New ENCOR Questions

June 23rd, 2020 in New ENCOR Questions Go to comments

Question 1

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

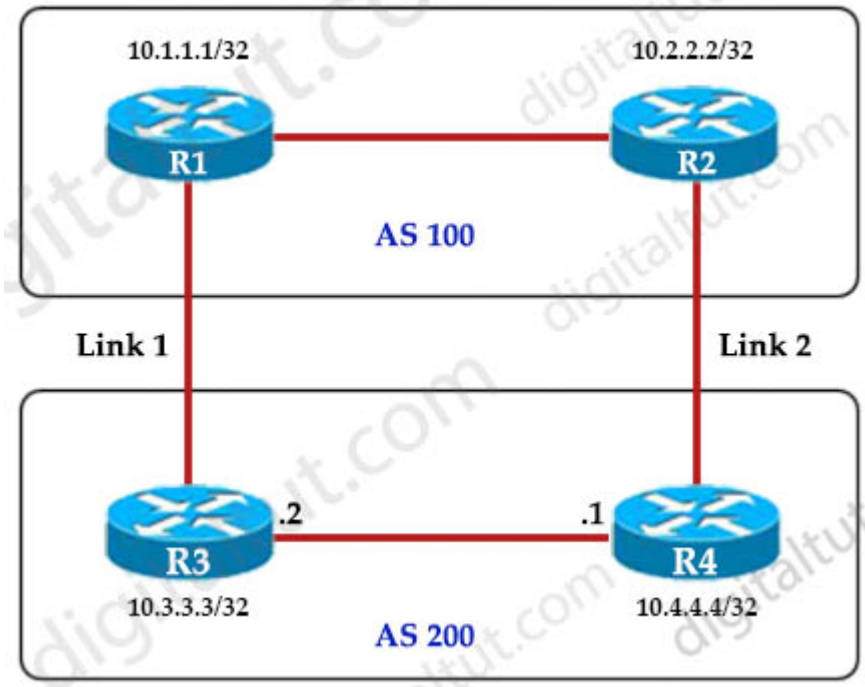
A. control-plane node
B. Identity Service Engine
C. RADIUS server
D. edge node

Answer: B

Question 2

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.

(Reference: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800c95bb.shtml#localpref)

Question 3

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

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

Answer: C

Explanation

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

Question 4

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

A.
```
class-map match-all CoPP_SSH
match access-group name CoPP_SSH
!
policy-map CoPP_SSH
class CoPP_SSH
police cir 100000
exceed-action drop
!
!
!
interface GigabitEthernet0/1
ip address 209.165.200.225 255.255.255.0
ip access-group 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
!
```

