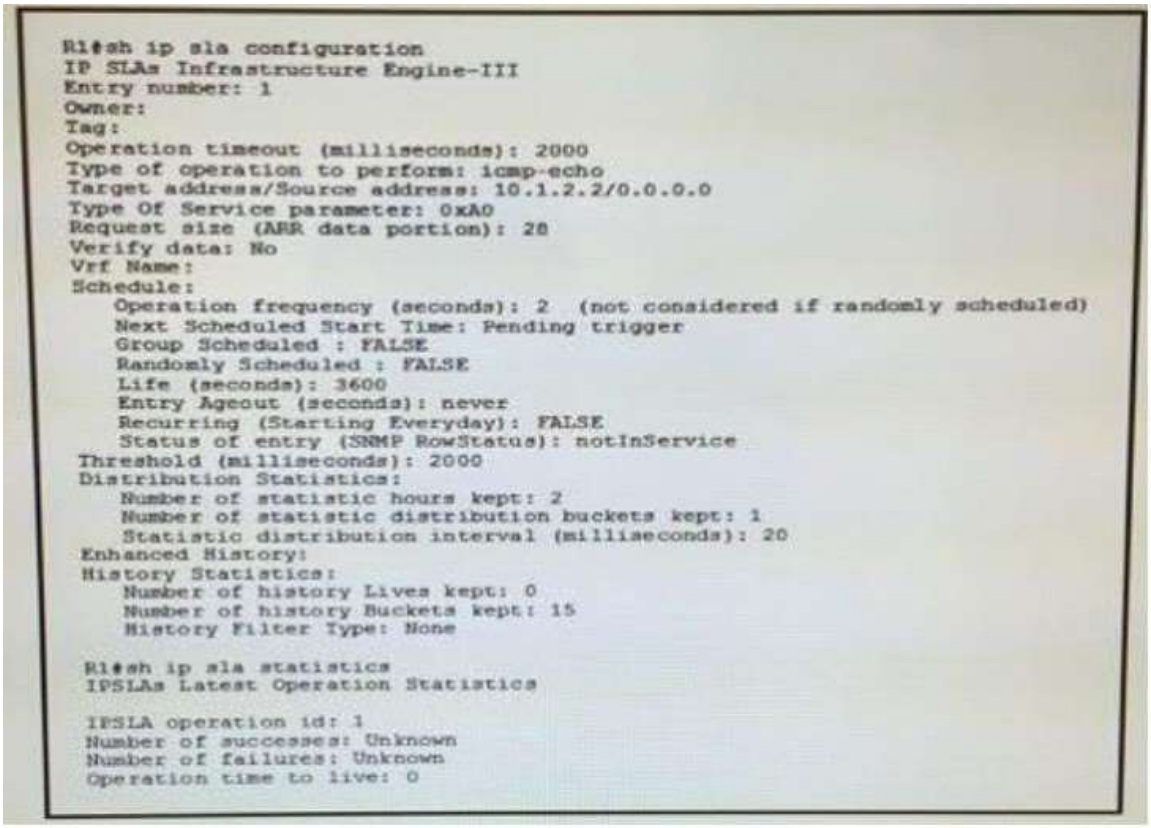
QUESTION 250
Refer to the exhibit, which type of connection does ERSPAN use to transport traffic from switch 1 to switch 2?



A. An SVI
B. A PPTP tunnel
C. A GRE tunnel
D. A VLAN

Answer: C

QUESTION 251
Refer to the exhibit. For which reason could the statistics for IP SLA operation 1 be unknown?



A. The ICMP echoes were lost in transit
B. Data verification has been disabled
C. The Type of Service parameter is configured incorrectly.
D. The Operation Frequency value is the same as the Operation Timeout value.
E. The IP SLA schedule is missing.

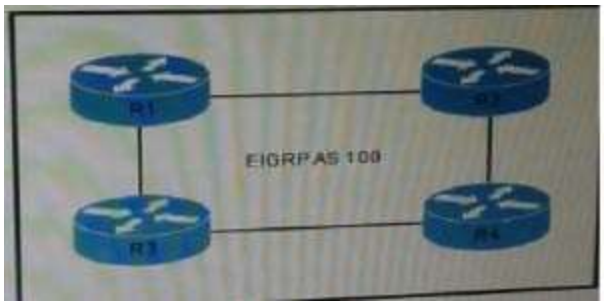
Answer: E

QUESTION 252
Which two OSPF network type require the use of a DR and BDR? (Choose two)

A. non-broadcast networks
B. point-to-point networks
C. point-to-point non-broadcast networks
D. broadcast networks
E. point-to-multipoint networks

Answer: AD

QUESTION 253
Refer to the exhibit. If this network is in the process of being migrated from EIGRP to OSPF, and all routers are now running both protocols, which action must you perform to complete the migration?



A. Change the EIGRP administrative distance to 95
B. Change the OSPF administrative distance to 95
C. Change the OSPF administrative distance to 115
D. Change the EIGRP administrative distance to 115

Answer: D

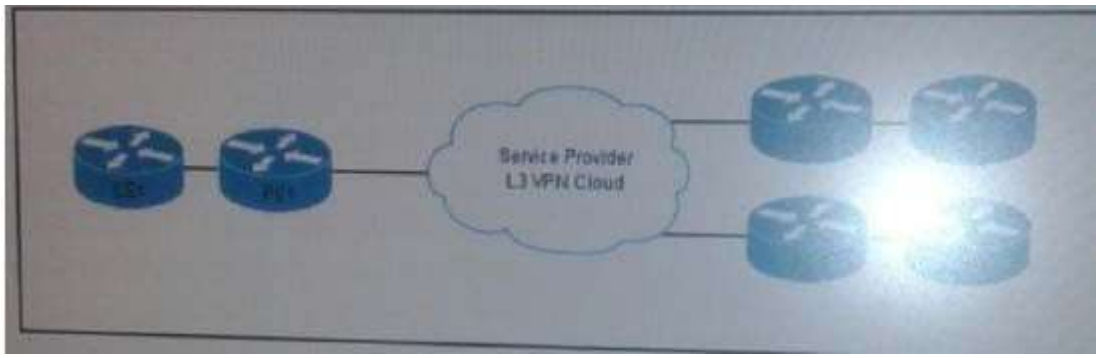
QUESTION 254
Refer to the exhibit. While troubleshooting an issue with a blocked switch port, you find this error in the switch log. Which action should you take first to locate the problem?

```
SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port FastEthernet0/1
in VLAN 10. Moved to loop-inconsistent state
```

A. Check the attached switch for a BPDU filter.
B. Test the link for unidirectional failures.
C. Execute the show interface command to check FastEthernet0/1.
D. Check the attached switch for an interface configuration issue.

Answer: A

QUESTION 255
Refer to the exhibit. How can you configure this network so that customers can transparently extend their networks through the provider?

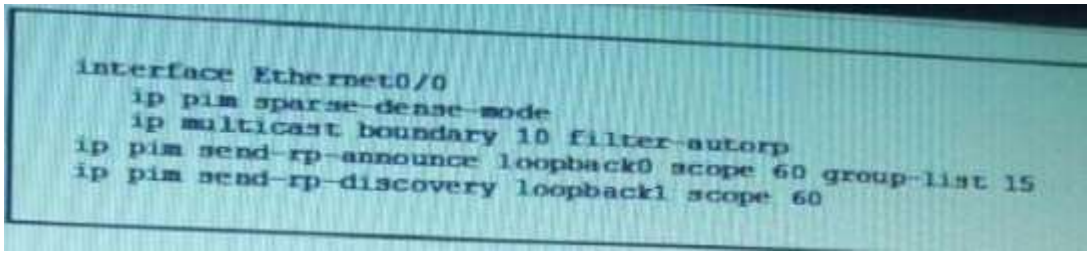


A. Configure eBGP peering among the CE routers.
B. Configure EIGRP OTP on the CE routers.
C. Configure eBGP peering between the CE and PE routers.

D. Configure OSPF peering between the CE and PE routers.

Answer: B

QUESTION 256
Refer to the exhibit. Which two effects of this configuration are true? (Choose 2)



A. It creates an administratively scoped boundary for ACL 60.
B. It sets the TTL for discovery messages to 60 hops.
C. It prevent the device from falling back to dense mode.
D. It sets announcement interval to 60 seconds.
E. It configure the router as the rendezvous point.

Answer: BE

QUESTION 257
Refer to the exhibit.

```
interface Ethernet 0/0
ip policy routemap PBR routemap PBR
match ip address 144
set ip nexthop 172.16.12.5
set ip nexthop recursive 192.168.3.2
```

Which statement describes how a router with this configuration treats packets if the devices at 172.16.12.5 and 192.168.3.2 are unreachable?

A. It routes the packet using the default routing table.
B. It routes the packet into a loop and drops it when the TTL reaches zero.
C. It drops the packet immediately.
D. It sends an ICMP source quench message.

Answer: A

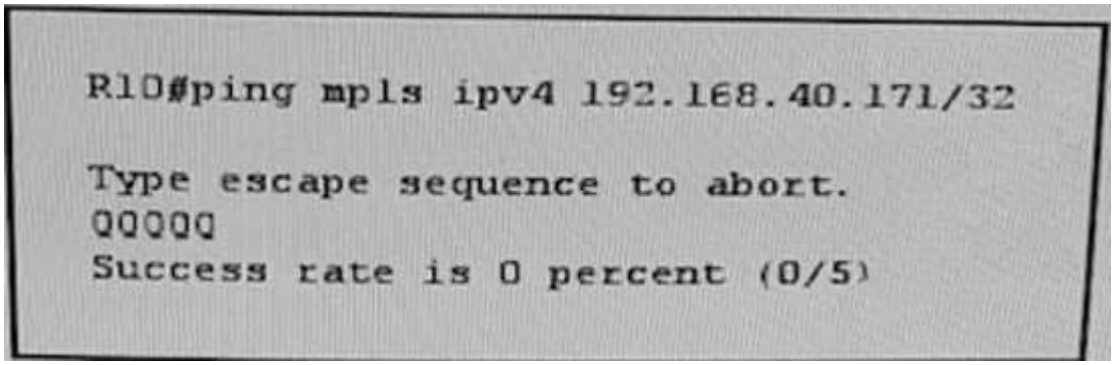
QUESTION 258
Which two statements about redistribution are true? (Choose two)

A. When BGP traffic is redistributed into OSPF eBGP and iBGP routes are advertised.
B. When EIGRP routes on a CE are redistributed through a PE into BGP, the Cost Community POI is set automatically.
C. When EIGRP traffic is redistributed into BGP, a default metric is required.
D. When BGP traffic is redistribute into OSPF the metric is set to 1 unless the metric is defined.

E. iBGP routes automatically redistribute into IGP if the routes are in the routing table.
F. When OSPF traffic is redistributed into BGP internal and external routes are redistributed.

Answer: BD

QUESTION 259
Refer to the exhibit. Which two conclusions can you draw from this command and its output?(Choose two.)



A. R10 has a missing label binding for 192.168.40.171/32
B. The MPLS ping failed.
C. 192.168.40.171/32 exists in the global routing table.
D. A valid LSP exists,and it matches the corresponding MPLS FEC.
E. The MPLS ping was successful.
F. R10 has valid label bingding for 192.168.40.171/32

Answer: AB

QUESTION 260
Which two options are required parts of an EEM policy? (Choose two.)

A. event register keyword
B. body
C. environment must defines
D. namespace import
E. entry status
F. exit status

Answer: AB

QUESTION 261
Refer to the exhibit. Which result will the EEM applet in the exhibit produce?

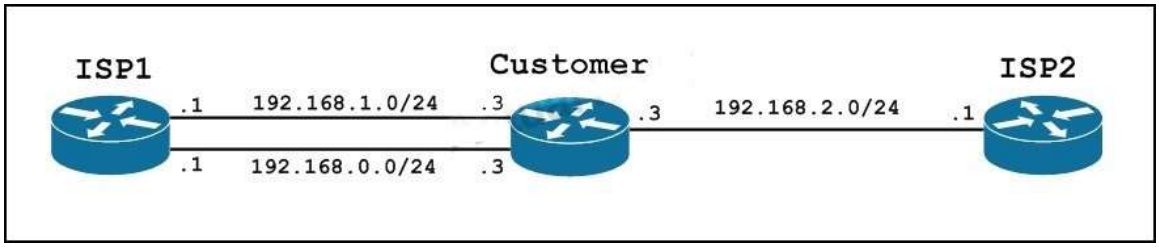
```
event manager applet CCIE
event timer cron name CCIE cron-entry  */5 * * * *
action 1 cli command "en"
action 2 cli command "show log"
```

lead2pass.com

A. The output of show version will be executed every 5 hours.
B. The output of show log will be executed every 5 hours.
C. The output of show log will be executed every Friday.
D. The output of show log will be executed every 5 minutes.

Answer: B
Explanation:
The cron entry indicates 5 hours. So the output of show log will be executed every 5 hours.

QUESTION 262
Refer to the exhibit. The customer wants to use IP SLA to create a failover to ISP2 when both Ethernet connections to ISP1 are down. The customer also requires that both connections to ISP1 are utilized during normal operations.



Which IP route configuration accomplishes these requirements for the customer?

A. ip route 0.0.0.0 0.0.0.0 192.168.0.1 track 1
ip route 0.0.0.0 0.0.0.0 192.168.1.1 track 2
ip route 0.0.0.0 0.0.0.0 192.168.2.1 track 3
B. ip route 0.0.0.0 0.0.0.0 192.168.0.1 track 1
ip route 0.0.0.0 0.0.0.0 192.168.1.1 track 2
ip route 0.0.0.0 0.0.0.0 192.168.2.1 track 4 100
C. ip route 0.0.0.0 0.0.0.0 192.168.0.1 track 1
ip route 0.0.0.0 0.0.0.0 192.168.1.1 track 2
ip route 0.0.0.0 0.0.0.0 192.168.2.1 track 3 100
D. ip route 0.0.0.0 0.0.0.0 192.168.0.1 track 1 1
ip route 0.0.0.0 0.0.0.0 192.168.1.1 track 2 2
ip route 0.0.0.0 0.0.0.0 192.168.2.1 track 3 3

Answer: C

QUESTION 263
An IP SLA fails to generate statistics. How can you fix the problem?

A. Add the verify-data command to the router configuration.
B. Reload the router configuration.

C. Remove the ip sla schedule statement from the router configuration and re-enter it.
D. Add the debug ip sla error command to the router configuration.
E. Add the debug ip sla trace command to the router configuration.

Answer: A

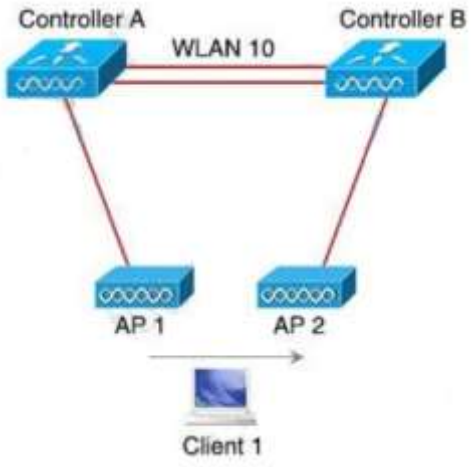
QUESTION 264
Refer to the exhibit. What does the snippet of code achieve?

```
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.

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).

QUESTION 265
Refer to the exhibit. Both controllers are in the same mobility group. Which result occurs when client 1 roams between APs that are registered to different controllers in the same WLAN?



A. Client 1 contact controller B by using an EoIP tunnel.
B. CAPWAP tunnel is created between controller A and controller B.

C. Client 1 users an EoIP tunnel to contact controller A.
D. The client database entry moves from controller A to controller B.

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.

QUESTION 266
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. Incandesent lights

Answer: AC
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 -> Incandesent 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.

QUESTION 267
Refer to the exhibit. What are two effects of this configuration? (Choose two.)

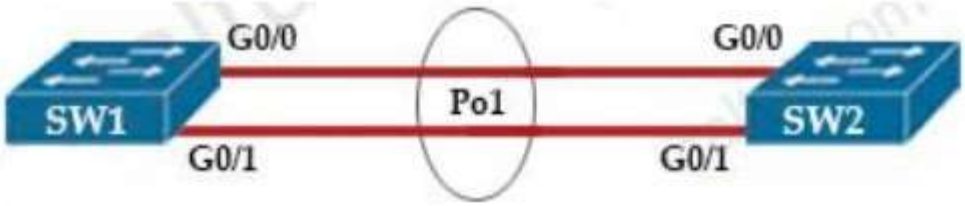
```
R1
interface GigabitEthernet0/0
ip address 192.168.250.2 255.255.255.0
standby 20 ip 192.168.250.1
standby 20 priority 120

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.

