



Vendor: Cisco

Exam Code: 350-401

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

Version: 20.092

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

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 trying 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 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.

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. Therefore it is called Fast Transition. 802.11r provides two methods of roaming:

- + Over-the-air: With this type of roaming, the client communicates directly with the target AP using IEEE 802.11 authentication with the Fast Transition (FT) authentication algorithm.
- + Over-the-DS (distribution system): With this type of roaming, the client communicates with the target AP through the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP and is then sent through the controller.

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

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

Reference: <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?

Name is Bob Johnson
Age is 75
is alive

Favorite foods are:

- Cereal
- Mustard
- Onions

- 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

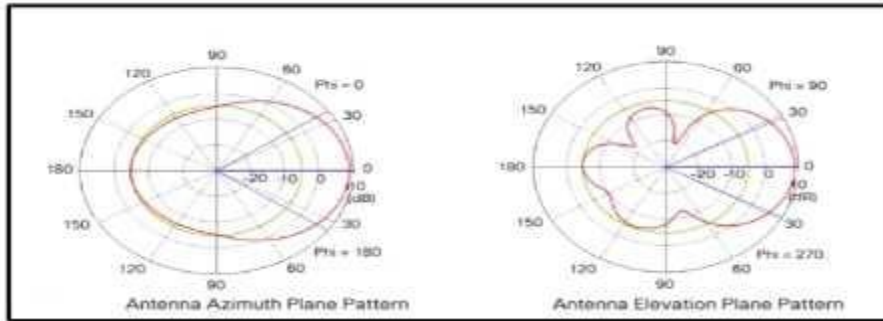
If a VRRP master router fails, which router is selected as the new master router?

- 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?



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

Answer: A

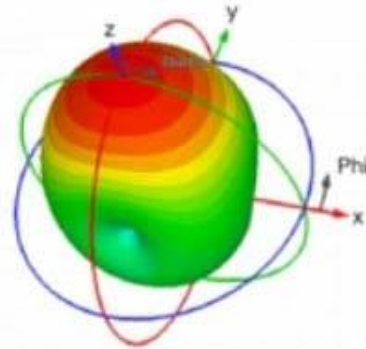
Explanation:

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.

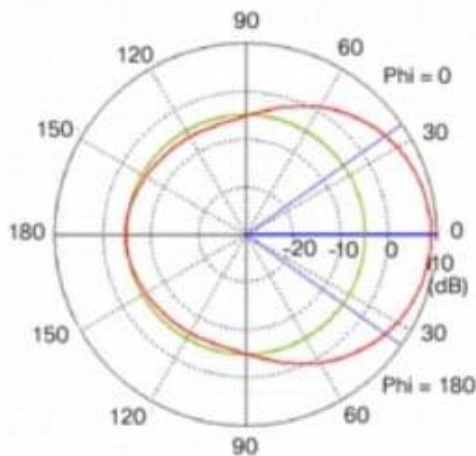
The azimuth and elevation plane patterns are derived by simply slicing through the 3D radiation pattern. In this case, the azimuth plane pattern is obtained by slicing through the x-z plane, and the elevation plane pattern is formed by slicing through the y-z plane. Note that there is one main lobe that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



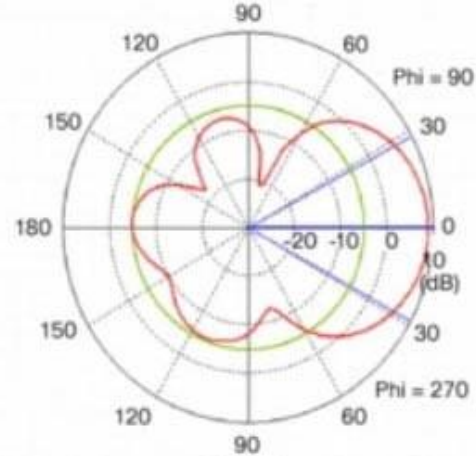
(a) Patch Antenna Model



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

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

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

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

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

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

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

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

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

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. RADIUS 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.

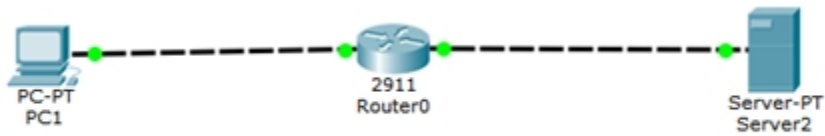
Which statement allows this traffic?

- 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 lt 80 host 209.165.201.25
- D. permit tcp host 209.165.200.225 host 209.165.201.25 eq 80