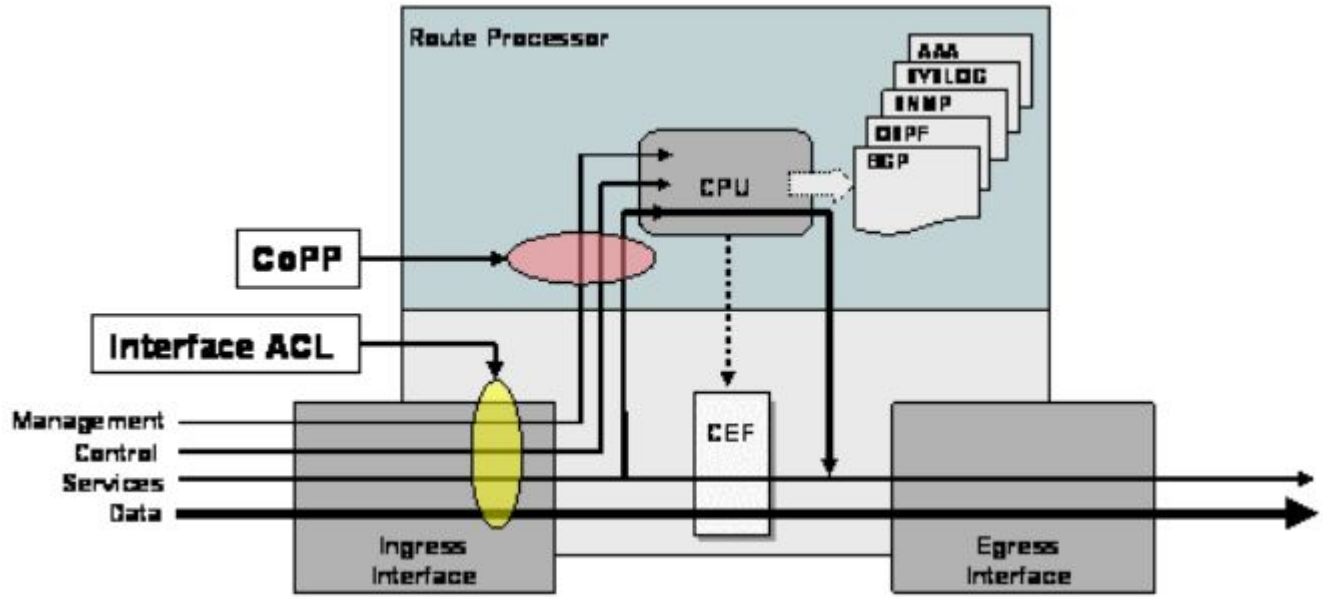
D.

```
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

Explanation

CoPP protects the route processor on network devices by treating route processor resources as a separate entity with its own ingress interface (and in some implementations, egress also). CoPP is used to police traffic that is destined to the route processor of the router such as:
+ Routing protocols like OSPF, EIGRP, or BGP.
+ Gateway redundancy protocols like HSRP, VRRP, or GLBP.
+ Network management protocols like telnet, SSH, SNMP, or RADIUS.



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

Question 5

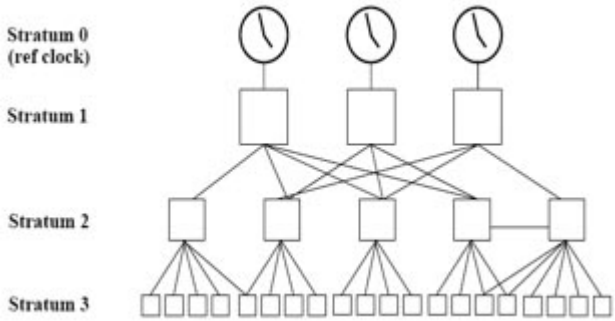
What NTP stratum level is a server that is connected directly to an authoritative time source?

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

Answer: B

Explanation

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



A stratum 2 server is connected to the stratum 1 server; then a stratum 3 server is connected to the stratum 2 server and so on. A stratum 2 server gets its time via NTP packet requests from a stratum 1 server. A stratum 3 server gets its time via NTP packet requests from a stratum-2 server… A stratum server may also peer with other

stratum servers at the same level to provide more stable and robust time for all devices in the peer group (for example a stratum 2 server can peer with other stratum 2 servers).

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

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

Question 6

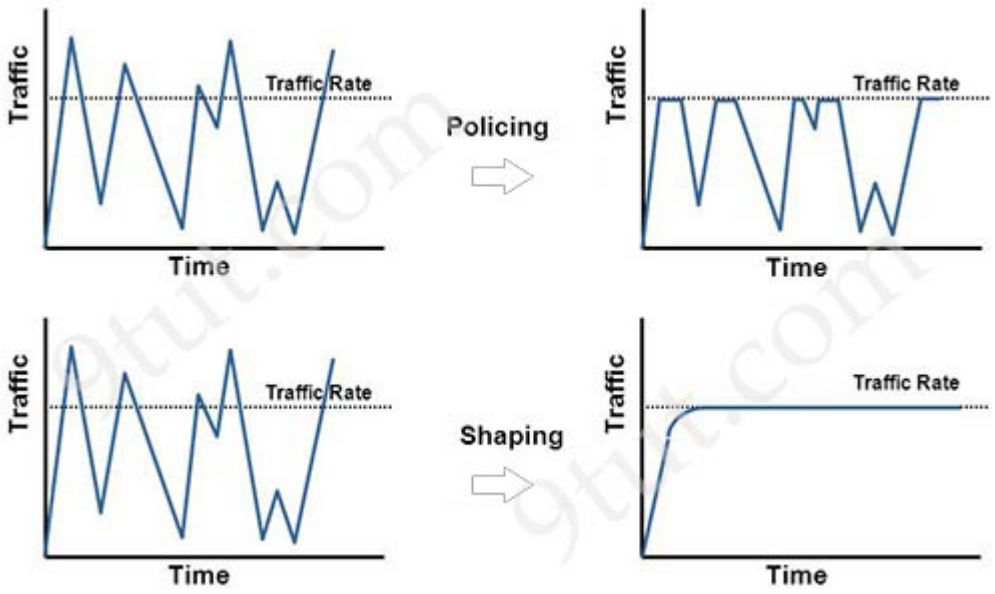
How does QoS traffic shaping alleviate network congestion?

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 7

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: C E

Explanation

Traffic policing propagates bursts. When the traffic rate reaches the configured maximum rate (or committed information rate), excess traffic is dropped (or remarked). The result is an output rate that appears as a saw-tooth with crests and troughs.

Unlike traffic shaping, traffic policing does not cause delay.

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

Also according to this Cisco link, “policing traffic as close to the source as possible”.

Question 8

What mechanism does PIM use to forward multicast traffic?

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

Answer: A

Explanation

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