Answer: AD

QUESTION 268
Refer to the exhibit. After an engineer configures an EtherChannel between switch SW1 and switch SW2, this error message is logged on switch SW2.




```
SW1# show etherchannel summary

! output omitted

Group    Port-channel    Protocol    Ports
--------+---------------+-----------+-----
1        Po1 (SD)            -
```

```
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.

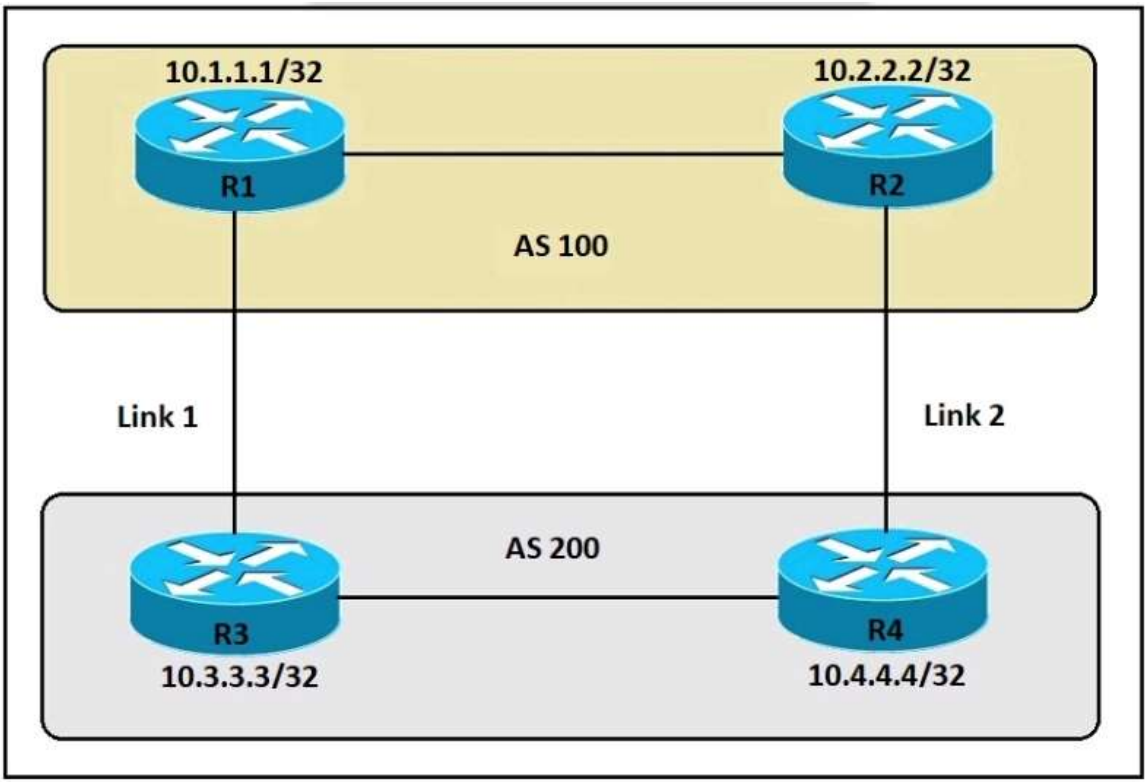
Answer: A
Explanation:
In this case, we are using your EtherChannel without a negotiation protocol. As a result, if the opposite switch is not also configured for EtherChannel operation on the respective ports, there is a danger of a switching loop. The EtherChannel Misconfiguration Guard tries to prevent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

QUESTION 269
Which deployment option of Cisco NQFW provides scalability?

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

Answer: C

QUESTION 270
Refer to the exhibit. An engineer must ensure that all traffic entering AS 200 from AS 100 chooses Link 2 as an entry point. Assume that all BGP neighbor relationships have been formed and that the attributes have not been changed on any of the routers.
Which configuration accomplishes this task?



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

Answer: A

QUESTION 271
What are two differences between the RIB and the FIB? (Choose two.)

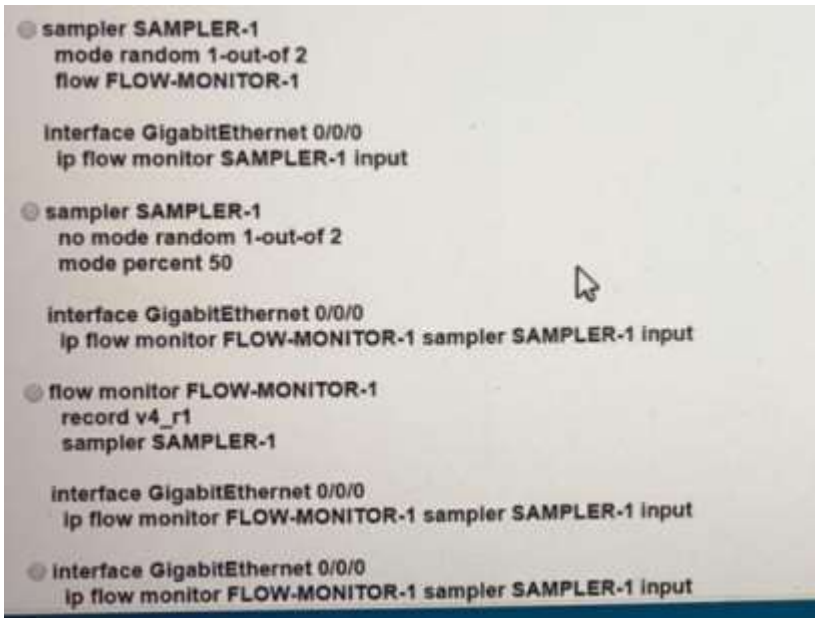
A. The FIB is derived from the data plane, and the RIB is derived from the FIB.
B. The RIB is a database of routing prefixes, and the FIB is the Information used to choose the egress interface for each packet.
C. FIB is a database of routing prefixes, and the RIB is the information used to choose the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

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

Answer: BE
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.

QUESTION 272
Refer to the exhibit. Which command set must be added to the configuration to analyze 50 packets out of every 100?

```
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 v_r1
 exit
!
sampler SAMPLER-1
 mode random 1 out-of 2
 exit
!
ip cef
!
interface GigabitEthernet0/0/0
 ip address 172.16.6.2 255.255.255.0
```



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

Answer: C

QUESTION 273
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

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.

QUESTION 274
What is the purpose of the LISP routing and addressing architecture?

A. It creates two entries for each network node, one for Its identity and another for its location on the network.
B. It allows LISP to be applied as a network visualization overlay though encapsulation.

C. It allows multiple Instances of a routing table to co-exist within the same router.
D. It creates head-end replication used to deliver broadcast and multicast frames to the entire network.

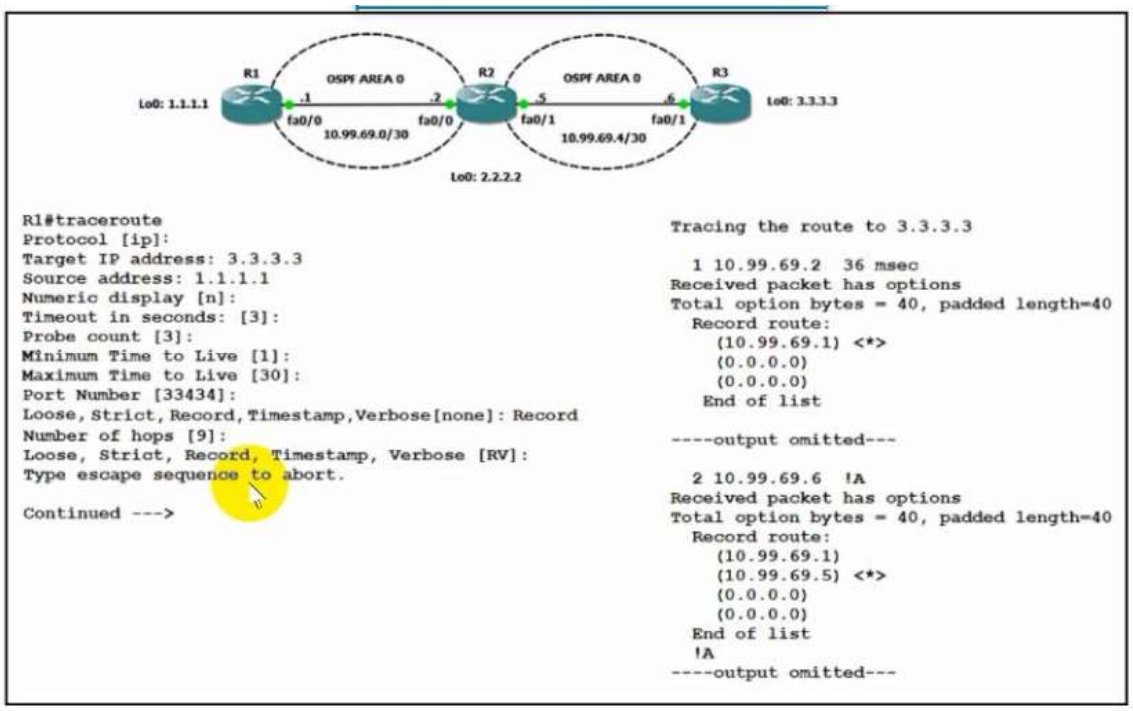
Answer: A
Explanation:
Locator ID Separation Protocol (LISP) solves this issue by separating the location and identity of a device through the Routing locator (RLOC) and Endpoint identifier (EID):
+ Endpoint identifiers (EIDs) ?assigned to end hosts.
+ Routing locators (RLOCs) ?assigned to devices (primarily routers) that make up the global routing system.

QUESTION 275
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.

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 = 108/interface bandwidth in bps)

QUESTION 276
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.

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.

QUESTION 277
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. JVVT
D. TLS

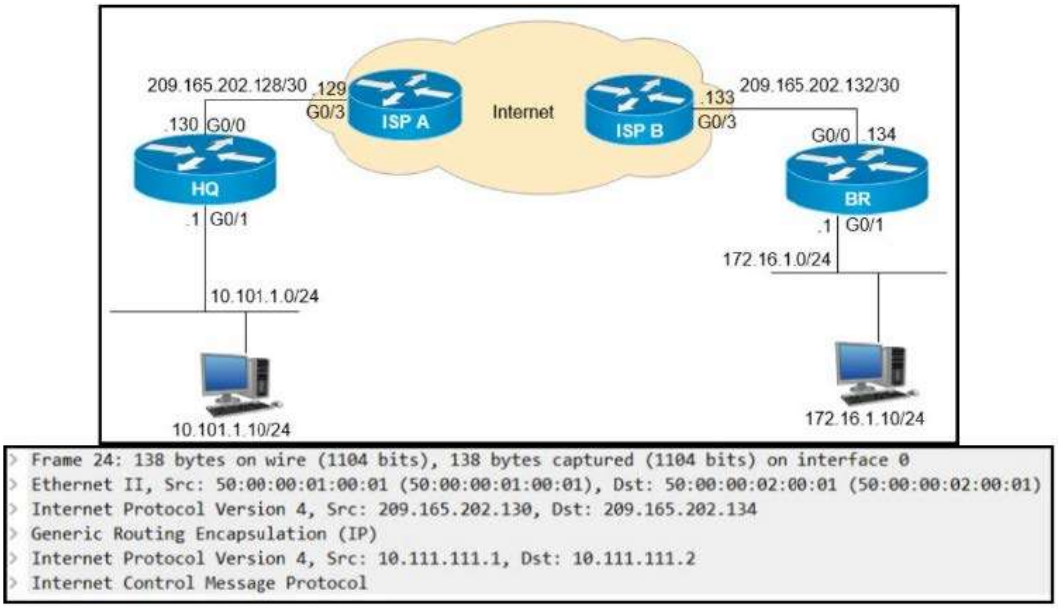
Answer: B
Explanation:
https://developer.atlassian.com/server/crowd/json-requests-and-responses/

QUESTION 278
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.

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.
Reference: https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/multivendor-support-southbound

QUESTION 279
Refer to the exhibit. A GRE tunnel has been created between HO and BR routers.
What is the tunnel IP on the HQ router?



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

Answer: A

QUESTION 280
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.

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: https://www.ciscolive.com/c/dam/r/ciscolive/latam/docs/2018/pdf/BRKEWN-2020.pdf

QUESTION 281
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.

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. Reference: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/69639-wlc-failover.html

QUESTION 282
Which control plane protocol is used between Cisco SD-WAN routers and vSmart controllers?

A. TCP
B. OMP
C. UDP
D. BGP

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.

QUESTION 283
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

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: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SY/configuration/guide/sy_swcg/stateful_switchover.html

QUESTION 284
Which deployment option of Cisco NGFW provides scalability?

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

Answer: D
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/asa- cluster-solution.html
Clustering lets you group multiple Firepower Threat Defense (FTD) units together as a single logical device. Clustering is only supported for the FTD device on the Firepower 9300 and the Firepower 4100 series. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices.

QUESTION 285
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

Answer: D
Explanation:
The LISP control plane messaging protocol is an architecture to communicate and exchange the relationship between these two

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

QUESTION 286
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
!

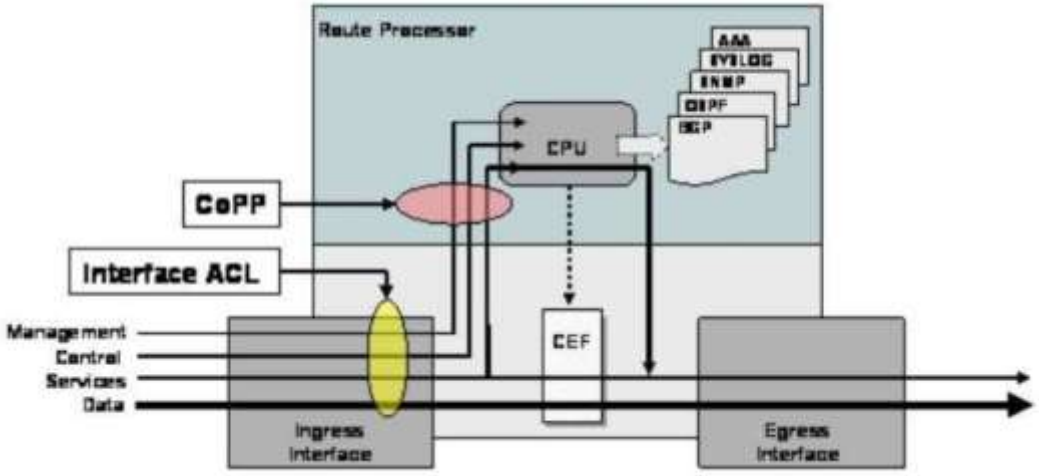
B. class-map match-all CoPP_SSH
match access-group name CoPP_SSH
!
Policy-map CoPP_SSH
class CoPP_SSH
police cir CoPP_SSH
exceed-action drop
!
Interface GigabitEthernet0/1
ip address 209.165.200.225 255.255.255.0
ip access-group ?out
duplex auto
speed auto
media-type rj45
service-policy input CoPP_SSH
!
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
!
```

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.

QUESTION 287
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

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.

QUESTION 288
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.

Answer: C

QUESTION 289
What is the function of the fabric control plane node In a Cisco SD-Access deployment?

A. It is responsible for policy application and network segmentation in the fabric.
B. It performs traffic encapsulation and security profiles enforcement in the fabric.
C. It holds a comprehensive database that tracks endpoints and networks in the fabric.
D. It provides Integration with legacy nonfabric-enabled environments.

Answer: C
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-segmentation-deploy-guide.html

QUESTION 290
Refer to the exhibit. 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?

```
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
```

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

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

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

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

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

Answer: B

QUESTION 291
Which entity is responsible for maintaining Layer 2 isolation between segments In a VXLAN environment?

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

Answer: C
Explanation:
VXLAN uses an 8-byte VXLAN header that consists of a 24-bit VNID and a few reserved bits. The

VXLAN header together with the original Ethernet frame goes in the UDP payload. The 24-bit VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments.
Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/vxlan/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_7x_chapter_010.html

QUESTION 292
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

Answer: D

QUESTION 293
Refer to the exhibit. 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?

```
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
```

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

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: https://www.theroutingtable.com/ip-sla-and-cisco-eem/

QUESTION 294
Refer to the exhibit. What ate 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 Rl 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.

Answer: AE

QUESTION 295
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

Answer: B
Explanation:
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:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swspan.html
Therefore in this question, we cannot configure a source VLAN because we configured source ports for RSPAN session 1 already.

QUESTION 296
Which element enables communication between guest VMs within a virtualized environment?