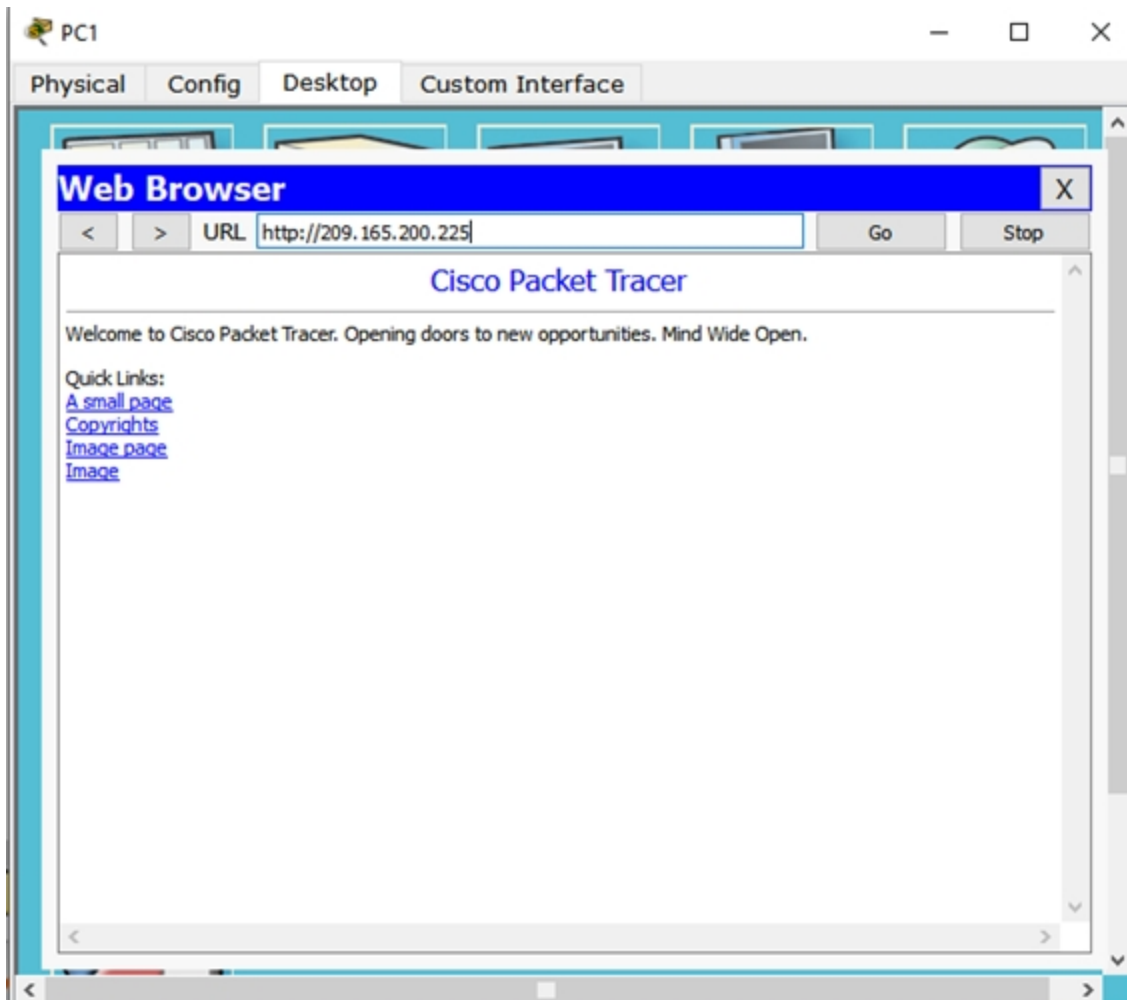
Answer: A

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.

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

Answer:

OSPF
link state routing protocol
metric is based on delay and reliability by default
makes it easy to segment the network logically

EIGRP
supports unequal path load balancing
distance vector routing protocol
constructs three tables as part of its operation: neighbor table, topology table and routing table

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	64517 i
*		192.168.101.14	80	80	0	64516 i
*		192.168.101.10			0	64515 64515 i
*>		192.168.101.2			32768	64513 i
*		192.168.101.6		80	0	64514 64514 i

- 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. NETCONF

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

- A. The EEM applet runs 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:

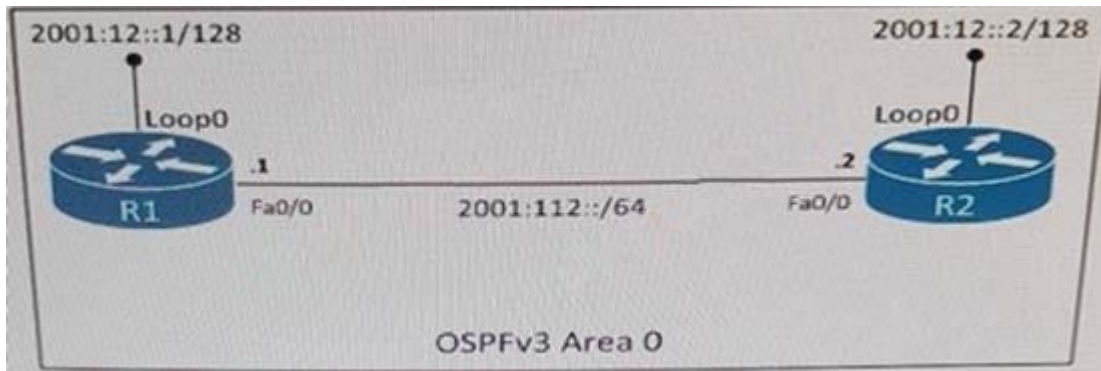
Cisco IOS XE supports the Yet Another Next Generation (YANG) data modeling language. YANG can be used with the Network Configuration Protocol (NETCONF) to provide the desired solution of automated and programmable network operations. NETCONF(RFC6241) is an XML-based protocol that client applications 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.yyyyyy.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/xr-3s/eem-xr-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_paper0900aecd806fb52.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, misordering and packet loss by 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:

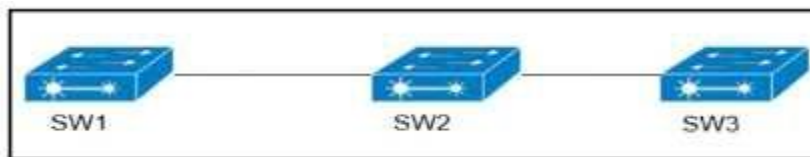
This paragraph was taken from the link <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/69340-web-auth-config.html#c5>:

“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: AD

Explanation:

The logging synchronous global configuration command also affects the display of messages to the console. When this command is enabled, messages appear only after you press Return.
Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swlog.html

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?

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

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

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

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

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 02039485748” 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/xr-16/qos-mqc-xr-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 Eligibility
- 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/xr-16-6/qos-mqc-xr-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/xs-16/qos-conavd-xe-16-book/qos-conavd-overview.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 relies 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 filter must 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](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?