PIM Sparse Mode (PIM-SM) uses a pull model to deliver multicast traffic. Only network segments with active receivers that have explicitly requested the data receive the traffic. PIM-SM distributes information about active sources by forwarding data packets on the shared tree. Because PIM-SM uses shared trees (at least initially), it requires the use of an RP. The RP must be administratively configured in the network.

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

Reference: Selecting MPLS VPN Services Book, page 193

Question 9

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

A. TLOC
B. RLOC
C. DNS

D. VTEP
E. EID

Answer: B E

Explanation

Locator ID Separation Protocol (LISP) is a network architecture and protocol that implements the use of two namespaces instead of a single IP address:
+ Endpoint identifiers (EIDs)—assigned to end hosts.
+ Routing locators (RLOCs)—assigned to devices (primarily routers) that make up the global routing system.

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

Question 10

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

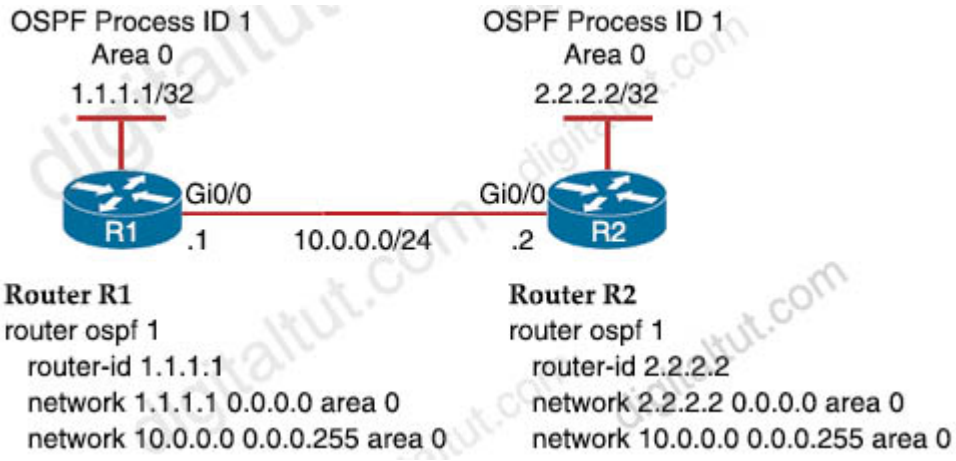
Answer: A

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 11

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 12

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: B C

Explanation

Broadcast radiation is the accumulation of broadcast and multicast traffic on a computer network. Extreme amounts of broadcast traffic constitute a broadcast storm.

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

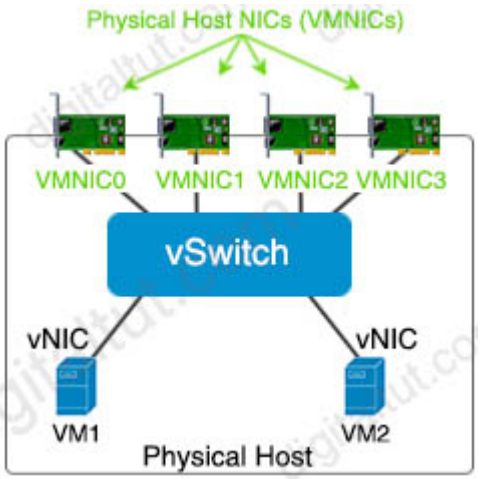
Also if virtual machines communicate via broadcast too much, broadcast radiation may occur.

Another reason for broadcast radiation is using a trunk (to extend VLANs) from the network switch to the physical server.

Note about the structure of virtualization in a hypervisor:

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

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



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

Question 13

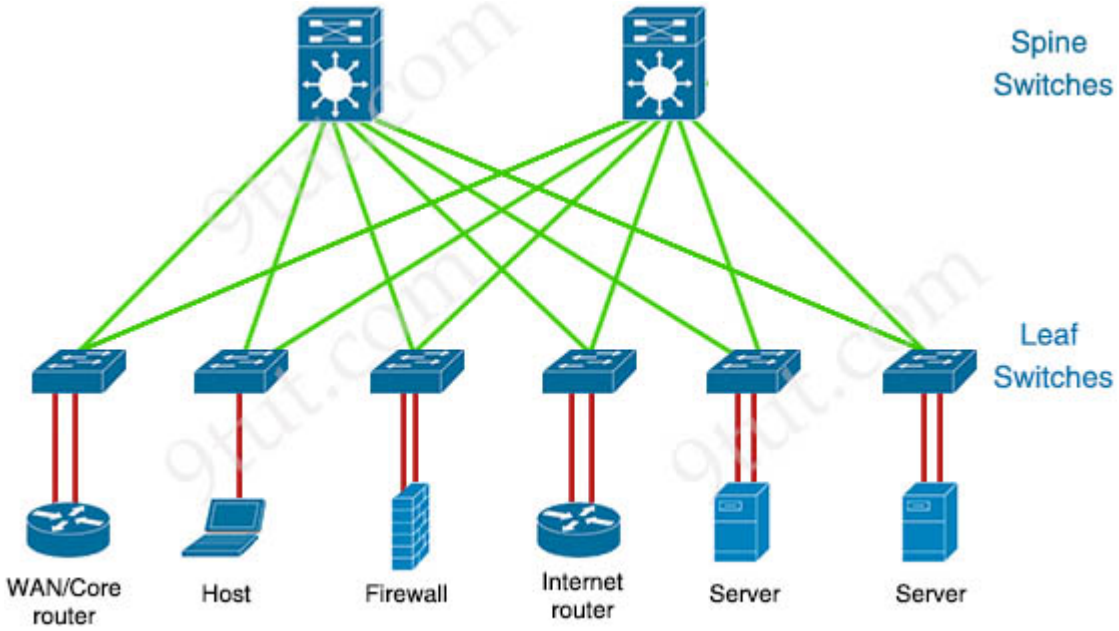
A company plans to implement intent-based networking in its campus infrastructure. Which design facilities a migrate from a traditional campus design to a programmer fabric designer?

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

Answer: C

Explanation