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

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.

QUESTION 297
Which action is performed by Link Management Protocol In a Cisco StackWise Virtual domain?

A. it determines if the hardware Is compatible to form the StackWise Virtual domain.
B. It determines which switch becomes active or standby.
C. It discovers the StackWise domain and brings up SVL interfaces.
D. It rejects any unidirectional link traffic forwarding.

Answer: D
Explanation:
The Link Management Protocol (LMP) performs the following functions: + Verifies link integrity by establishing bidirectional traffic forwarding, and rejects any unidirectional links + Exchanges periodic hellos to monitor and maintain the health of the links + Negotiates the version of StackWise Virtual header between the switches StackWise Virtual link role resolution
Reference: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-stack-wp-cte-en.html

QUESTION 298
A network engineer is configuring Flexible Netflow and enters these commands:

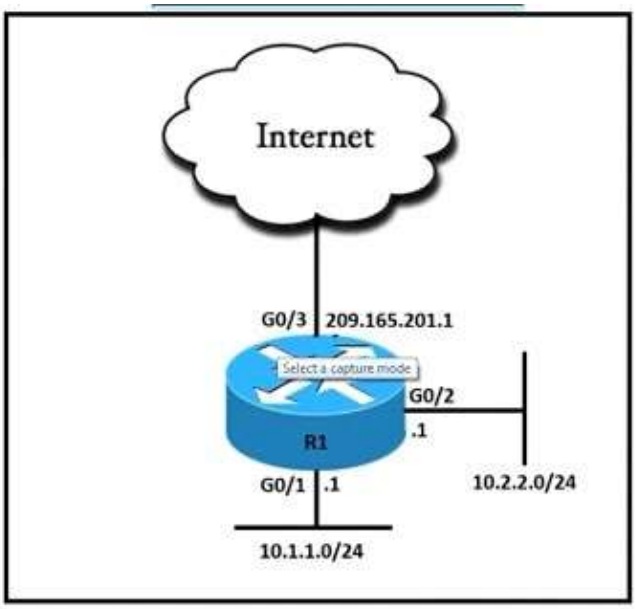
```
Sampler Netflow1
Mode random one-out-of 100
Interface fastethernet 1/0
Flow-sampler netflow1
```

Which are two results of implementing this feature instead of traditional Netflow? (Choose two.)

A. CPU and memory utilization are reduced.
B. Only the flows of top 100 talkers are exported
C. The data export flow is more secure.
D. The number of packets to be analyzed are reduced
E. The accuracy of the data to be analyzed is improved

Answer: AD

QUESTION 299
Refer to the exhibit. An engineer must allow all users In the 10.2.2.0/24 subnet to access the Internet. To conserve address space, the public interface address of 209.165.201.1 must be used for all external communication. Which command set accomplishes these requirements?



A.
```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 interface G0/2 overload
```

B.
```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 209.165.201.1
```

C.
```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 interface G0/3
```

D.
```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 interface G0/3 overload
```

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.

QUESTION 300
Which router is elected the IGMP Querier when more than one router is in the same LAN segment?

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

Answer: B
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 all-systems 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:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/2_2_e/multicast/configuration_guide/b_mc_1522e_3750x_3560x_cg/b_ipmc_3750x_3560x_chapter_01000.html

QUESTION 301
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	R2
key chain cisco123 key 1 key-string Cisco123!	key chain cisco123 key 1 key-string cisco123!
Ethernet0/0 - Group 10 State is Active 8 state changes, last state change 00:03:33 Virutal 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 Virutal IP address is 192.168.0.1 Active virtual MAC address is 0000.0c07.ac0a Local virtual MAC address is 0000.0c07.ac0a (v1 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

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.
key-string [encryption-type] text-string: Configures the text string for the key. The text-string argument is alphanumeric, case-sensitive, and supports special characters.
Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/security/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_chapter_01111.pdf

QUESTION 302
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

Answer: C
Explanation:
Access Points
+ AP is directly connected to FE (or to an extended node switch) + AP is part of Fabric overlay
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKEWN-2020.pdf

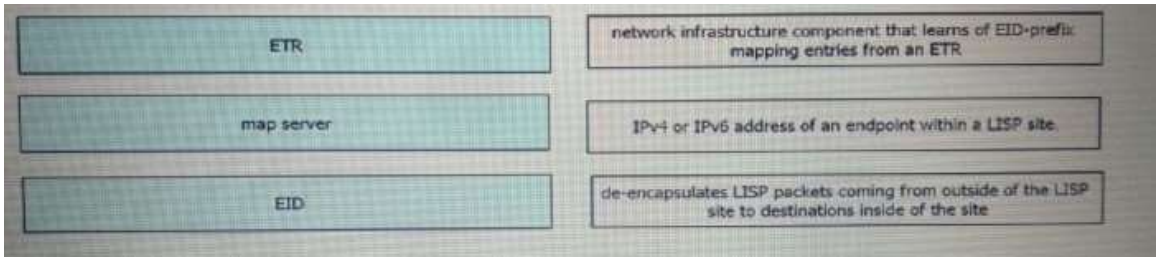
QUESTION 303
What are two considerations when using SSO as a network redundancy feature? (Choose two)

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

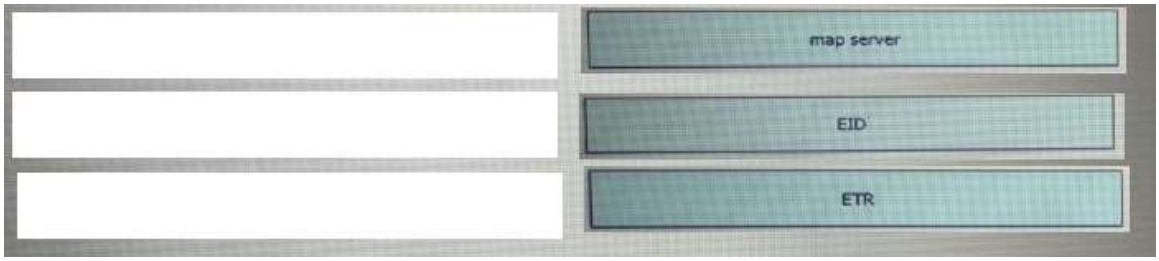
Answer: DE
Explanation:
against failure due to the Supervisor or loss of service because of software problems. The access layer typically provides Layer 2 services with redundant switches making up the distribution layer. The Layer 2 access layer can benefit from SSO deployed without NSF. Some Enterprises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

QUESTION 304
Drag and Drop Question

Drag and drop the LIPS components on the left to the correct description on the right.

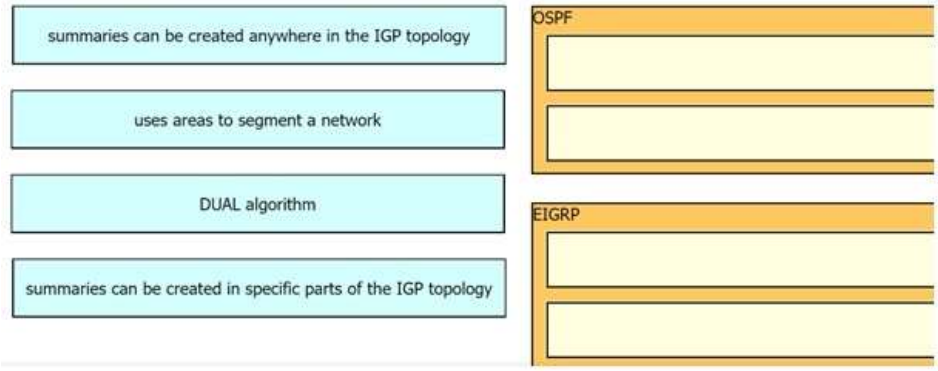


Answer:

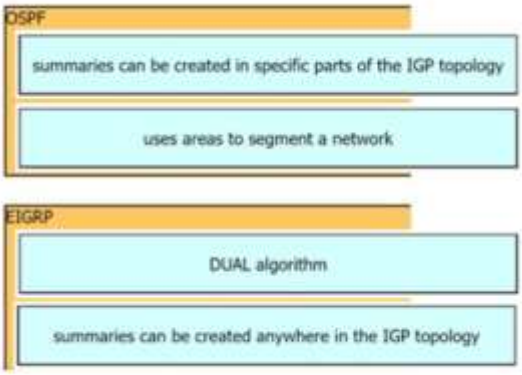


QUESTION 305
Drag and Drop Question

Drag and Drop the decryptions from the left onto the routing protocol they describe on the right.

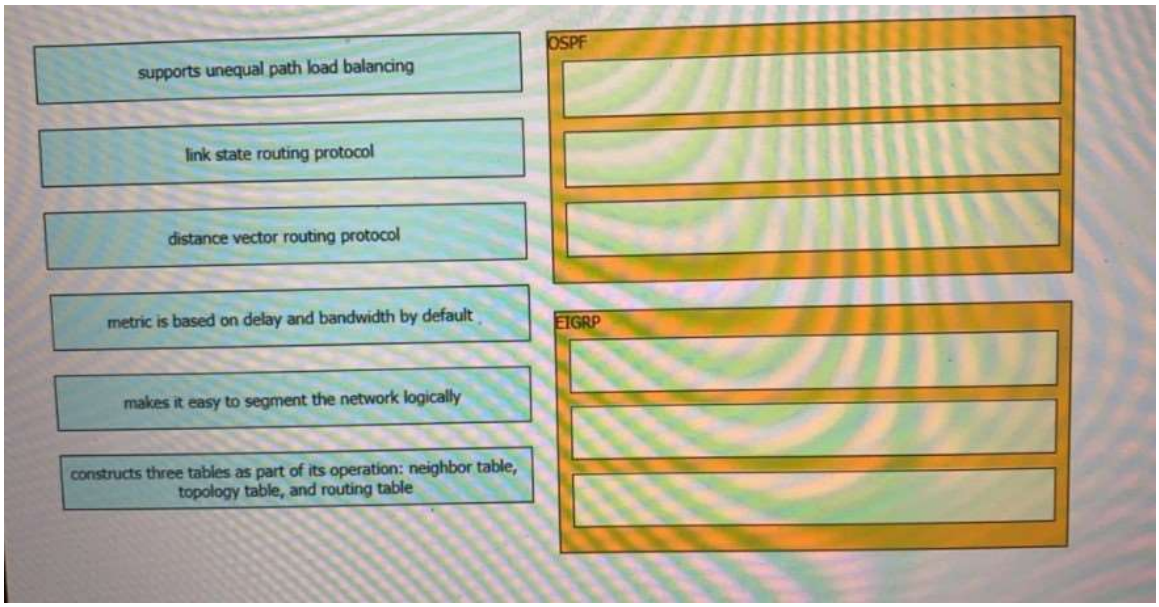


Answer:

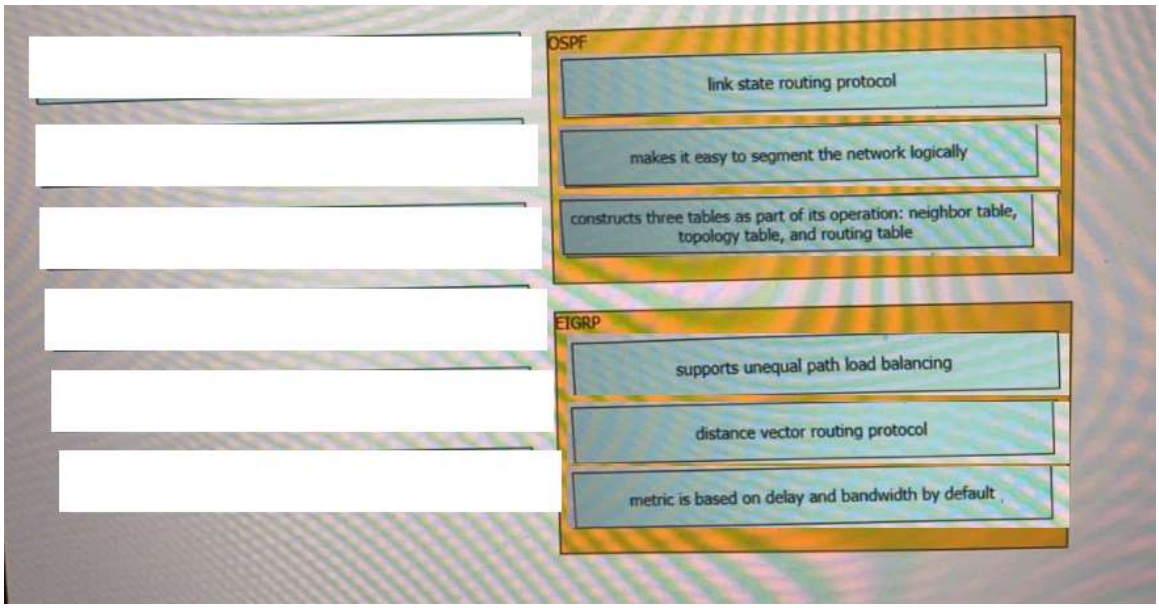


QUESTION 306
Drag and Drop Question

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

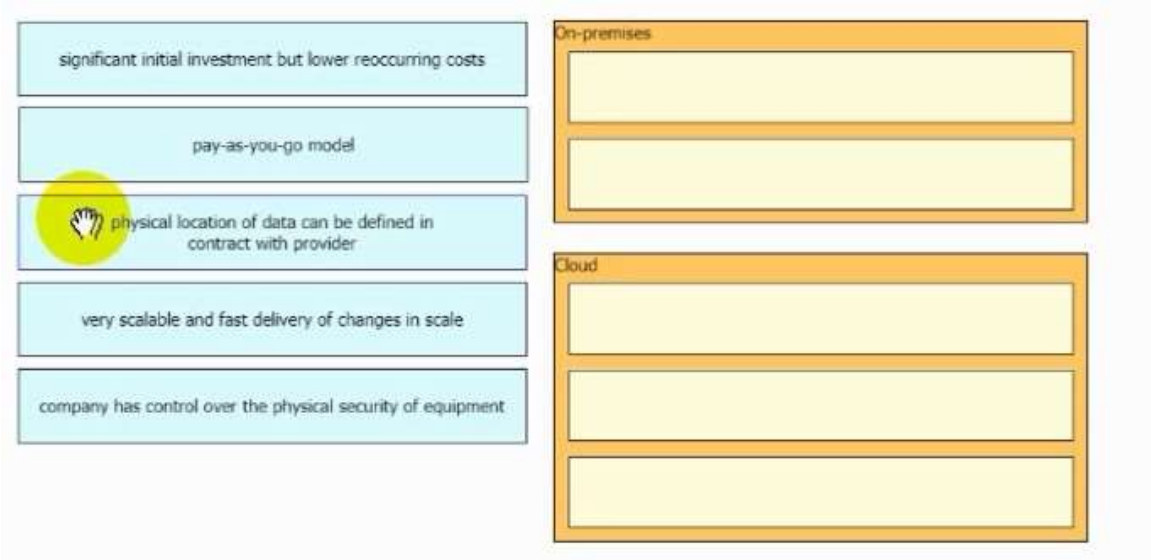


Answer:

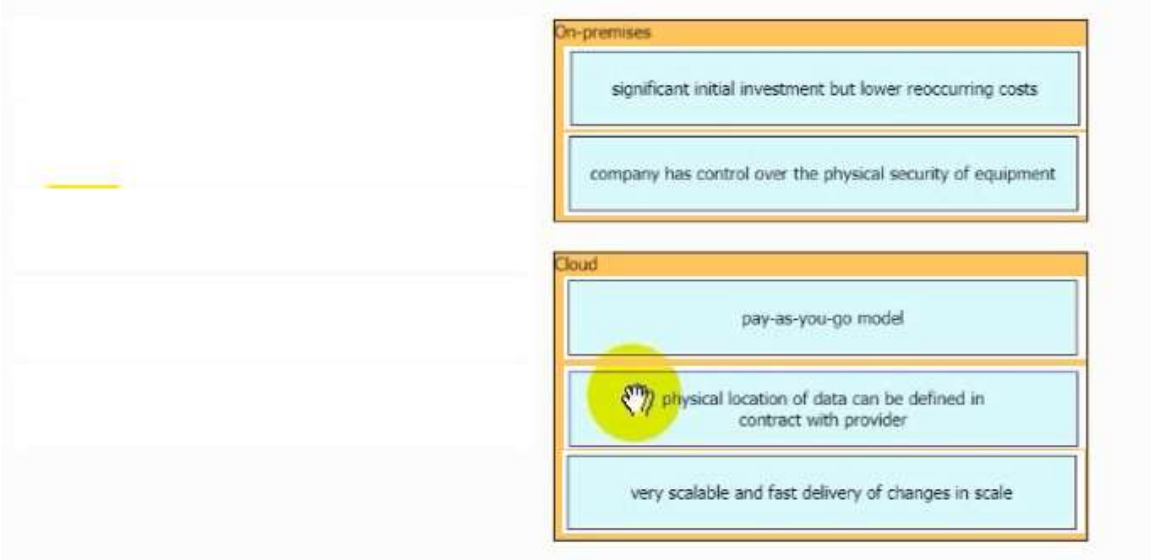


QUESTION 307
Drag and Drop Question

Drag and drop the characteristics from the left to the correct Infrastructure deployment type on the right.