The screenshot shows a network configuration window with tabs for General, Security, QoS, Policy-Mapping, and Advanced. Under the Security tab, there are sub-tabs for Layer 2, Layer 3, and AAA Servers. The Layer 3 sub-tab is active, showing sections for Fast Transition, Protected Management Frame (PMF), WPA+WPA2 Parameters, and Authentication Key Management. In the WPA+WPA2 Parameters section, WPA Policy is disabled and WPA2 Policy-AES is checked. In the Authentication Key Management section, 802.1X, CCKM, PSK (checked), FT 802.1X, and FT PSK are listed, each with an 'Enable' button. The PSK Format is set to ASCII.

- 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](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?

| Client Properties       |                                           | AP Properties         |                 |
|-------------------------|-------------------------------------------|-----------------------|-----------------|
| RAC Address             | 90.09:ef:86:07:bd                         | AP Address            | 172.22.253.20   |
| IP Address              | 192.168.100.196                           | AP Name               | 172.22.253.20   |
| Client Type             | Regular                                   | AP Type               | Mobile          |
| User Name               |                                           | WPA2 Profile          | WPA2            |
| Port Number             | 20                                        | Status                | Associated      |
| Interface               | Staff                                     | Association ID        | 0               |
| VLAN ID                 | 3602                                      | 802.11 Authentication | Open System     |
| LLN version             | Not Supported                             | Reason Code           | 1               |
| RF Version              | Not Supported                             | Status Code           | 0               |
| Mobility Role           | Anchor                                    | CF Putable            | Not Implemented |
| Mobility Peer           | 172.22.253.20                             | CF Poll Request       | Not Implemented |
| IP Address              |                                           | Short Preamble        | Implemented     |
| Policy Manager          | SNR                                       | PSOC                  | Not Implemented |
| State Management        | No                                        | Channel Agility       | Not Implemented |
| Protection Uptime (Sec) | 3719                                      | Timeout               | 0               |
| Power Save              | Off                                       | WPA State             | WPA Enable      |
| Current TxPowerSet      | 5.5,11.0,5.0,9.0,12.0,10.0,26.0,35.0,43.0 |                       |                 |
| RateSet                 | 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 password-encryption" 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 D 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](http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0e.shtml))

Neighbors Stuck in Exstart/Exchange State

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

#### 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 popular 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 based on 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 network 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](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 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 password 7 045802150C2E
 login
line vty 5 15
 password 7 045802150C2E
 login
!
end

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

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

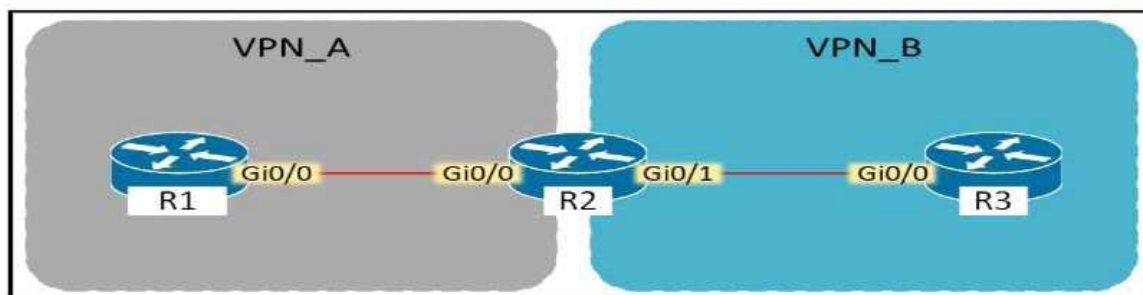
**Answer: A**

**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

- C. Management VRF
- D. VRF VPN\_A

**Answer:** D

#### **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](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://YOURIPins'
switchuser='USERID'
switchpassword='PASSWORD'