Intent-based Networking (IBN) transforms a hardware-centric, manual network into a controller-led network that captures business intent and translates it into policies that can be automated and applied consistently across the network. The goal is for the network to continuously monitor and adjust network performance to help assure desired business outcomes. IBN builds on software-defined networking (SDN). SDN usually uses spine-leaf architecture, which is typically deployed as two layers: spines (such as an aggregation layer), and leaves (such as an access layer).



Question 14

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

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

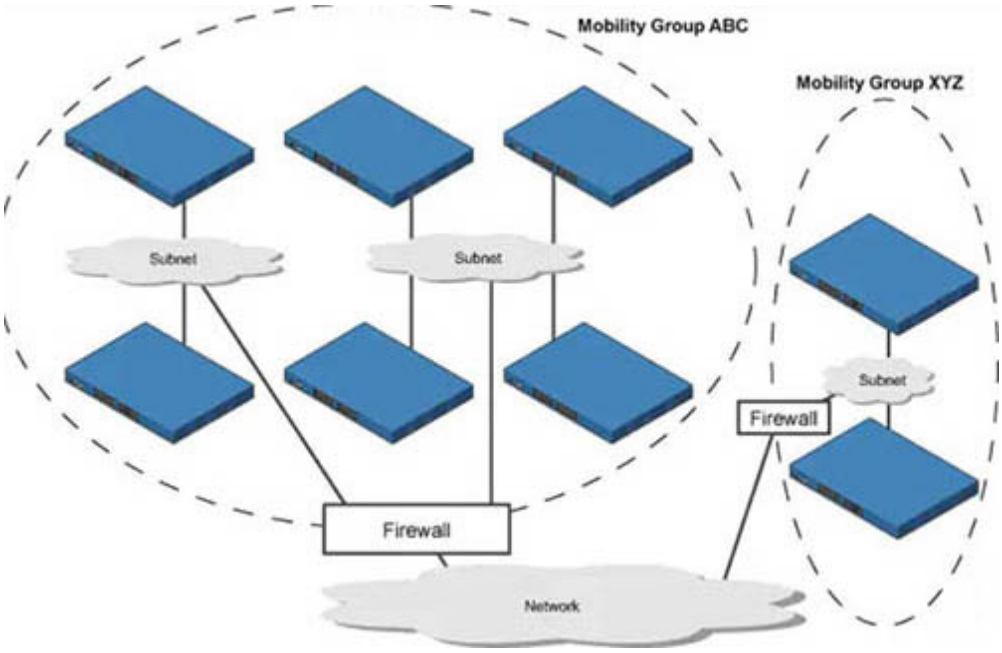
A prerequisite for configuring Mobility Groups is “All controllers must be configured with the same virtual interface IP address”. If all the controllers within a mobility group are not using the same virtual interface, inter-controller roaming may appear to work, but the handoff does not complete, **and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

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

Answer A is not correct because when the client moves to a different mobility group (with different mobility group name), that client would be connected (provided that the new connected controller had information about this client in its mobility list already) or drop (if the new connected controller have not had information about this client in its mobility list). For more information please read the note below.

Note:

A mobility group is a set of controllers, identified by the same mobility group name, that defines the realm of seamless roaming for wireless clients. By creating a mobility group, you can enable multiple controllers in a network to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers in the same mobility group can share the context and state of client devices as well as their list of access points so that they do not consider each other's access points as rogue devices.



Let's take an example:

The controllers in the ABC mobility group share access point and client information with each other. The controllers in the ABC mobility group do not share the access point or client information with the XYZ controllers, which are in a different mobility group. Therefore if a client from ABC mobility group moves to XYZ mobility group, **and the new connected controller does not have information about this client in its mobility list,** that client will be dropped.

Note: Clients may roam between access points in different mobility groups if the controllers are included in each other's mobility lists.