Answer:



QUESTION 308
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

Answer: A

QUESTION 309
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.

Answer: B
Explanation:
If the system clock has not been set, the date and time are preceded by an asterisk (*) to indicate that the date and time are probably not correct.
Reference:https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/mod_frameset.htm

QUESTION 310
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

Answer: C
Explanation:
The "exec-timeout" command is used to configu e 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 "exe -timeout 10 0" command to set the user inactivity timer to 600 seconds (10 minutes).

QUESTION 311
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.

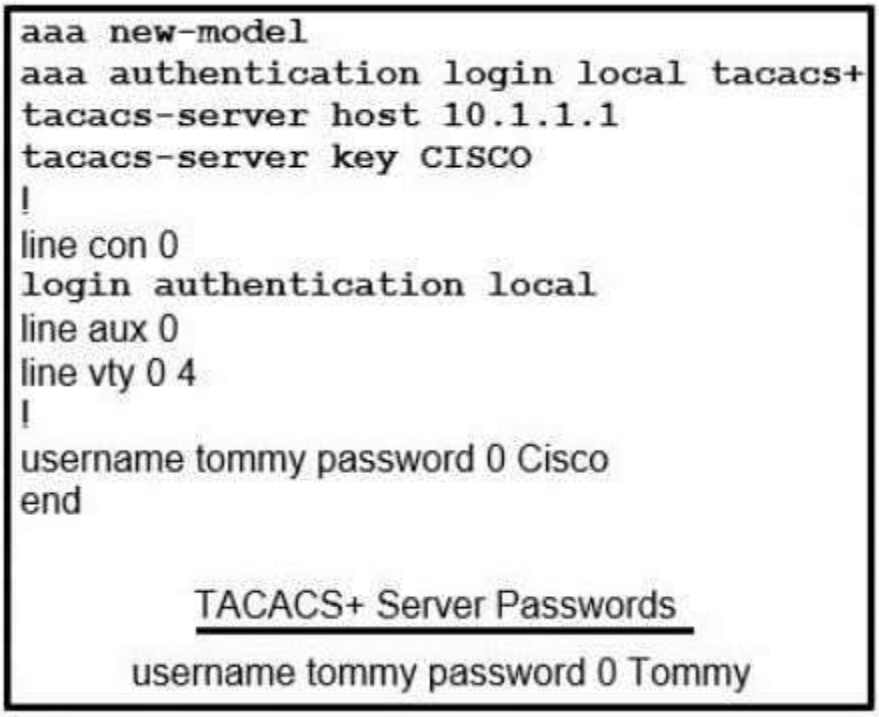
Answer: B
Explanation:
Note: The administrator can set the root bridge priority to 0 in an effort to secure the root bridge position. But there is no guarantee against a bridge with a priority of 0 and a lower MAC address. The root guard feature provides a way to enforce the root bridge placement in the network.

QUESTION 312
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

Answer: D
Explanation:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/87/b_wireless_high_client_density_design_guide.html

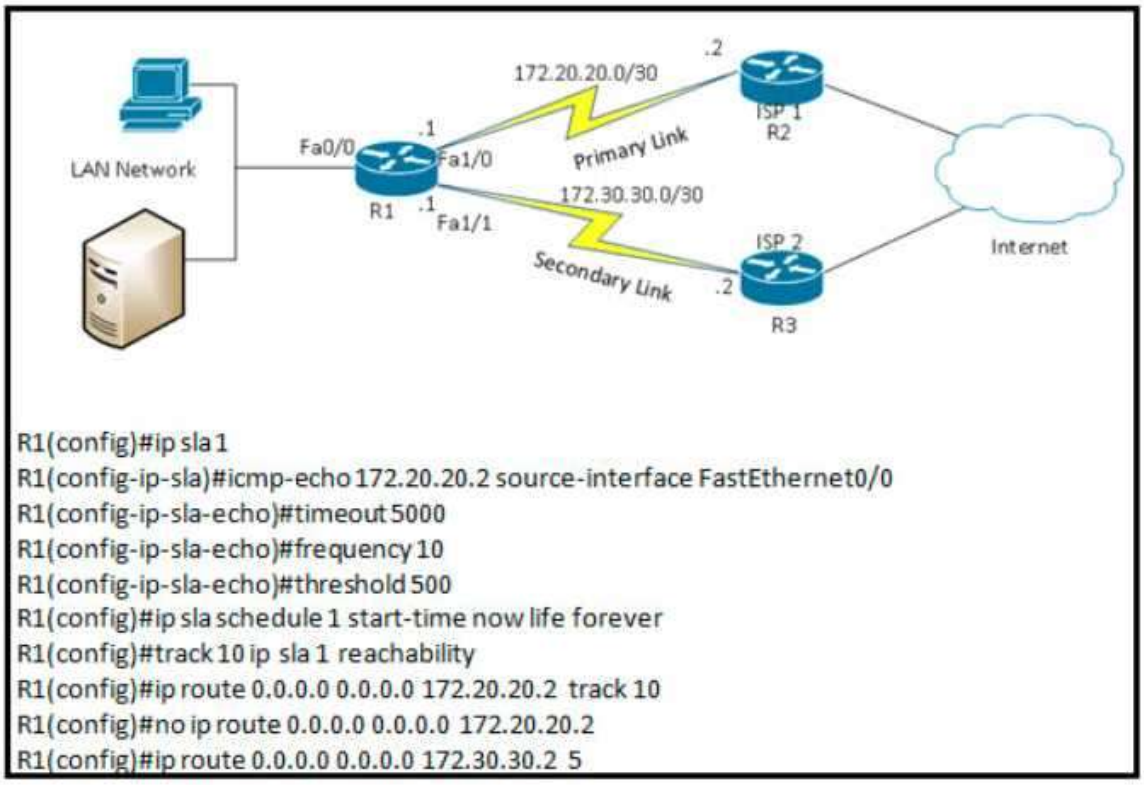
QUESTION 313
Refer to the exhibit. Which password allows access to line con 0 for a username of "tommy" under normal operation?



A. Cisco
B. local
C. 0 Cisco
D. Tommy

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.
https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/200606-aaa-authentication-login-default-local.html

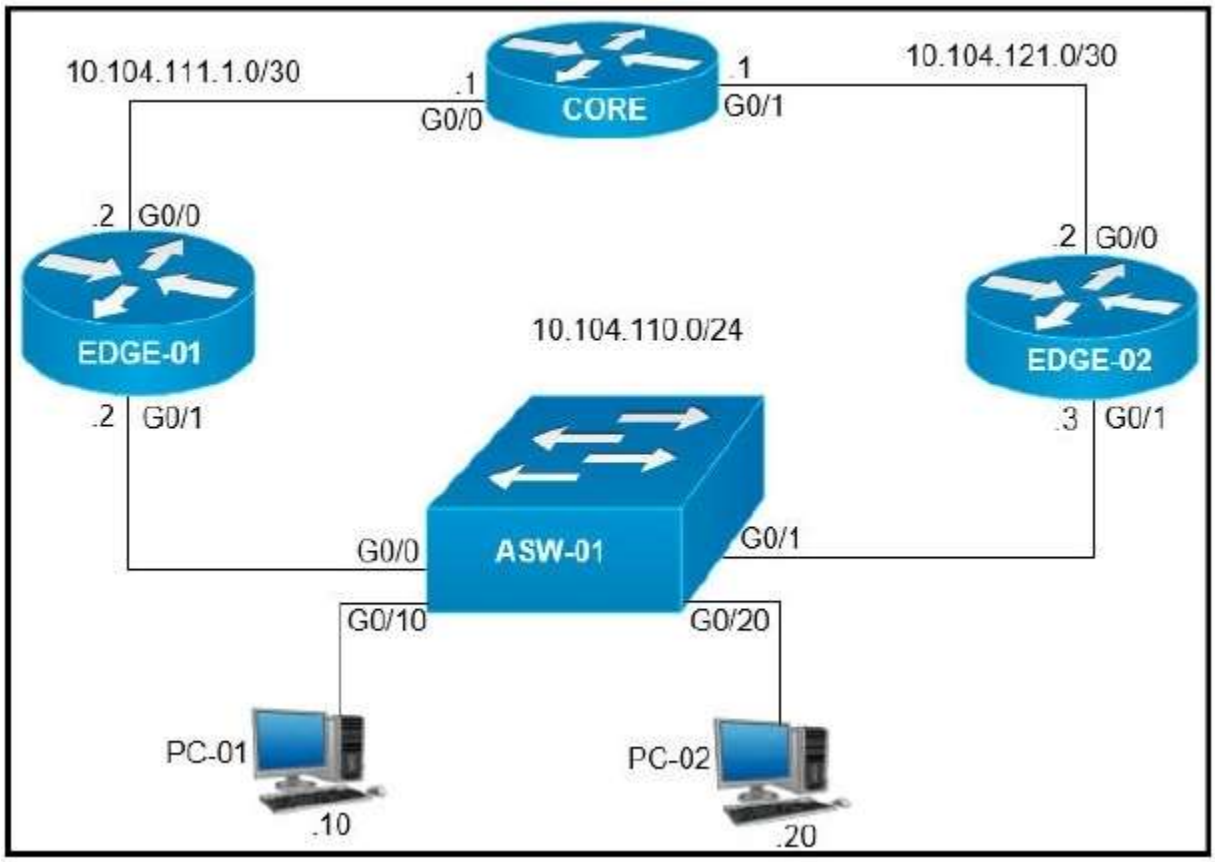
QUESTION 314
Refer to exhibit. What are two reasons for IP SLA tracking failure? (Choose two)



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

Answer: CD

QUESTION 315
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 GO/1 on Core
B. G0/0 on Edge-01 and G0/0 on Edge-02
C. GO/1on Edge-01 and GO/1 on Edge-02
D. G0/0 and GO/1 on ASW-01

Answer: C

QUESTION 316
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

Answer: CDE

QUESTION 317

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

A. LISP
B. VRF Lite
C. VRF
D. VXLAN

Answer: D
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.

Chapter	Section
SD-Access Operational Planes	Control Plane – LISP
	Data Plane – VXLAN
	Policy Plane – Cisco TrustSec
	Management Plane – Cisco DNA Center

QUESTION 318
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 Customerl 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 VlanlO
ip route 172.16.1.0 255.255.255.0 Vlan20
B. ip route vrf Customerl 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 Customerl
C. ip route vrf Customerl 172.16.1.0 255.255.255.0 172.16.1.1 Customerl
ip route vrf Customer 192.168.1.200 255.255.255.255 192.168.1.1 Customer2
D. ip route vrf Customerl 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 VlanlO
ip route 172.16.1.0 255.255.255.0 Vlan20

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 uses 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".
https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200158-Configure-Route-Leaking-between-Global-a.html

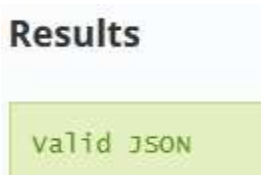
QUESTION 319
Refer to the exhibit. What is the JSON syntax that is formed from the data?



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"]}

Answer: A
Explanation:

```
{
    "Make": "Gocar",
    "Model": "Zoom",
    "Features": ["Power Windows", "Manual Dnve", "Auto AC"]
}
```



QUESTION 320
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

Answer: C
Explanation:
- FIFO (first-in, first-out). 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.

QUESTION 321
Which devices does Cisco DNA Center configure when deploying an IP-based access control policy?

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

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

QUESTION 322
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

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).

QUESTION 323
What are two common sources of interference for WI-FI networks? (Choose two.)

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

Answer: AC

QUESTION 324
In a wireless Cisco SD-Access deployment, which roaming method is used when a user moves from one access point to another on a different access switch using a single WLC?

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

Answer: D
Explanation:
https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKEWN-2020.pdf

QUESTION 325
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.
Questions & Answers PDF P-180

Answer: A
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/cfg-de-fnflow-exprts.html

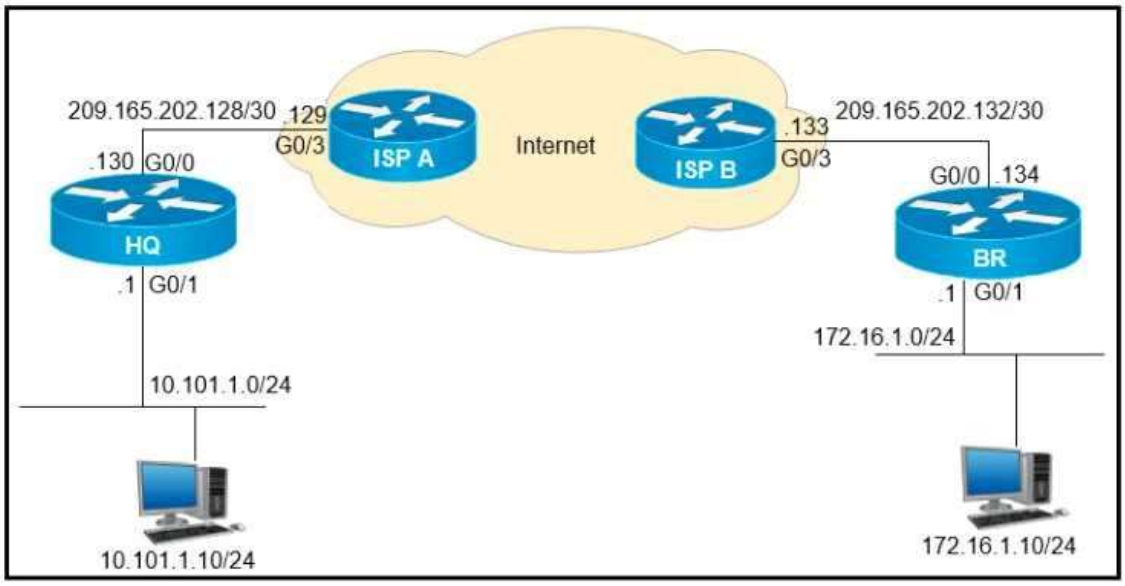
QUESTION 326
Refer to the exhibit. Cisco DNA Center has obtained the username of the client and the multiple devices that the client is using on the network. How is Cisco DNA Center getting these context details?



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

Answer: A
Explanation:
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3-30/user_guide/b_cisco_dna_center_ug_1_3_3_0/b_cisco_dna_center_ug_1_3_2_0_chapter_01100.h

QUESTION 327
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?
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?




```
interface Tunnel1
 ip address 209.165.202.130 255.255.255.252
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.129
```

```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.133
```

```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.129
```

```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.134
```

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

Answer: D
Explanation:
https://community.cisco.com/t5/networking-documents/how-to-configure-a-gre-tunnel/ta-p/3131970#toc-hId--1446104265

QUESTION 328

What is a fact about Cisco EAP-FAST?

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

Answer: A
Explanation:
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.

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-fixed/72788-CSSC-Deployment-Guide.html

QUESTION 329
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

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.

QUESTION 330
Which DHCP option provides the CAPWAP APs with the address of the wireless controller(s)?

A. 43
B. 66
C. 69
D. 150

Answer: A
Explanation:

DHCP Option 43

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.