myheaders={'content-type':'application/json'}
payload={
 "ins_api": {
 "type": "cli_show",
 "version": "1.0",
 "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_instmp": "06/14/1970 09:49:54",
 "chassis_id": "Nexus9000 9318IYC-FX chassis",
 "cpu_name": "Intel(R) Xeon(R) CPU @ 1.80GHz",
 "memory": "24633488",
 "mem_type": "MS",
 "nr_uscs": "134703",
 "nr_ctime": "Sun Mar 10 15:41:46 2019",
 "nr_reason": "Reset Requested by CLI command reload",
 "nr_sys_ver": "7.0(3)I7(4)",
 "nr_service": "",
 "manufacturer": "Cisco Systems, Inc",
 "TABLE_package_list": {
 "ROW_package_list": {
 "package_id": 0
 }
 }
 }
 }
 }
 }
}
```

- 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  $\text{metric} < \text{variance} * \text{best\_metric}$  into the local routing table, provided that it meets the feasibility condition to prevent routing loop. The path that meets this requirement is called a feasible successor. If a path is not a feasible successor, it is not used in load balancing.

Note: The feasibility condition states that, the Advertised Distance (AD) of a route must be lower than the feasible distance of the current successor route.

### 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 GigabitEthernet0/0 interface of the router.

However, the router can still ping hosts on the 209.165.200.0/24 subnet.

Which explanation of this behavior is true?

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

**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: A**

**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.

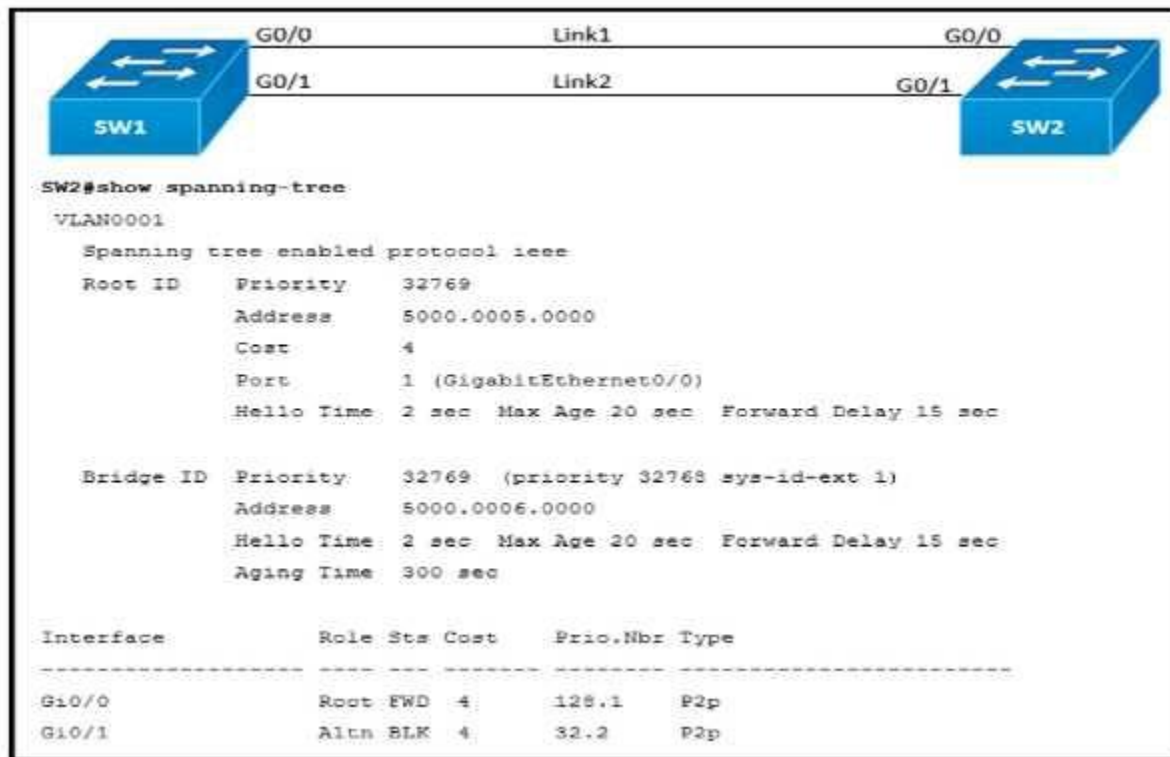
+ Netconf and CLI - Netconf is a standards-based protocol used by the vManage NMS to provision a vSmart controller. In addition, each vSmart controller provides local CLI access and AAA.

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 Link2 to resolve the issue?



- 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:** A

**Explanation:**

Ansible can communicate with modern Cisco devices via SSH or HTTPS so it does not require an SSH server -> Answer B is not correct.

An Ansible ad-hoc command uses the /usr/bin/ansible command-line tool to automate a single task on one or more managed nodes. Ad-hoc commands are quick and easy, but they are not reusable -> It is not a requirement either -> Answer C is not correct.

Ansible Tower is a web-based solution that makes Ansible even more easy to use for IT teams of all kinds. But it is not a requirement to run Ansible -> Answer D is not correct.

Therefore only answer A is the best choice left. An Ansible controller (the main component that manages the nodes), is supported on multiple flavors of Linux, but it cannot be installed on Windows.

#### 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-CONTROILLER.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](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](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

R2
interface GigabitEthernet0/1
 ip address 192.0.2.2 255.255.255.252
 ip ospf 1 area 0
 ip ospf cost 500
```

- 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 interval 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 not supported on Cisco devices.
- C. It required certificates for authentication.
- D. It is used for HTTP and HTTPS requests.

**Answer: C**

**Explanation:**

The https-based protocol-RESTCONF (RFC 8040), which is a stateless protocol, uses secure HTTP methods to provide CREATE, READ, UPDATE and DELETE (CRUD) operations on a conceptual datastore containing YANG-defined data -> RESTCONF only uses HTTPS.

RESTCONF servers MUST present an X.509v3-based certificate when establishing a TLS connection with a RESTCONF client. The use of X.509v3-based certificates is consistent with NETCONF over TLS -> Answer C is correct.

Reference: <https://tools.ietf.org/html/rfc8040>

#### QUESTION 105

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

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

**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.

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

**Answer:**

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

**QUESTION 107**

Drag and Drop Question

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

|                                                   |                         |
|---------------------------------------------------|-------------------------|
| causes TCP retransmission when traffic is dropped | <b>Traffic Policing</b> |
| buffers excessive traffic                         |                         |
| introduces no delay and jitter                    |                         |
| introduces delay and jitter                       |                         |
| drops excessive traffic                           |                         |
| typically delays, rather than drops traffic       |                         |

**Answer:**

|  |                                                   |
|--|---------------------------------------------------|
|  | <b>Traffic Policing</b>                           |
|  | causes TCP retransmission when traffic is dropped |
|  | introduces no delay and jitter                    |
|  | drops excessive traffic                           |
|  | <b>Traffic Shaping</b>                            |
|  | buffers excessive traffic                         |
|  | introduces delay and jitter                       |
|  | typically delays, rather than drops traffic       |

**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](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

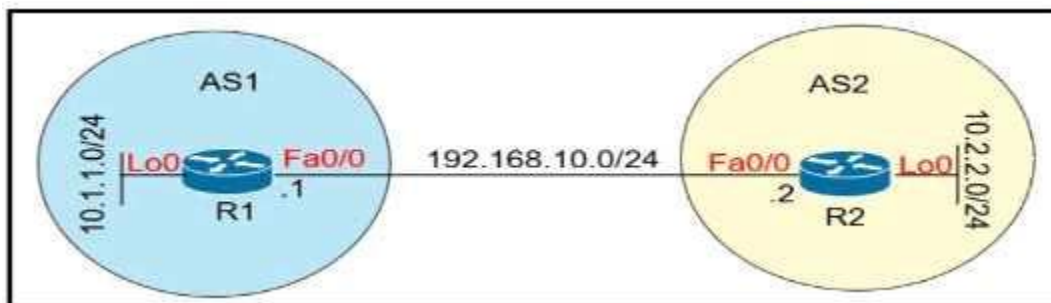
#### Explanation:

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 10.0.0.0.0.0.1
- 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: 00011111 = 31).