Question 15

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 16

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 17

A network administrator is preparing a Python script to configure a Cisco IOS XE-based device on the network. The administrator is worried that colleagues will make changes to the device while the script is running. Which operation of the client manager in prevent colleague making changes to the device while the script is running?

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

Answer: B

Explanation

The example below shows the usage of lock command:

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

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

Question 18

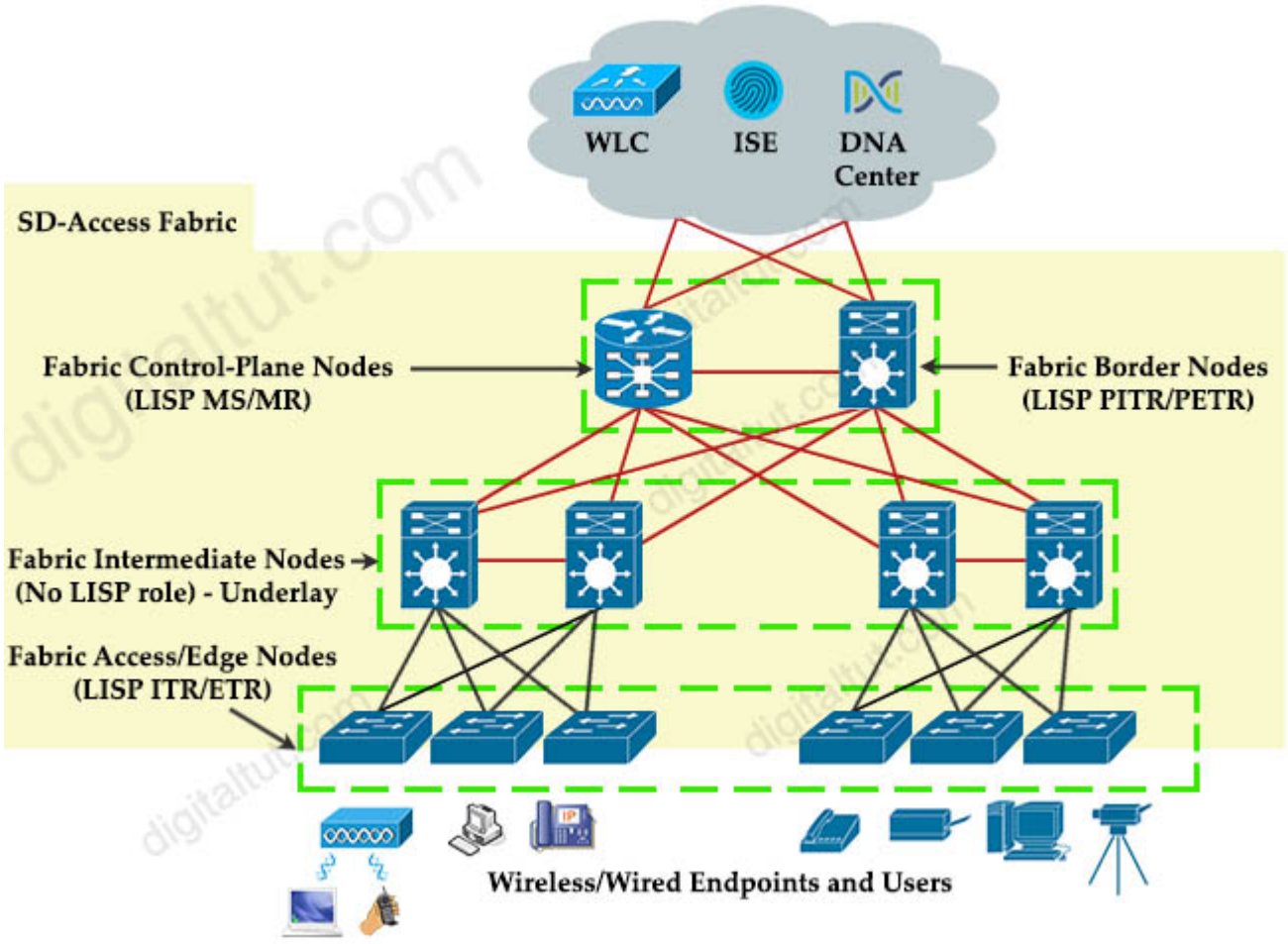
What are two device roles in Cisco SD-Access fabric? (Choose two)

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

Answer: C E

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.



Reference: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide

Question 19

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:

+ accepts LISP encapsulated map requests: LISP map resolver
+ learns of EID prefix mapping entries from an ETR: LISP map server

+ receives traffic from LISP sites and sends it to non-LISP sites: LISP proxy ETR
+ receives packets from site-facing interfaces: LISP ITR

Explanation

ITR is the function that maps the destination EID to a destination RLOC and then encapsulates the original packet with an additional header that has the source IP address of the ITR RLOC and the destination IP address of the RLOC of an Egress Tunnel Router (ETR). After the encapsulation, the original packet become a LISP packet.

ETR is the function that receives LISP encapsulated packets, decapsulates them and forwards to its local EIDs. This function also requires EID-to-RLOC mappings so we need to point out an "map-server" IP address and the key (password) for authentication.

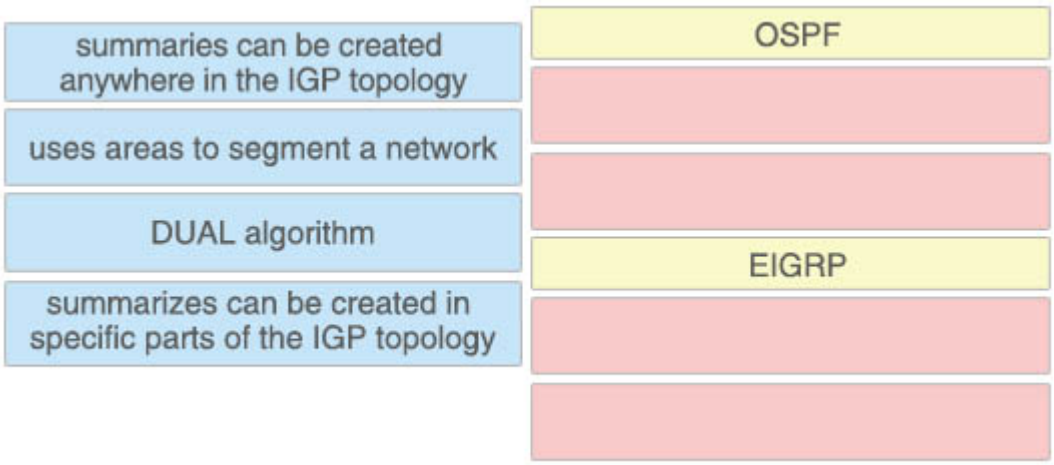
A LISP **proxy ETR** (PETR) implements ETR functions on behalf of non-LISP sites. A PETR is typically used when a LISP site needs to send traffic to non-LISP sites but the LISP site is connected through a service provider that does not accept nonroutable EIDs as packet sources. PETRs act just like ETRs but for EIDs that send traffic to destinations at non-LISP sites.