QUESTION 331
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

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
```

QUESTION 332
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

Answer: A
Explanation:
https://community.cisco.com/t5/networking-documents/cam-content-addressable-memory-vs-tcam-ternary-content/ta-p/3107938

QUESTION 333
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, bu 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

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.

QUESTION 334
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

Answer: C
Explanation:
Unlike HSRP or GLBP, VRPP is an open standard. Only VRRPv3 supports both IPv4 and IPv6.

QUESTION 335

Which unit measures the power of a radio signal with reference to 1 milliwatt?

A. dBw
B. dBm
C. mW
D. dBi

Answer: C

QUESTION 336
What is a characteristic of MACsec?

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

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.
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-9/configuration_guide/sec/b_169_sec_9300_cg/macsec_encryption.html

QUESTION 337
Which two components are supported by LISP? (choose two)

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

Answer: AB
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. 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

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

QUESTION 338
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

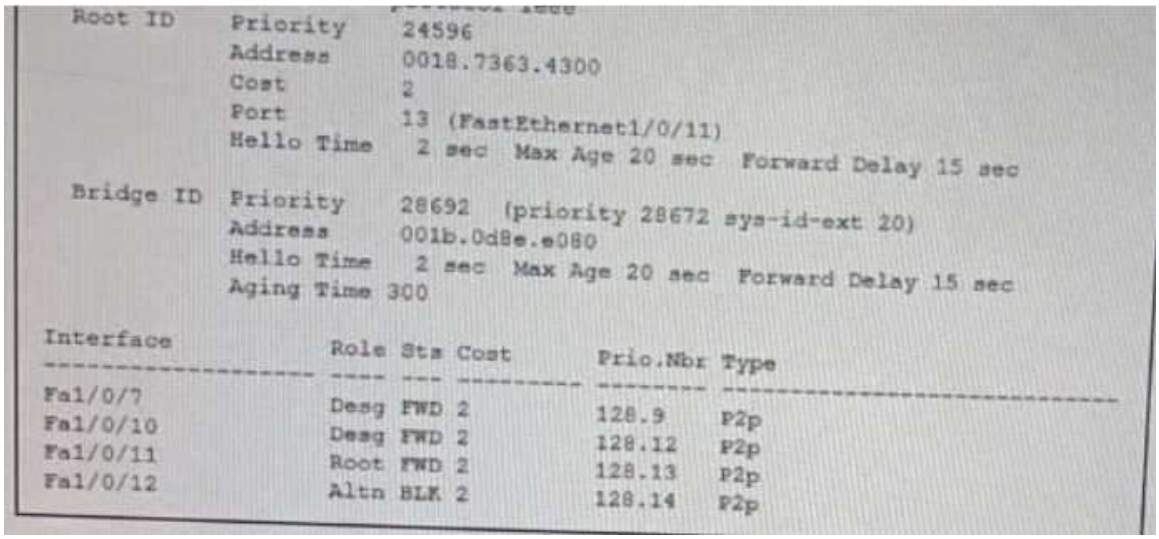
Answer: D
Explanation
A next gene ation firewall adds additional features such as application control, integrated intrusion prevention (IPS) and often more advanced threat prevention capabilities like sandboxing.

QUESTION 339
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

Answer: B

QUESTION 340
Refer to the exhibit. What does the output confirm about the switch's spanning tree configuration?



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

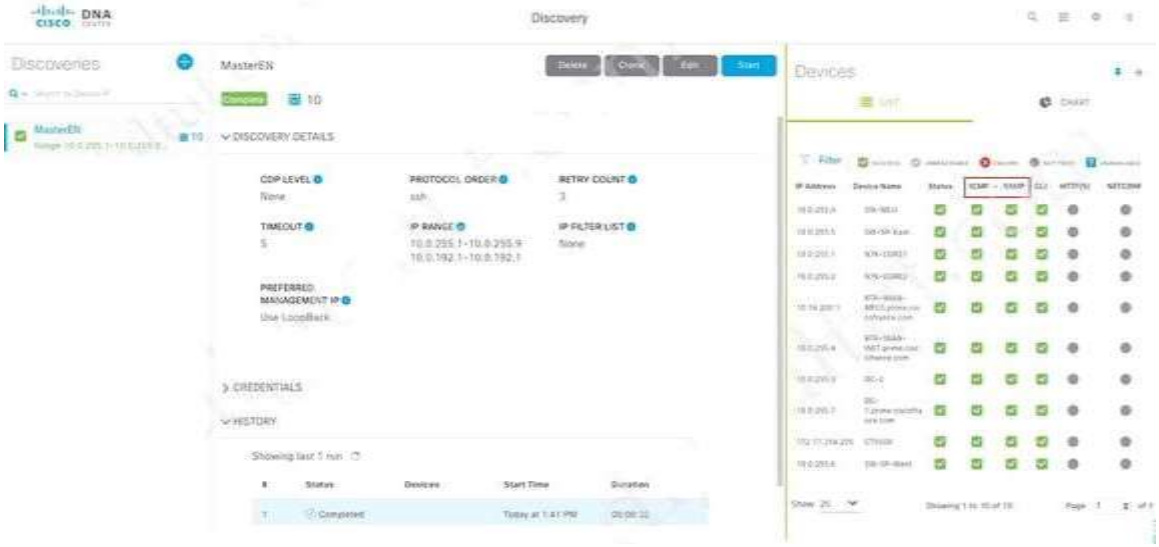
Answer: C

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" unde "VLAN 20" so it can say the switch is running in PVST+ mode.

QUESTION 341
Which two southbound interfaces originate from Cisco DMA 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

Answer: AE
Explanation:
In the figure below, we can see ICMP & SNMP can reach to underlay switches.



QUESTION 342
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

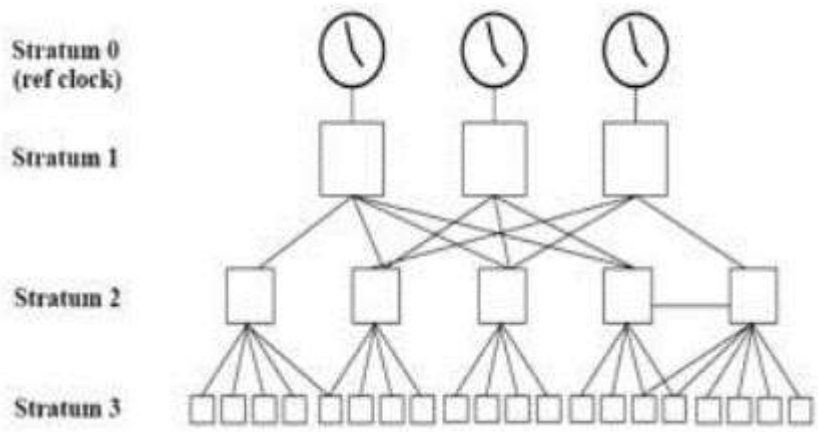
Answer: C
Explanation:
Paravirtualization works differently from the full virtualization. It doesn't need to simulate the hardware for the virtual machines. The hypervisor is installed on a physical server (host) and a guest OS is installed into the environment. Virtual guests aware that it has been 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 paravirtual ation, guests will directly communicate with the host (hypervisor) using drivers.

QUESTION 343
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

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.

QUESTION 344
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 commun cate with networks outside the fabric
C. to connect external Layer 3 networks to the SD Access fabric.
D. to connect APs and wireles endpoints to the SD-Access fabric

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: https://www.cisco.com/c/dam/m/hr_hr/training-events/2019/cisco-connect/pdf/VH-Cisco-SD-Access-Connecting.pdf

QUESTION 345
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 switc operates in PVST+
B. Both switches operate in the PVST+ mode
C. Spanning tree is disabled automatically on the network
D. Both switches operate in the Rapid PVST+ mode.

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

QUESTION 346
Which solution do laaS service providers use to extend a Layer 2 segment across a Layer 3 network?

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

Answer: C

QUESTION 347
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

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.

QUESTION 348
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

Answer: D

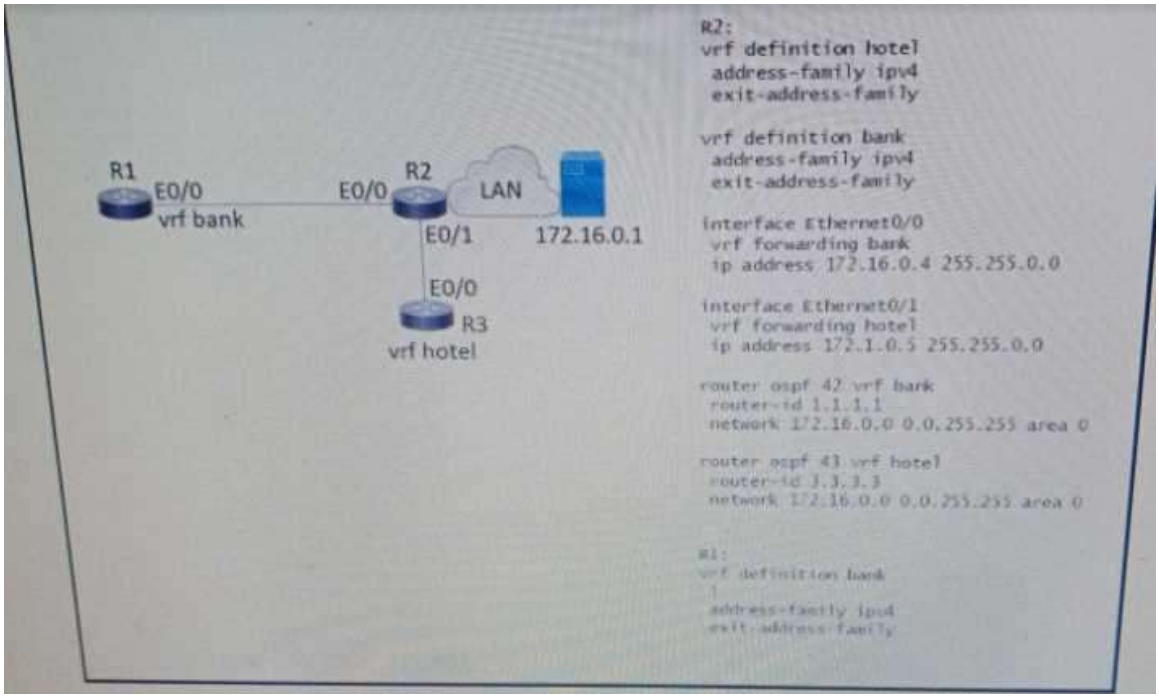
QUESTION 349
A customer has recently implemented a new wireless infrastructure using WLC-5520S at a site directly next to a large commercial airport Users report that they intermittently lose Wi-Fi connectivity, and troubleshooting reveals it is due to frequent channel changes Which two actions fix this issue? (Ch os 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 writ) 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

Answer: AC
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 switch ng the operating frequency of the 5.0 GHz (802.11a/h) radio to one that is not interfering with he radar systems.
Reference:
https://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RadioChannelDFS.pdf

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 conta ns 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:
https://documentation.meraki.com/MR/WiFi Basics and Best Practices/Channel Planning Best P ractices

QUESTION 350
Refer to the exhibit. Which configuration must be applied to R1 to enable R1 to reach the server at 172.16.0.1?



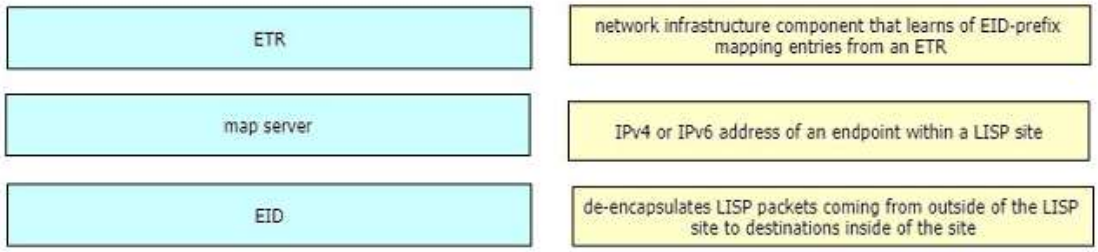


A. Option A
B. Option B
C. Option C
D. Option D

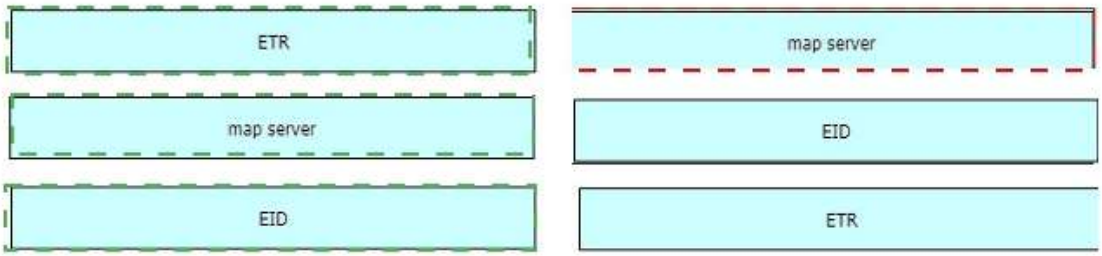
Answer: A

QUESTION 351
Drag and Drop Question

Drag and drop the LISP components on the left to the correct description on the right



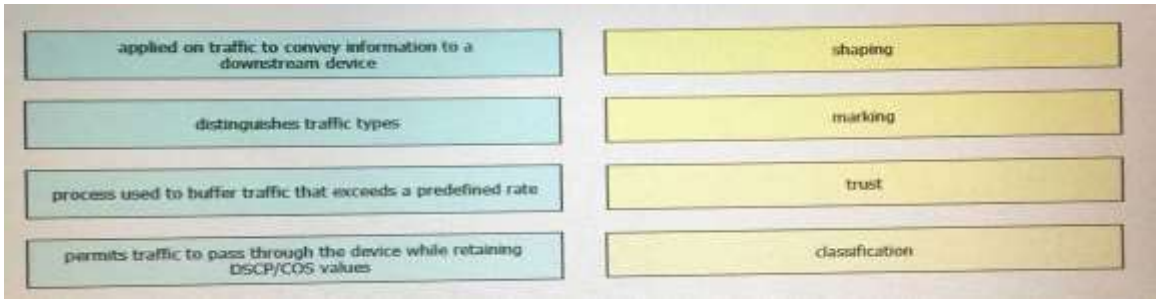
Answer:



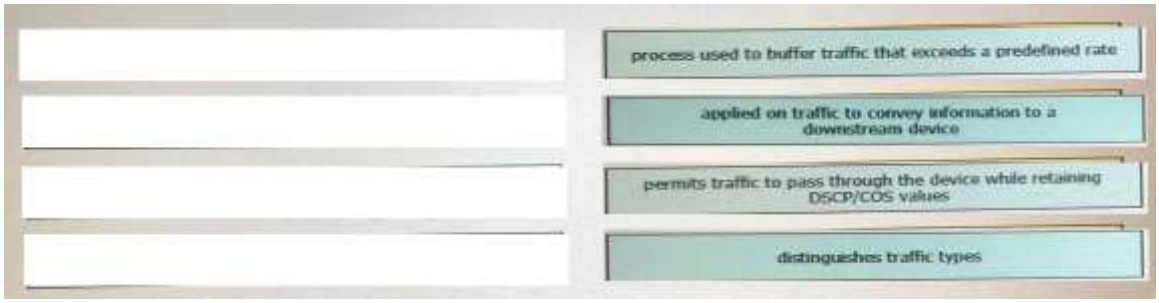
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irloverview.html#GUID-92481C7B-F44D-4D8C-8085-A2E98530CA50

QUESTION 352
Drag and Drop Question

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

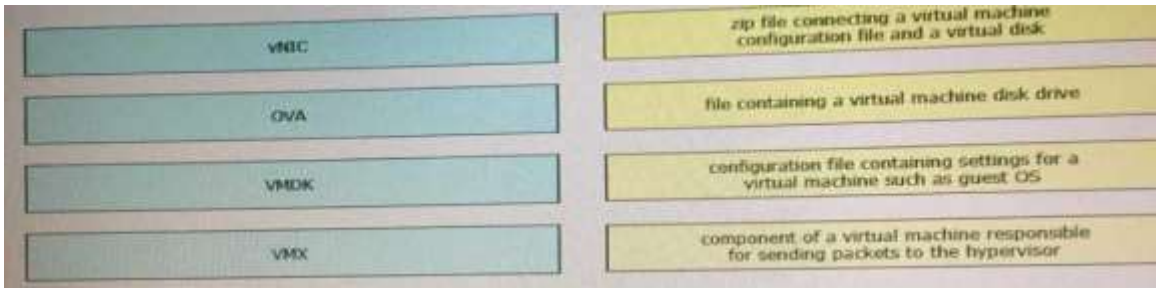


Answer:

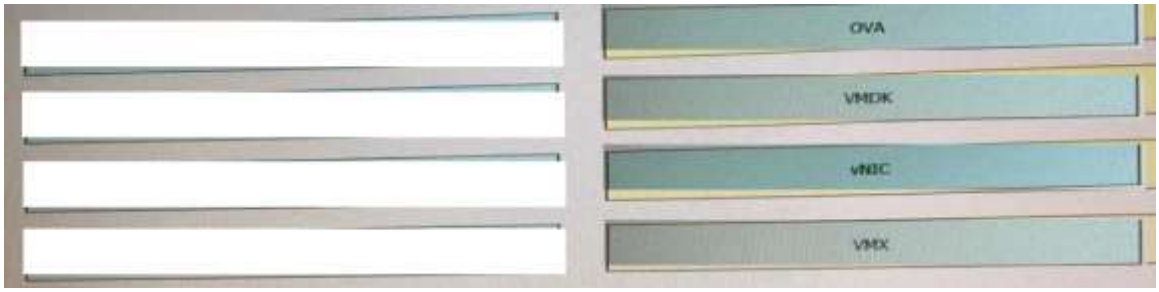


QUESTION 353
Drag and Drop Question

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



Answer:



QUESTION 354
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

Answer: D

QUESTION 355
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. GigabitEthemet0/1 and GigabitEthernet0/1.40
B. only GigabitEthernet0/1
C. only GigabttEthernet0/0
D. Gigabit Ethernet0/0 and GigabitEthemet0/1

Answer: A

QUESTION 356
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",
"softwareeVersion": "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'])
```