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

Therefore network 172.23.16.0 0.0.15.255 ranges from 172.23.16.0 to 172.23.31.255.

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

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

Therefore in this question, only the statement "permit 10.0.0.1 0.0.0.254" will allow all 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 and must be connected directly to the fabric border node.
- B. It is in FlexConnect mode and must be connected directly to the fabric border node.
- C. It is in local mode and must be connected directly to the fabric edge switch.
- D. It is in FlexConnect mode and must be connected directly to the fabric edge switch.

**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:**

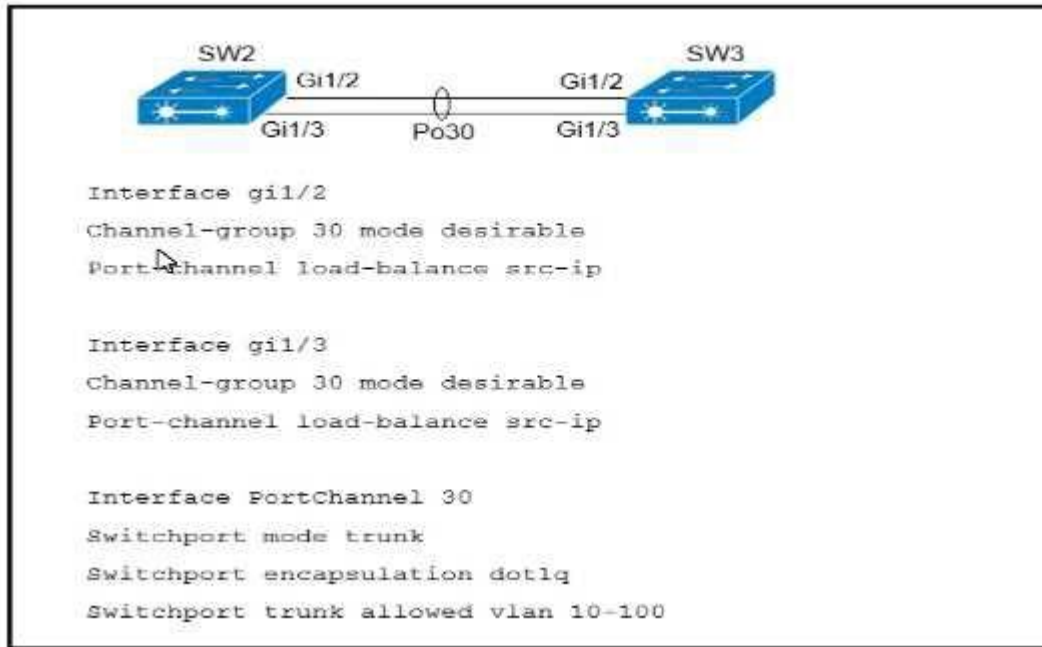
The EAP-FAST protocol is a publicly accessible IEEE 802.1X EAP type that Cisco developed to support customers that cannot enforce a strong password policy and want to deploy an 802.1X EAP type that does not require digital certificates.

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 made, the port channel does not establish. Based on the configuration excerpt of SW3, what is the cause of the problem?



- A. The port channel 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 load 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 GigabitEthernet 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

**QUESTION 124**

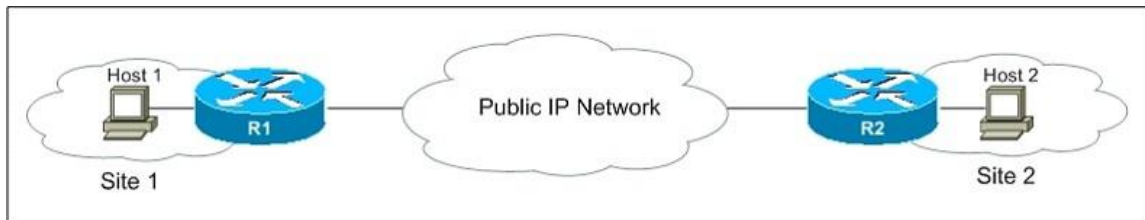
Into which two pieces of information does the LISP protocol split the device identity? (Choose two.)

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

**Answer:** AB

**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

**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**

**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**

**QUESTION 129**

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

- A. RADIUS authentication queries the router's local username database.
- B. TACACS+ authentication uses an RSA server to authenticate users.
- C. Local user names are case-insensitive.
- D. Local authentication is maintained on the router.
- E. KRB5 authentication disables user access when an incorrect password is entered.

**Answer: 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**



**QUESTION 133**

Which configuration restricts the amount of SSH 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: C**

#### 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**

#### QUESTION 135

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

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

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

**QUESTION 138**

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

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

**Answer:** B

**Explanation:**

<https://www.cisco.com/c/en/us/td/docs/security/firepower/ftd-api/guide/ftd-rest-api/auth-ftd-rest-api.pdf>