Map Server (MS) processes the registration of authentication keys and EID-to-RLOC mappings. ETRs sends periodic Map-Register messages to all its configured Map Servers.

Map Resolver (MR): a LISP component which accepts LISP Encapsulated Map Requests, typically from an ITR, quickly determines whether or not the destination IP address is part of the EID namespace

Question 20

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



Answer:

OSPF:
+ uses areas to segment a network
+ summarizes can be created in specific parts of the IGP topology

EIGRP:
+ summaries can be created anywhere in the IGP topology
+ DUAL algorithm

Explanation

Unlike OSPF where we can summarize only on ABR or ASBR, in EIGRP we can summarize anywhere.

Manual summarization can be applied anywhere in EIGRP domain, on every router, on every interface via the **ip summary-address eigrp** *as-number address mask* [*administrative-distance*] command (for example: ip summary-address eigrp 1 192.168.16.0 255.255.248.0). Summary route will exist in routing table as long as at least one more specific route will exist. If the last specific route will disappear, summary route also will fade out. The metric used by EIGRP manual summary route is the minimum metric of the specific routes.

Question 21

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 22

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: B D

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 23

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

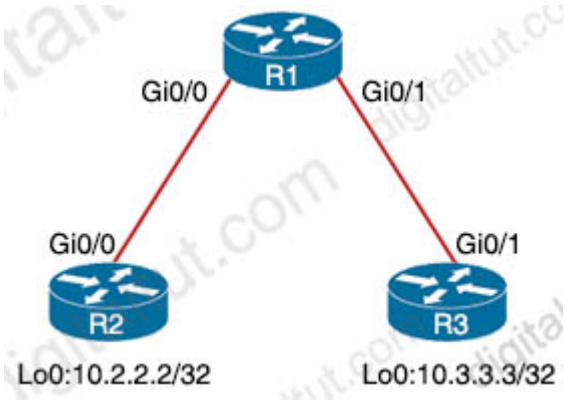
Answer: D

Explanation

An lightweight AP (LAP) operates in one of six different modes:
+ **Local mode** (default mode): measures noise floor and interference, and scans for intrusion detection (IDS) events every 180 seconds on unused channels
+ **FlexConnect**, formerly known as **Hybrid Remote Edge AP (H-REAP)**, mode: allows data traffic to be switched locally and not go back to the controller. The FlexConnect AP can perform standalone client authentication and switch VLAN traffic locally even when it's disconnected to the WLC (Local Switched). FlexConnect AP can also tunnel (via CAPWAP) both user wireless data and control traffic to a centralized WLC (Central Switched).
+ **Monitor mode**: does not handle data traffic between clients and the infrastructure. It acts like a sensor for location-based services (LBS), rogue AP detection, and IDS
+ **Rogue detector mode**: monitor for rogue APs. It does not handle data at all.