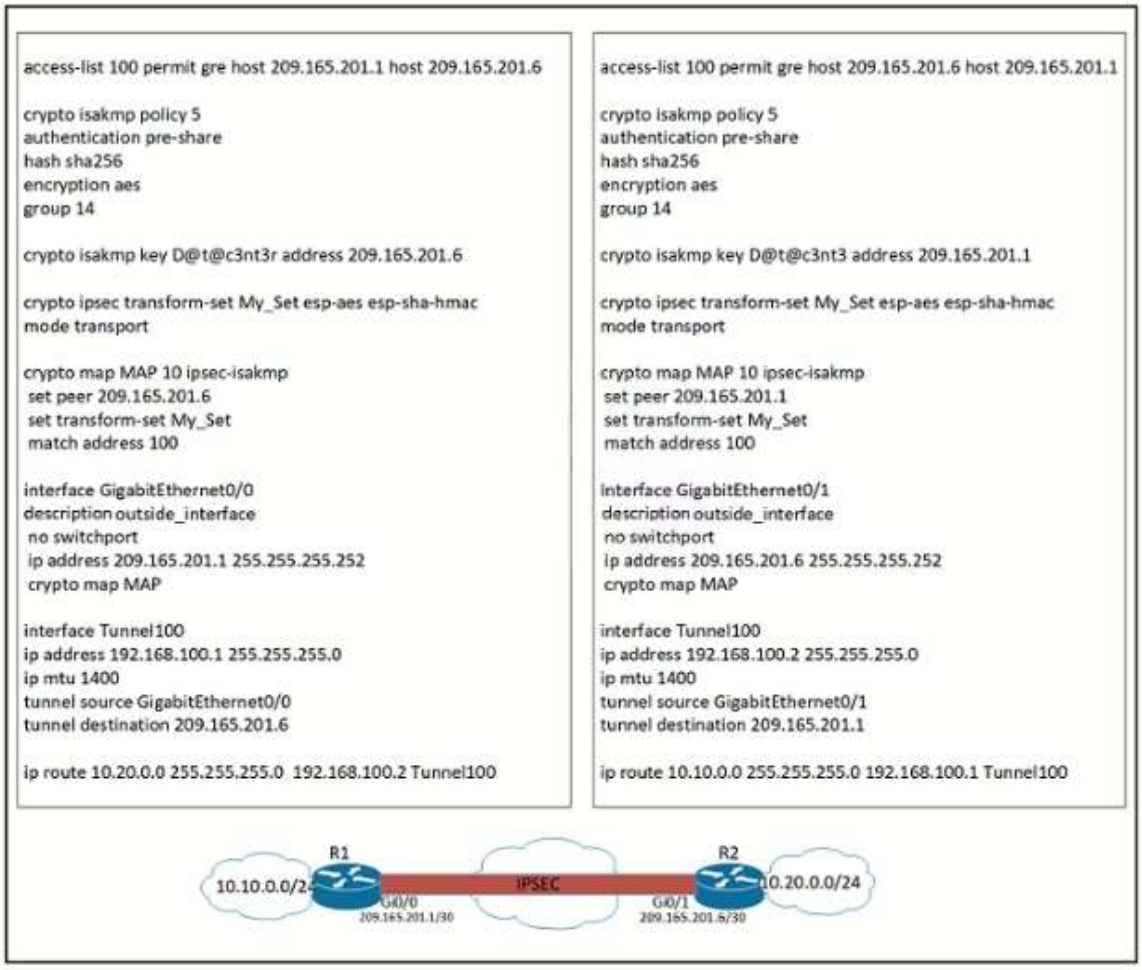
B.
```
json_data = response.json()
print(json_data[response][0][upTime])
```

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

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

Answer: C

QUESTION 357
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 |>]
E. Create an IPsec profile, associate the transform-set ACL. and apply the profile to the tunnel interface

Answer: AE

QUESTION 358
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-V1503-1" (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

Answer: AD

QUESTION 359
Refer to the exhibit. What step resolves the authentication issue?

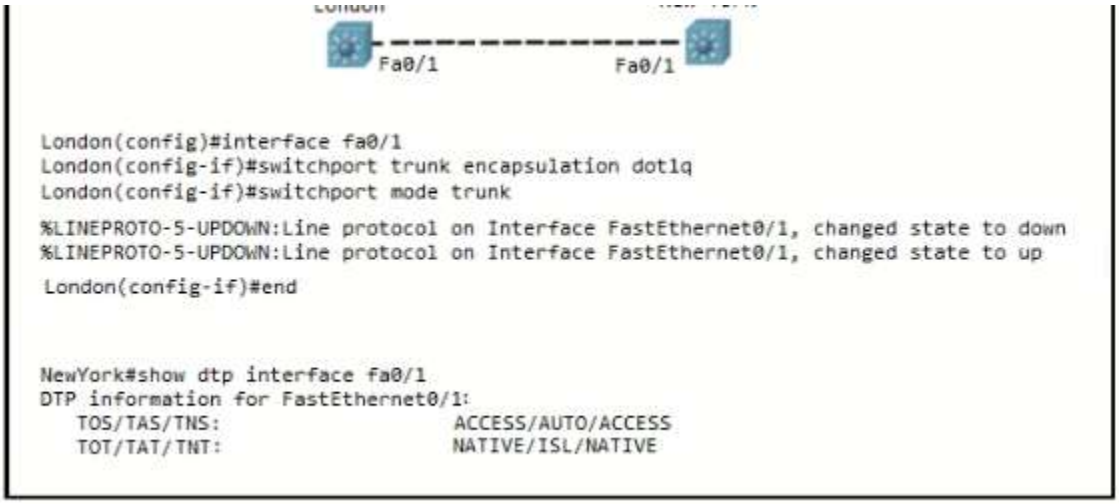
```
TYPE    PROT SYSTEM IP      ID      ID     PRIVATE IP                              PUBLI
PUBLIC IP                           PORT   LOCAL COLOR     PROXY STATE UPTIME      ID
------------------------------------------------------------------------------------
------------------------------------------------------------------------------------
------
vsmart  dtls 4.4.4.70       100     1      192.168.100.80
12446 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
```



A. use basic authentication
B. change the port to 12446
C. target 192 168 100 82 in the URI
D. restart the vsmart host

Answer: D

QUESTION 360
Refer to the exhibit Communication between London and New York is down.
Which command set must be applied to resolve this issue?



A.
```
NewYork(config)#int f0/1
NewYork(config)#switchport 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#
```

Answer: B

QUESTION 361
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

Answer: BE

QUESTION 362
What is a VPN in a Cisco SD-WAN deployment?

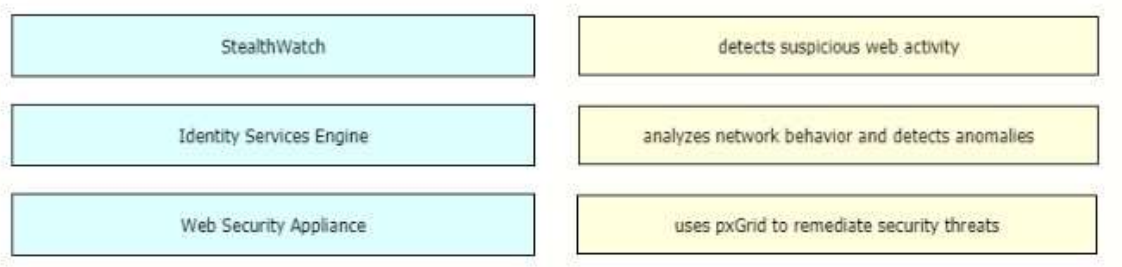
A. common exchange point between two different services

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

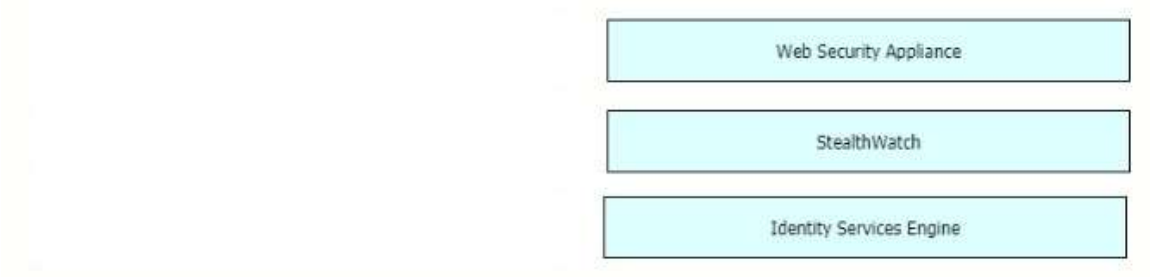
Answer: C

QUESTION 363
Drag and Drop Question

Drag and drop the solutions that comprise Cisco Cyber Threat Defense from the left onto the objectives they accomplish on the right.

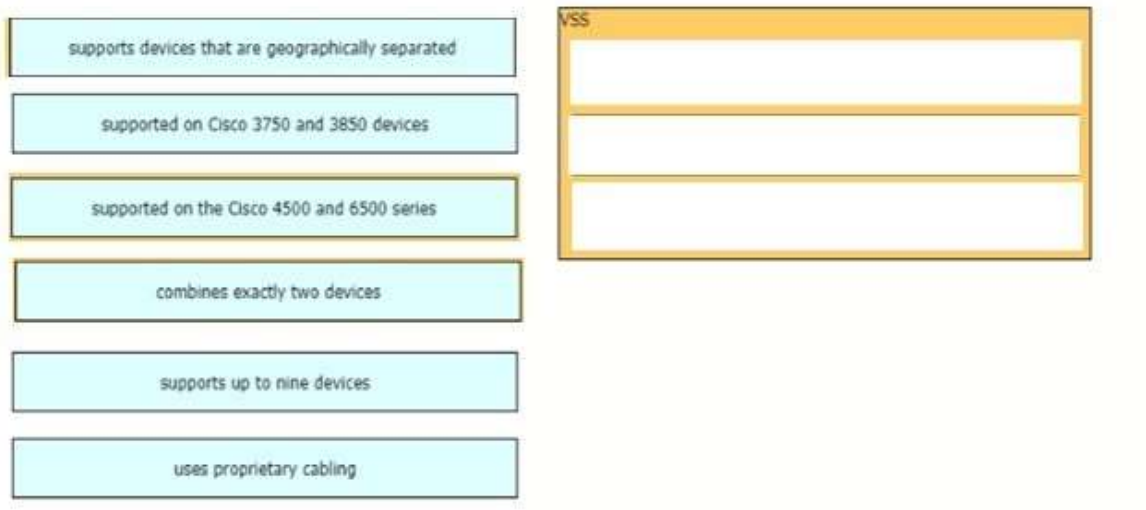


Answer:

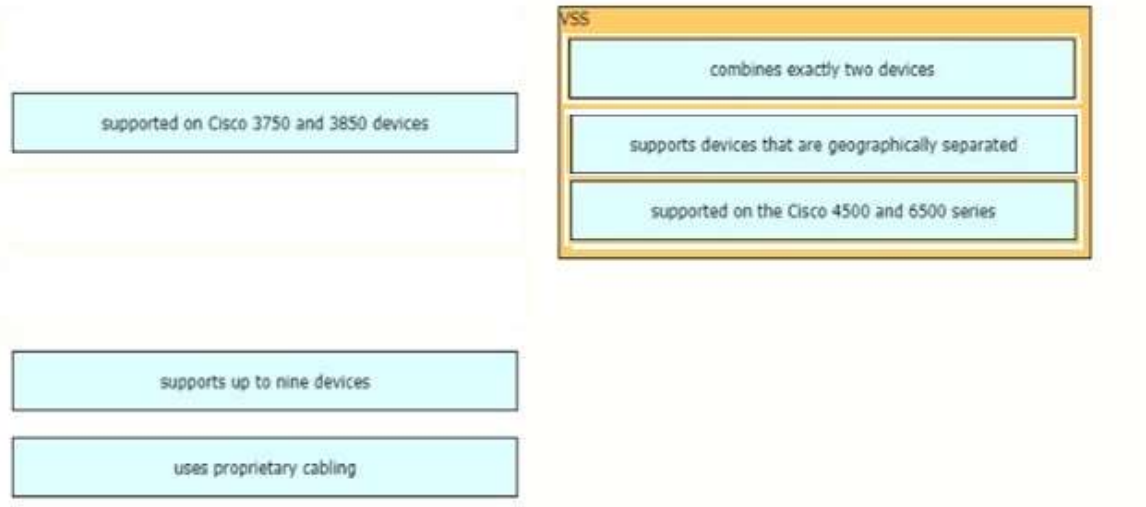


QUESTION 364
Drag and Drop Question

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

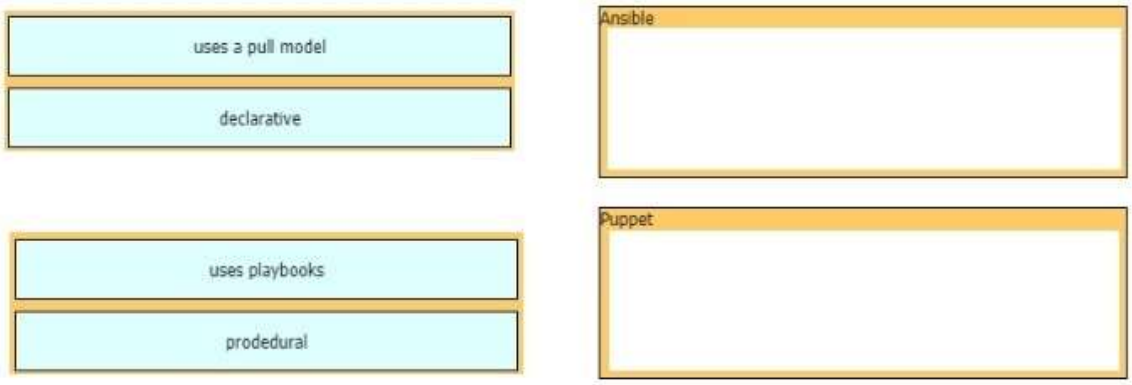


Answer:

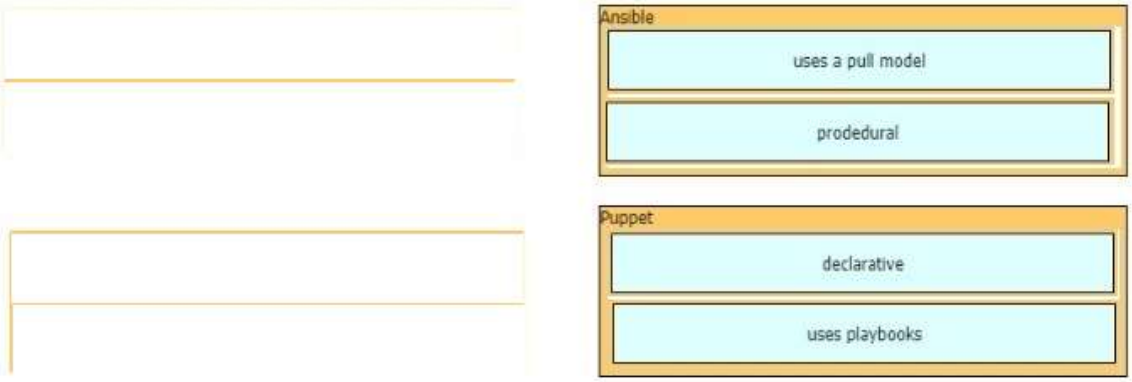


QUESTION 365
Drag and Drop Question

Drag and drop the characteristic from the left onto the orchestration tools that they describe on the right.



Answer:



QUESTION 366
Which data plane protocol does EIGRP Over the Top use?

A. MPLS
B. GRE
C. LISP
D. IP-in-IP

Answer: C

QUESTION 367
Which two actions, when applied in the LAN network segment, will facilitate Layer 3 CAPWAP discovery for lightweight AP? (Choose two.)