**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:**

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

**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

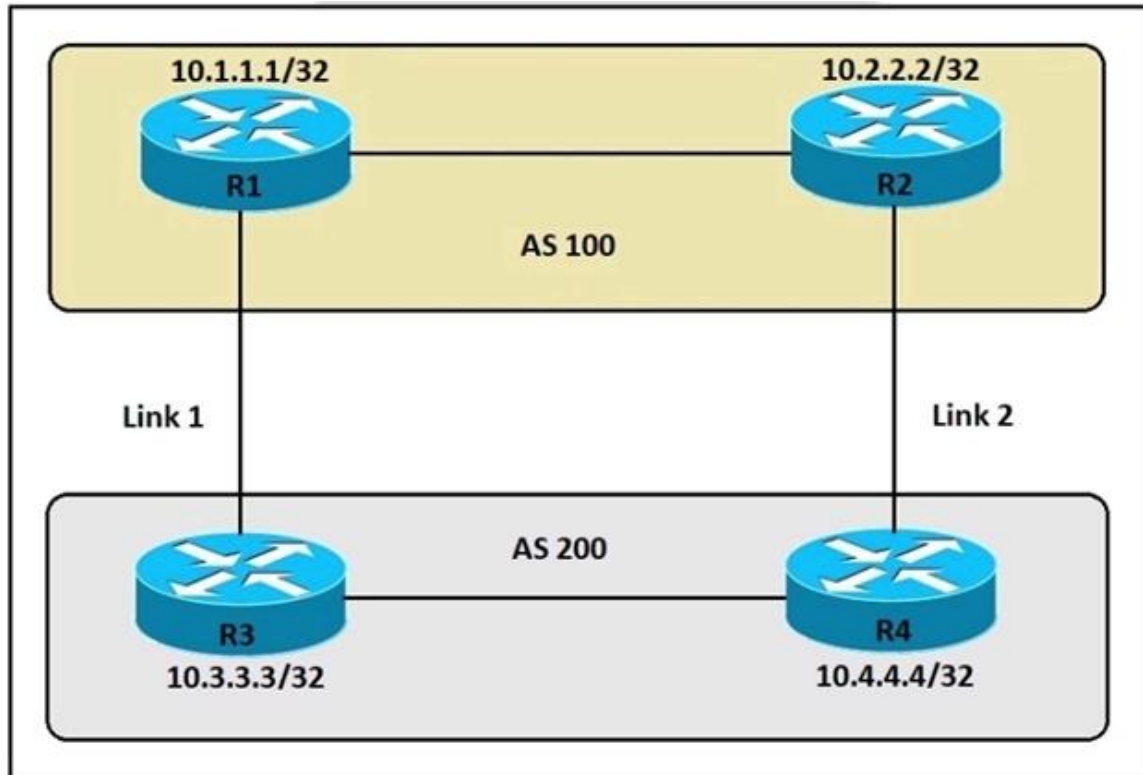
**Answer:** B

**Explanation:**

[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](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)neighbor 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**

**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**

**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:** C

**QUESTION 151**

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

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

**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

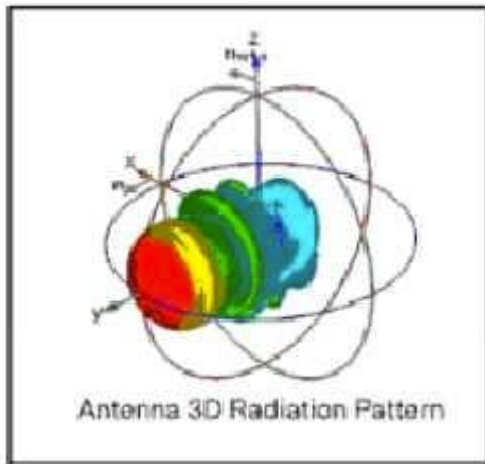
**Explanation:**

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**

**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**

**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

**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?

**WLANs > Edit 'Guest\_Wireless'**

| General                                                                       |                   | Security |  | QoS         |                                             | Policy-Mapping    |  | Advanced |  |
|-------------------------------------------------------------------------------|-------------------|----------|--|-------------|---------------------------------------------|-------------------|--|----------|--|
| Layer 2                                                                       |                   | Layer 3  |  | AAA Servers |                                             |                   |  |          |  |
| Select AAA servers below to override use of default servers on this WLAN      |                   |          |  |             |                                             |                   |  |          |  |
| <b>RADIUS Servers</b>                                                         |                   |          |  |             |                                             |                   |  |          |  |
| RADIUS Server Overwrite interface <input checked="" type="checkbox"/> Enabled |                   |          |  |             |                                             |                   |  |          |  |
| Interface Priority <span>WLAN</span>                                          |                   |          |  |             |                                             |                   |  |          |  |
| <b>Authentication Servers</b>                                                 |                   |          |  |             | <b>Accounting Servers</b>                   |                   |  |          |  |
| <input checked="" type="checkbox"/> Enabled                                   |                   |          |  |             | <input checked="" type="checkbox"/> Enabled |                   |  |          |  |
| Server 1                                                                      | <span>None</span> |          |  |             | Server 1                                    | <span>None</span> |  |          |  |
| Server 2                                                                      | <span>None</span> |          |  |             | Server 2                                    | <span>None</span> |  |          |  |
| Server 3                                                                      | <span>None</span> |          |  |             | Server 3                                    | <span>None</span> |  |          |  |
| Server 4                                                                      | <span>None</span> |          |  |             | Server 4                                    | <span>None</span> |  |          |  |
| Server 5                                                                      | <span>None</span> |          |  |             | Server 5                                    | <span>None</span> |  |          |  |
| Server 6                                                                      | <span>None</span> |          |  |             | Server 6                                    | <span>None</span> |  |          |  |

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

**Answer: A**

**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**

**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: A**

#### QUESTION 162

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



Which command set resolves this error?

- A. SW1(config-if)#**interface G0/0**  
SW1(config-if)#**no spanning-tree bpdudfilter**  
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 facilitates a migrate from a traditional campus design to a programmer fabric designer?