A. Utilize DHCP option 17.
B. Configure WLC IP address on LAN switch.
C. Utilize DHCP option 43.
D. Configure an ip helper-address on the router interface
E. Enable port security on the switch port

Answer: CD

QUESTION 368
Refer to the exhibit. Which JSON syntax is derived from this data?



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

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

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

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

Answer: C

QUESTION 369
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

Answer: BD

QUESTION 370
Which outcome is achieved with this Python code?

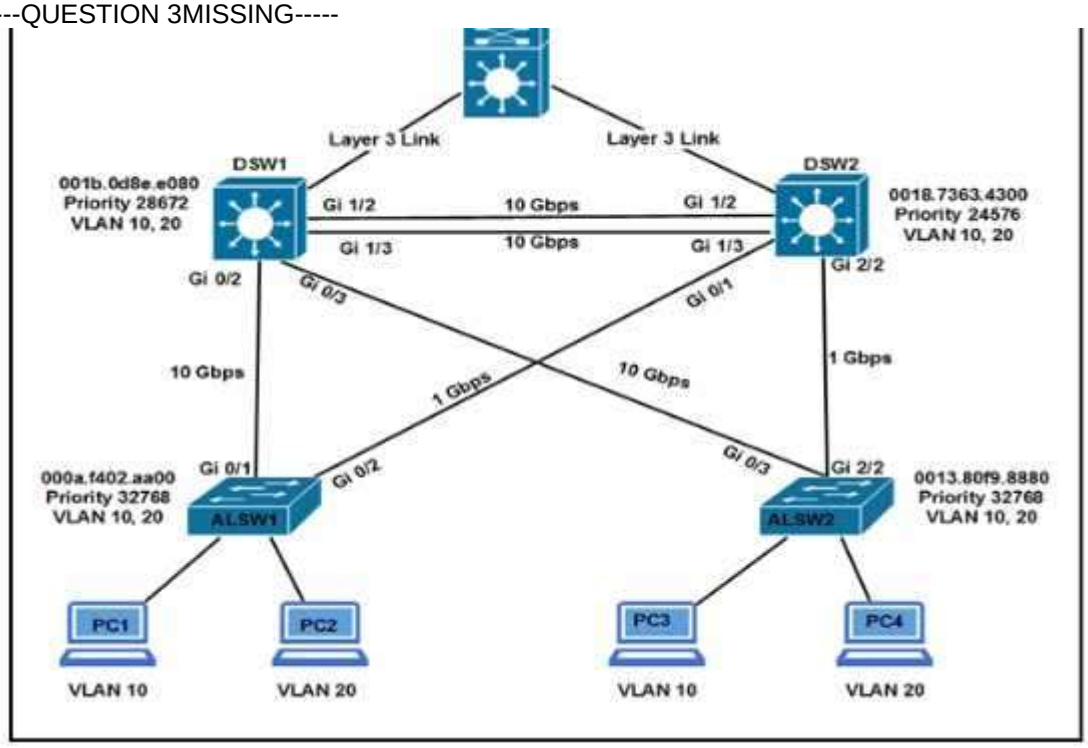
```
client.connect ( ip,  port= 22, username= usr, password= pswd )
stdin,  stdout, stderr = client.exec_command ( 'show ip bgp 192.168.101.0 bestpath\n ' )
print (stdout)
```

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

Answer: C

QUESTION 371
----QUESTION 3MISSING-----



A. DSW2(config if)#spanning-tree port-priority 128
B. DSW2(config-if)#spanning-tree port-priority 16
C. DSW2(onfig-if)#interface gi1/3
D. DSW1(config-if)#interface gi1/3
E. DWS1(config-if)#spanning-tree port-priority 0

Answer: DE

QUESTION 372
In a Cisco SD-Access solution, what is the role of the Identity Services Engine?

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

Answer: C

QUESTION 373
What is the data policy in a Cisco SD-WAN deployment?

A. list of ordered statements that define node configurations and authentication used within the SD-WAN overlay
B. Set of statements that defines how data is forwarded based on IP packet information and specific VPNs
C. detailed database mapping several kinds of addresses with their corresponding location
D. group of services tested to guarantee devices and links liveliness within the SD-WAN overlay

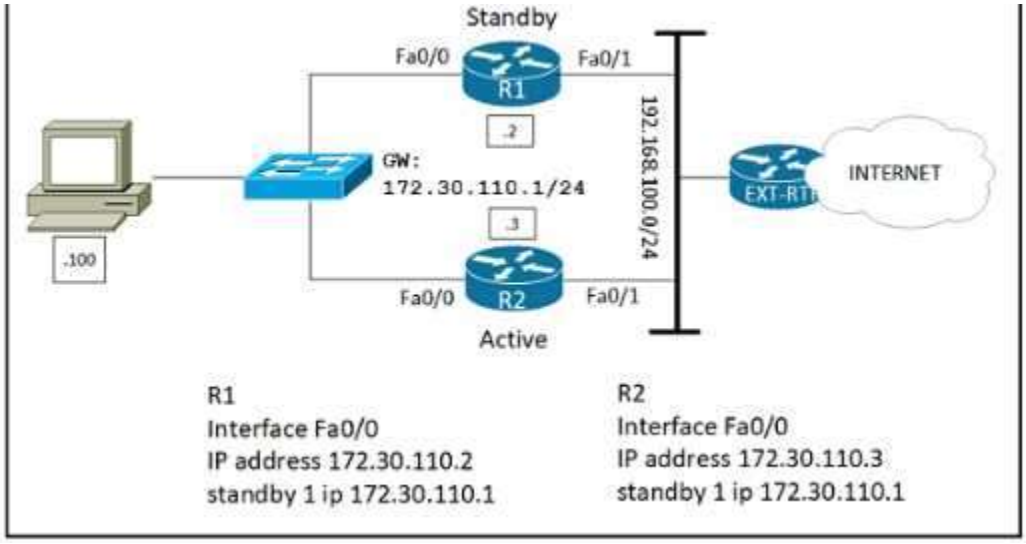
Answer: B

QUESTION 374
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 cl ssification for critical network traffic
B. provide redundant Layer 3 point-to-point links between the core devices for more predictable and faster convergence
C. provide advanced network security features such as 802. IX, DHCP snooping, VACLs, and port security
D. provide redundant aggregation for access layer devices and first-hop redundancy protocols such as VRRP

Answer: A

QUESTION 375
Refer to the exhibit. Which configuration change ensures that R1 is the active gateway whenever it is in a functional state for the 172.30.110.0724 network?



A.
R1
standby 1 preempt
R2
standby 1 priority 90

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

C.
```
R2
standby 1 priority 100
standby 1 preempt
```

D.
```
R2
standby 1 priority 90
standby 1 preempt
```

Answer: D

QUESTION 376
What ate 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

Answer: AD

QUESTION 377
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

Answer: C

QUESTION 378
Refer to the exhibit. Which action resolves the EtherChannel issue between SW2 and SW3?



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


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

A. Configure switchport mode trunk on SW2.
B. Configure switchport nonegotiate on SW3
C. Configure channel-group 1 mode desirable on both interfaces.
D. Configure channel-group 1 mode active on both interfaces.

Answer: D

QUESTION 379
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) jWEP
D. OPEN

Answer: AC

QUESTION 380
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.

Answer: C

QUESTION 381
Which encryption hashing algorithm does NTP use for authentication?

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

Answer: B

QUESTION 382
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"],
}
```

Answer: C

QUESTION 383
Refer to the exhibit. An engineer must assign an IP address of 192.168.1.1/24 to the GigabitEthemet1 in erface.
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

Answer: BE

QUESTION 384
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.

Answer: C

QUESTION 385
Which technology does VXLAN use to provide segmentation for Layer 2 and Layer 3 traffic?

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

Answer: D

QUESTION 386
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

Answer: AC
Explanation:
https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/16450-mcastguide0 html

QUESTION 387
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

Answer: C

QUESTION 388
What is provided by the Stealthwatch component of the Cisco Cyber Threat Defense solution?

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

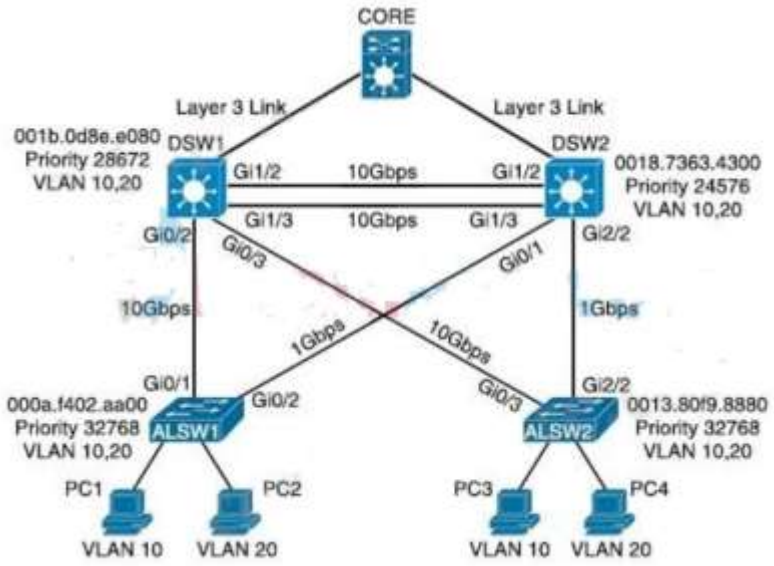
Answer: A

QUESTION 389
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

Answer: B

QUESTION 390
Refer to the exhibit. Assuming all links are functional, which path does PC1 take to reach DSW1?



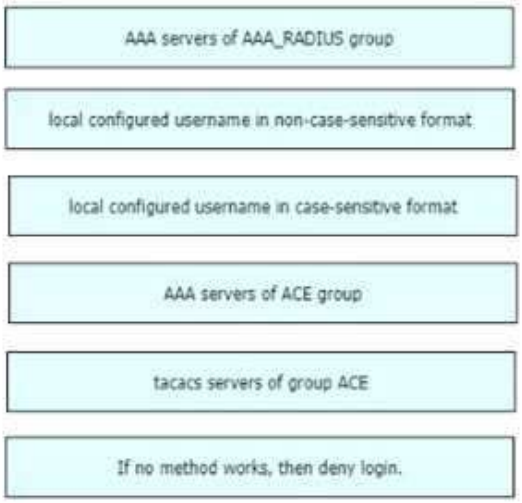
A. PC1 goes from ALSW1 to DSW1
B. PC1 goes form ALSW1 to DSW2 to ALSW2 to DSW1
C. PC1 goes from ALSW1 to DSW2 to Core to DSW1
D. PC1 goes from ALSW1 to DSW2 to DSW1

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.

QUESTION 391
Drag and Drop Question

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

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



Answer:



QUESTION 392
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

QUESTION 393
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

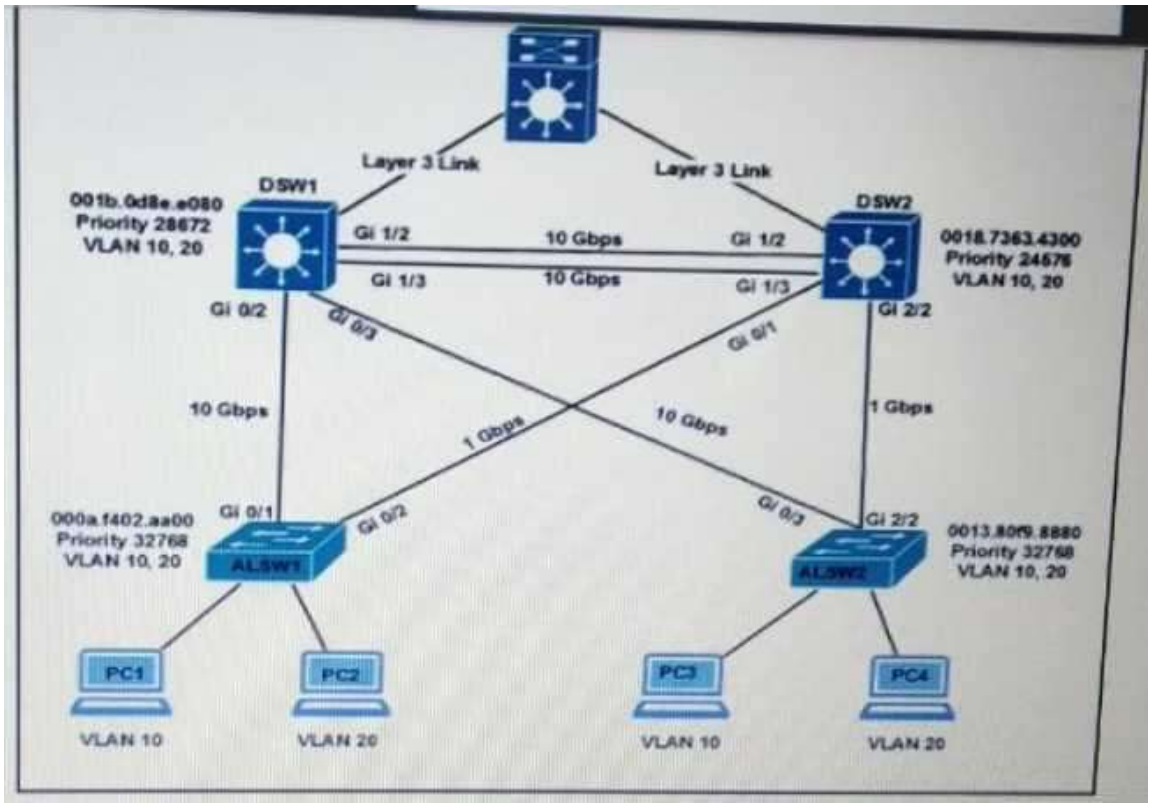
QUESTION 394
Refer to the exhibit. What is the effect of introducing the sampler feature into the Flexible NetFlow configuration on the router?

```
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

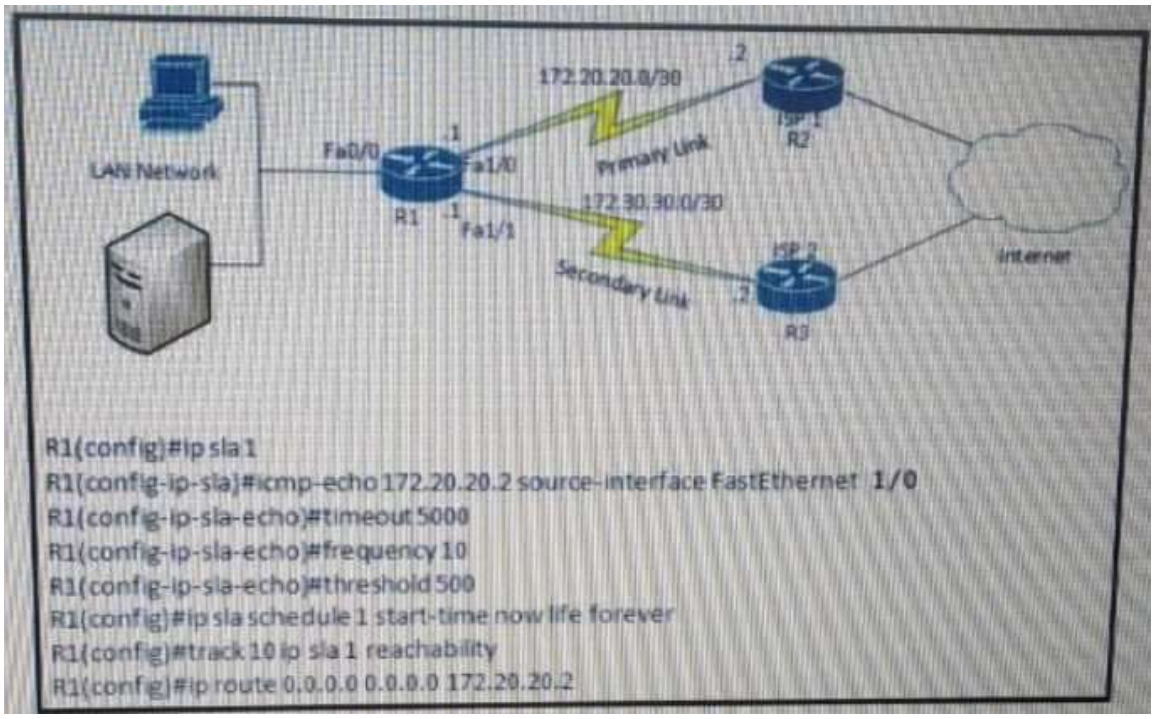
QUESTION 395
Refer to the exhibit. All switches are configured with the default port priority value.
Which two commands ensure that traffic from PC1 is forwarded over Gi1/3 trunk port between DWS1 and DSW2? (Choose two)



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

Answer: AB

QUESTION 396
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.