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

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

**Answer: D**

**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**

**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 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?

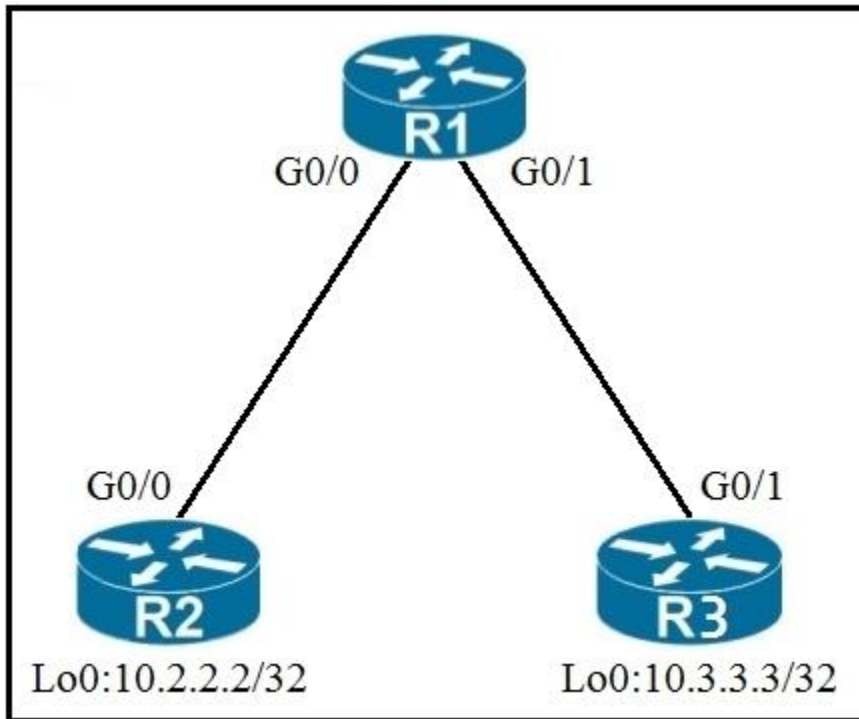
- A. tunneling traffic from IPv6 to IPv4 VXLANs
- B. allowing encrypted communication on the local VXLAN Ethernet segment
- C. encapsulating and de-encapsulating VXLAN Ethernet frames
- D. tunneling traffic from IPv4 to IPv6 VXLANs



Answer: C

**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**

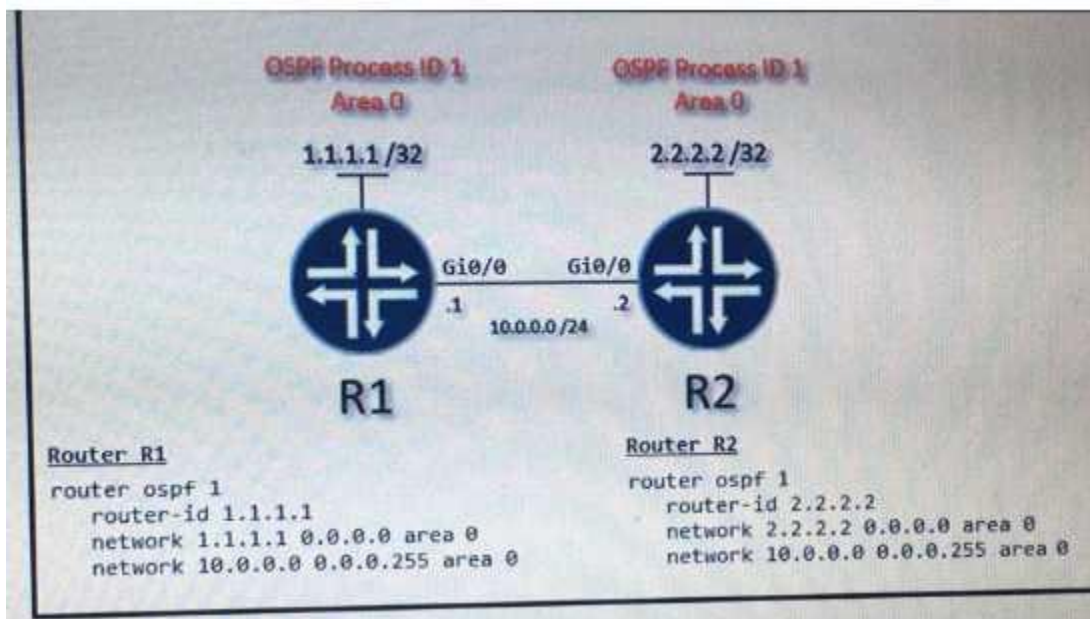
**Explanation:**

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?



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**

**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**

**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: B**

**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 is 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: D**

**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 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

#### QUESTION 182

Drag and Drop Question

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



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

**Answer:**

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

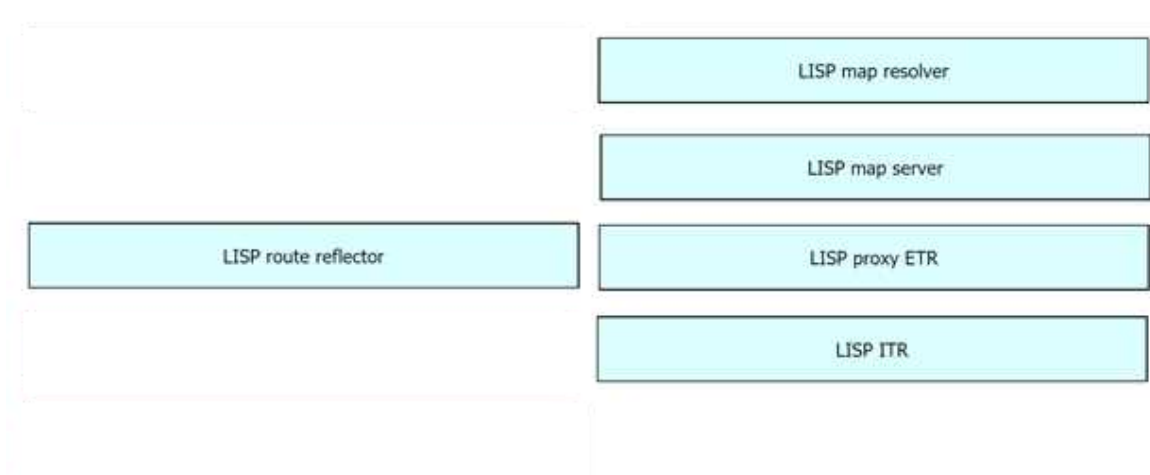
### QUESTION 183

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.