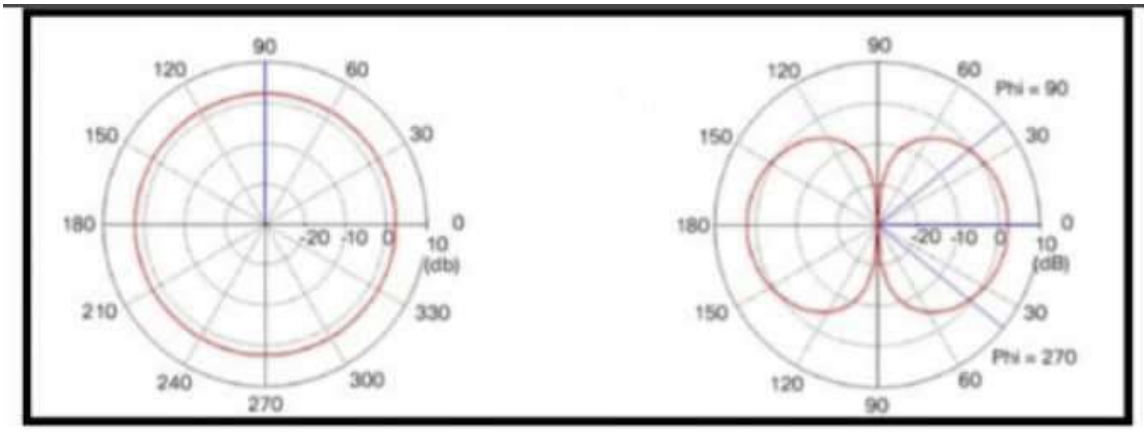
Answer: C

QUESTION 397
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: CD

QUESTION 398
Refer to the exhibit. Which type of antenna is show on the radiation patterns?



A. Dipole
B. Yagi
C. Patch
D. Omnidirectional

Answer: A

QUESTION 399
Which protocol is implemented to establish secure control plane adjacencies between Cisco SD-WAN nodes?

A. IKE
B. DTIS
C. IPsec
D. ESP

Answer: C

QUESTION 400
What is the recommended MTU size for a Cisco SD-Access Fabric?

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

Answer: A

QUESTION 401
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

QUESTION 402
What is the wireless received signal strength indicator?

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

Answer: D

QUESTION 403
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

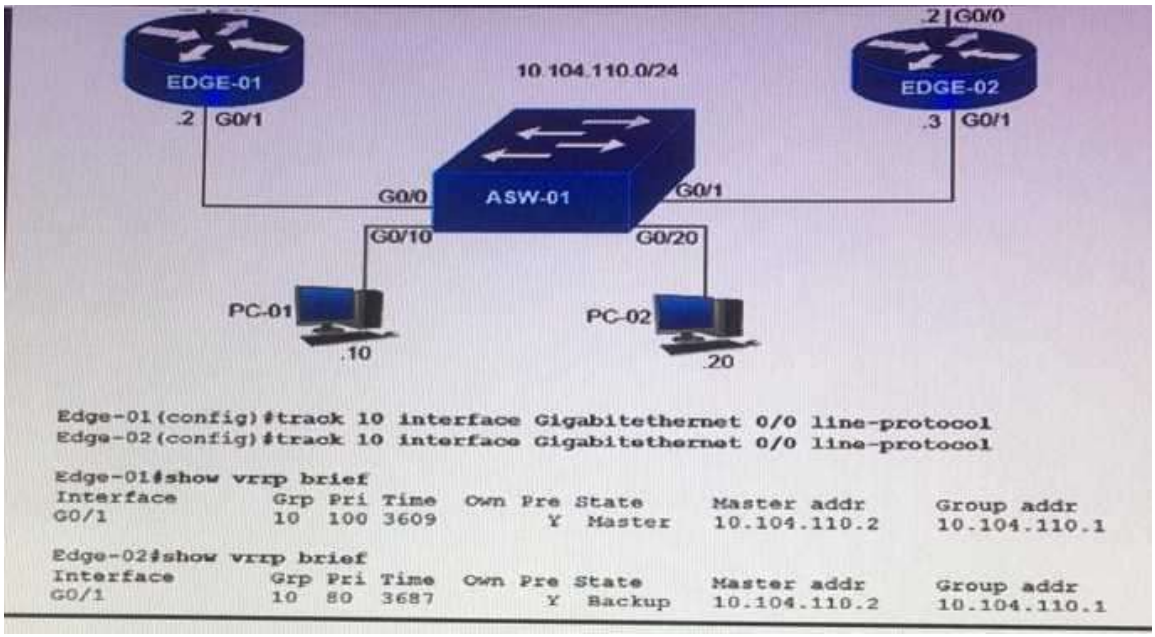
Answer: A

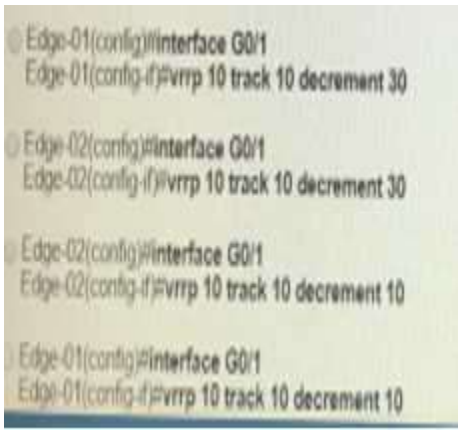
QUESTION 404
When does a stack master lose its role?

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: A

QUESTION 405
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

QUESTION 406
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

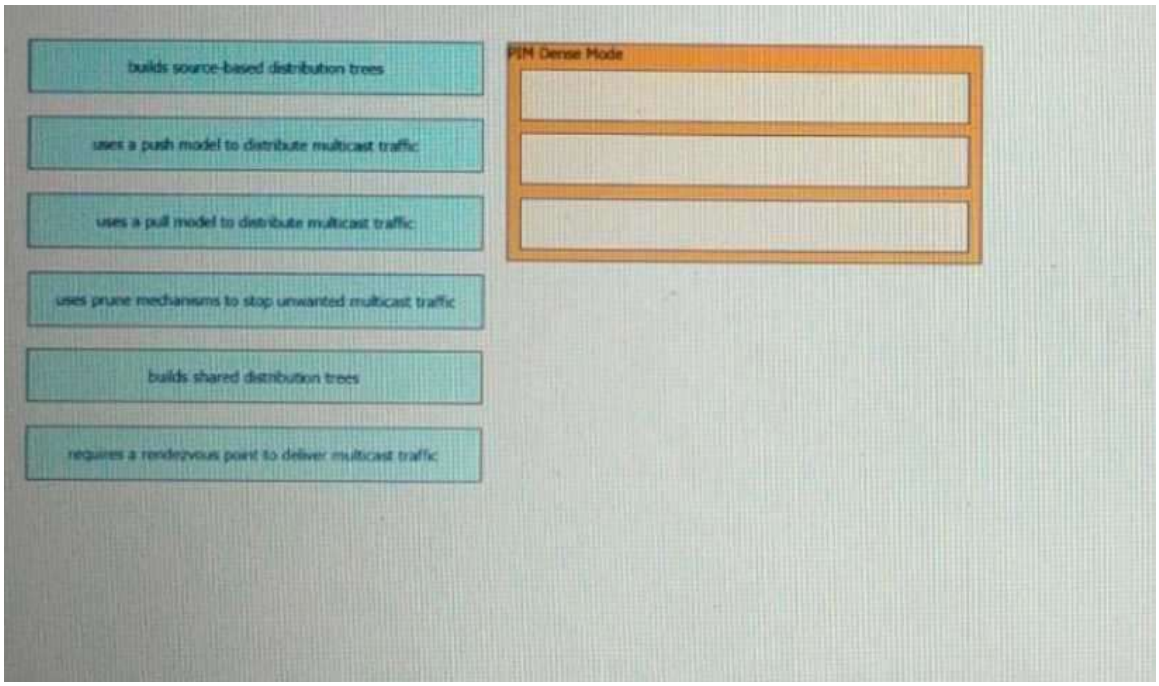
QUESTION 407
What is a benefit of a virtual machine when compared with a physical server?

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.

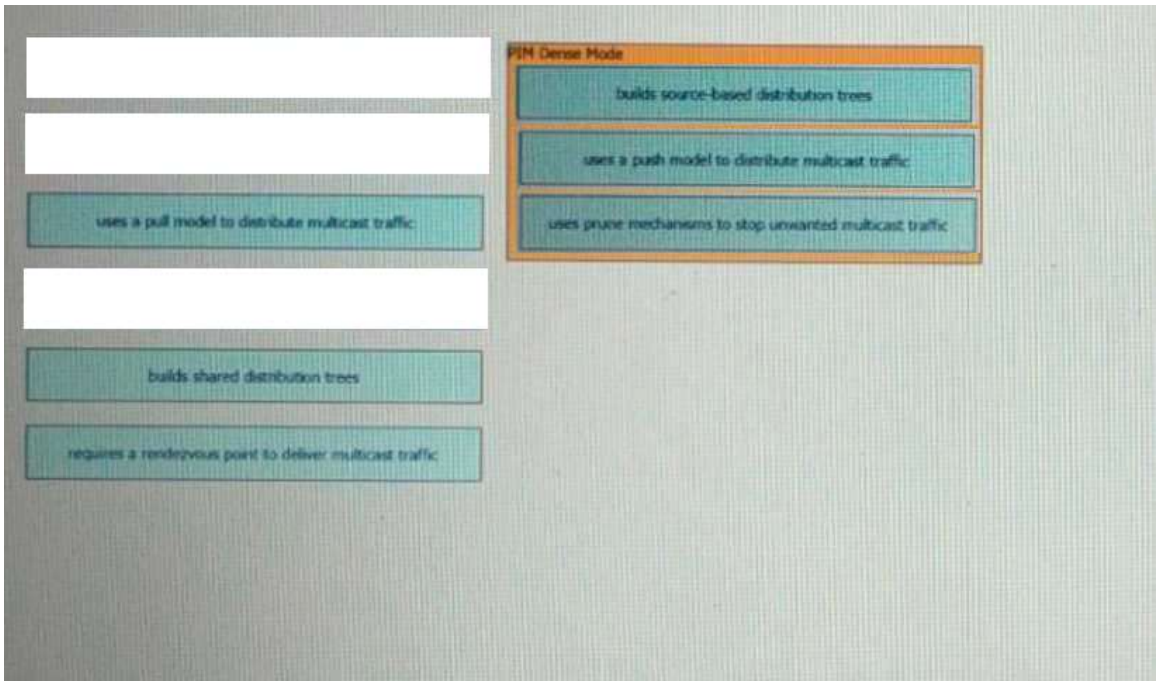
Answer: A

QUESTION 408
Drag and Drop Question

Drag and drop characteristics of PIM dense mode from the left to the right.



Answer:



QUESTION 409
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

Answer: D

QUESTION 410
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

Answer: B

QUESTION 411
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 swich2 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
```

- switch1(config)# **interface GigabitEthernet 1/1**
  switch1(config-if)# **switchport mode access**
  switch1(config-if)# **switchport access vlan 10**

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

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

Answer: BD

QUESTION 412
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

Answer: B

QUESTION 413
Refer to the exhibit. Which outcome is achieved with this Python code?

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

A. displays the output of the show command in an unformatted way
B. displays the output of the show command in a formatted way
C. connects to a Cisco device using Telnet and exports the routing table information

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

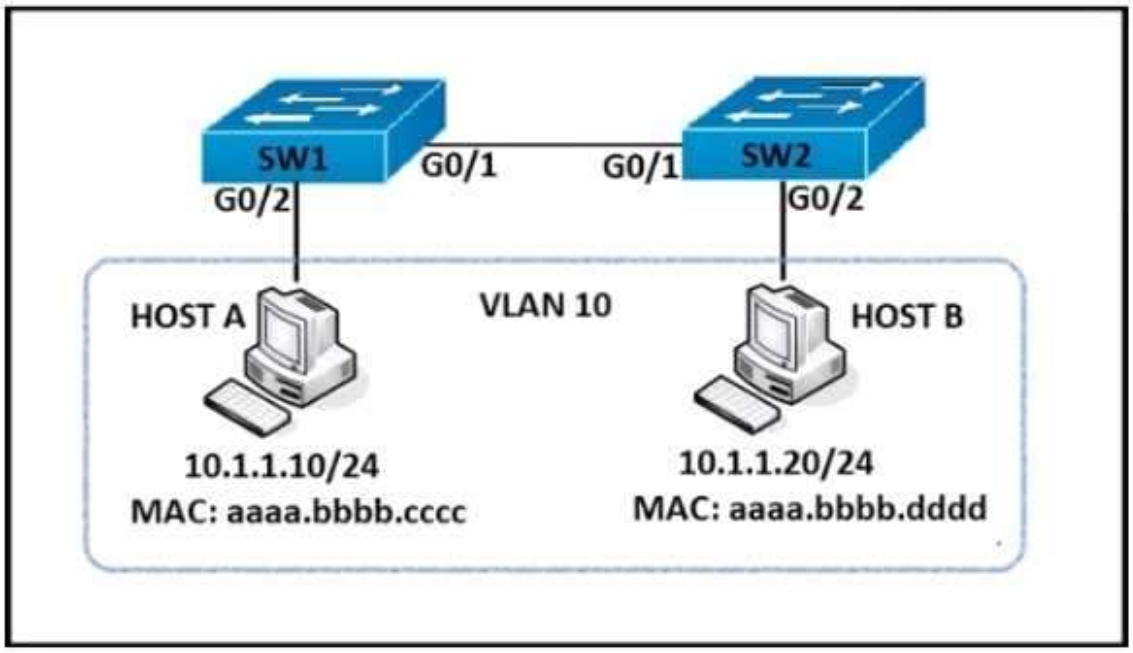
Answer: B

QUESTION 414
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

Answer: A

QUESTION 415
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

Answer: A

QUESTION 416
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 1.3.6.1.4.1.9.9.109.1.1.1.1.3 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"

Answer: B

QUESTION 417
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

Answer: C

QUESTION 418
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.

Answer: B

QUESTION 419
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.

Answer: B

QUESTION 420
How do cloud deployments differ from on-prem deployments?

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

Answer: B

QUESTION 421
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

Answer: D

QUESTION 422
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

QUESTION 423
What is a characteristic of a WLC that is in master controller mode?

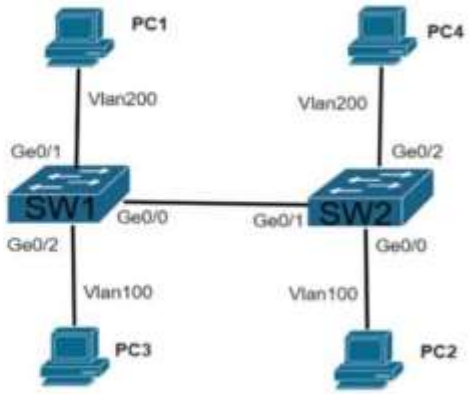
A. All new APs that join the WLAN are assigned to the master controller.
B. The master controller is responsible for load balancing all connecting clients to other controllers.
C. All wireless LAN controllers are managed by the master controller.
D. Configuration on the master controller is executed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

Answer: A

QUESTION 424
Refer to the exhibit. The connection between SW1 and SW2 is not operational.
Which two actions resolve the issue? (Choose two.)

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

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



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

Answer: CE

QUESTION 425
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 1syslog write "OSPF ROUTING ERROR"

Answer: C

QUESTION 426
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

Answer: D

QUESTION 427
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.

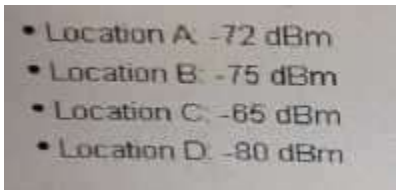
Answer: A

QUESTION 428
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: AB

QUESTION 429
An engineer measures the Wi-Fi coverage at a customer site. The RSSI values are recorded as follows:



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

A. The signal strength at location B is 10 dB better than location C.
B. Location D has the strongest RF signal strength.
C. The signal strength at location C is too weak to support web surfing.
D. The RF signal strength at location B is 50% weaker than location A
E. The RF signal strength at location C is 10 times stronger than location B

Answer: DE

QUESTION 430
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.

Answer: C

QUESTION 431

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

Answer: ABE

QUESTION 432
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

Answer: A

QUESTION 433
Which three methods does Cisco DNA Center use to discover devices? (Choose three.)

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

Answer: ACF