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

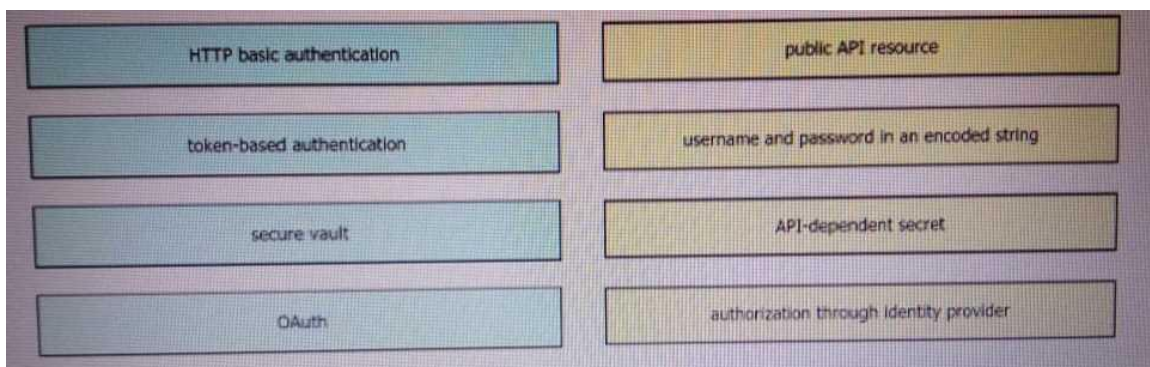
**Answer:**



**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**

**QUESTION 186**

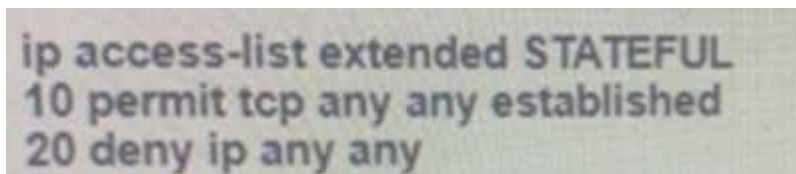
Which characteristic distinguishes Ansible from Chef?

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

**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**

**QUESTION 188**

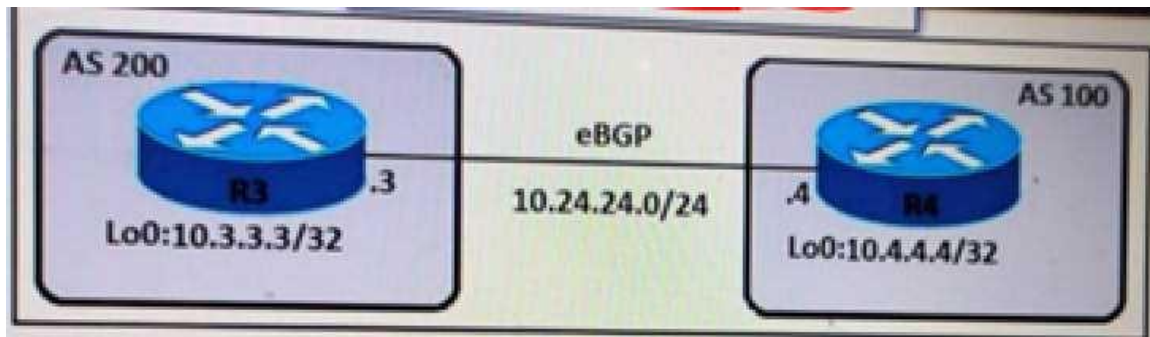
What function does vxlan perform in an SD-Access deployment?

- 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?



- ☐ 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
- ☐ 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
- ☐ 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

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

**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?



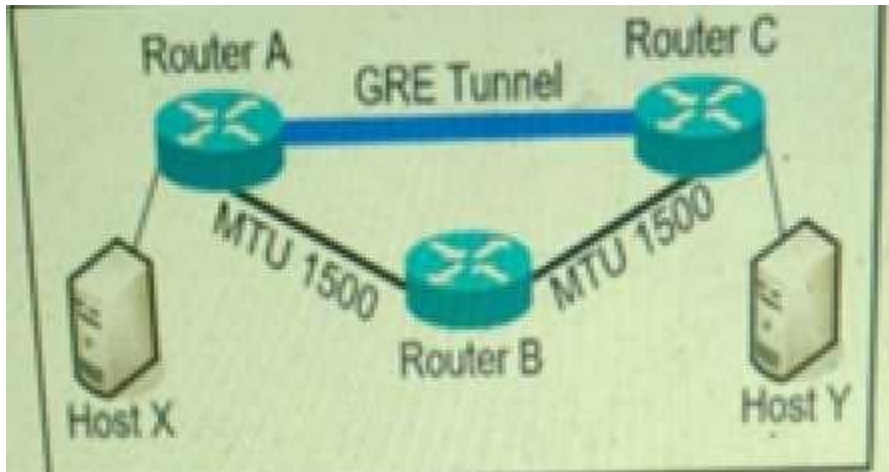
- R1(config)# interface GigabitEthernet 0/0  
R1(config)# ip nat outside
- R1(config)# interface GigabitEthernet 0/1  
R1(config)# ip nat inside
- R1(config)# interface GigabitEthernet 0/0  
R1(config-if)# ip nat outside
- R1(config)# interface GigabitEthernet 0/1  
R1(config-if)# ip nat inside
- R1(config)# interface GigabitEthernet 0/0  
R1(config-if)# ip nat inside
- R1(config)# interface GigabitEthernet 0/1  
R1(config-if)# ip nat outside
- R1(config)# interface GigabitEthernet 0/0  
R1(config)# ip nat inside
- R1(config)# interface GigabitEthernet 0/1  
R1(config)# ip nat outside

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

**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-byte IPv4 packet traverses the GRE tunnel from host X to host Y, assuming the DF bit is cleared?



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

**Answer: A**

**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**

**QUESTION 193**

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 lt 80 host 209.165.201.25
- D. permit tcp host 209.165.200.225 host 209.165.201.25 eq 80

**Answer: B**

**QUESTION 194**

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:**

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