+ **Sniffer mode**: run as a sniffer and captures and forwards all the packets on a particular channel to a remote machine where you can use protocol analysis tool (Wireshark, Airopeek, etc) to review the packets and diagnose issues. Strictly used for troubleshooting purposes.
+ **Bridge mode:** bridge together the WLAN and the wired infrastructure together.

Question 24

Refer to the exhibit.



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

A.
R3(config)#time-range WEEKEND
R3(config-time-range)#periodic Saturday Sunday 00:00 to 23:59

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

R3(config)#interface Gi0/1
R3(config-if)#ip access-group 150 out

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

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

R1(config)#interface Gi0/1
R1(config-if)#ip access-group 150 in

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

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

R1(config)#interface Gi0/1
R1(config-if)#ip access-group 150 in

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

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

R3(config)#interface Gi0/1
R3(config-if)#ip access-group 150 out

Answer: C

Explanation

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

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

Question 25

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

A. Command Runner
B. Template Editor

C. Application Policies
D. Authentication Template

Answer: B

Explanation

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

Reference: 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 26

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: B

Explanation

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

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

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

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

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01100.html

In three types of client roaming above, only with Inter-Subnet Roaming the controllers are in different subnets.

Question 27

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

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

Answer: D

Question 28

Refer to the exhibit.

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

What is the result when a technician adds the **monitor session 1 destination remote vlan 233** command?

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

Answer: A

Question 29

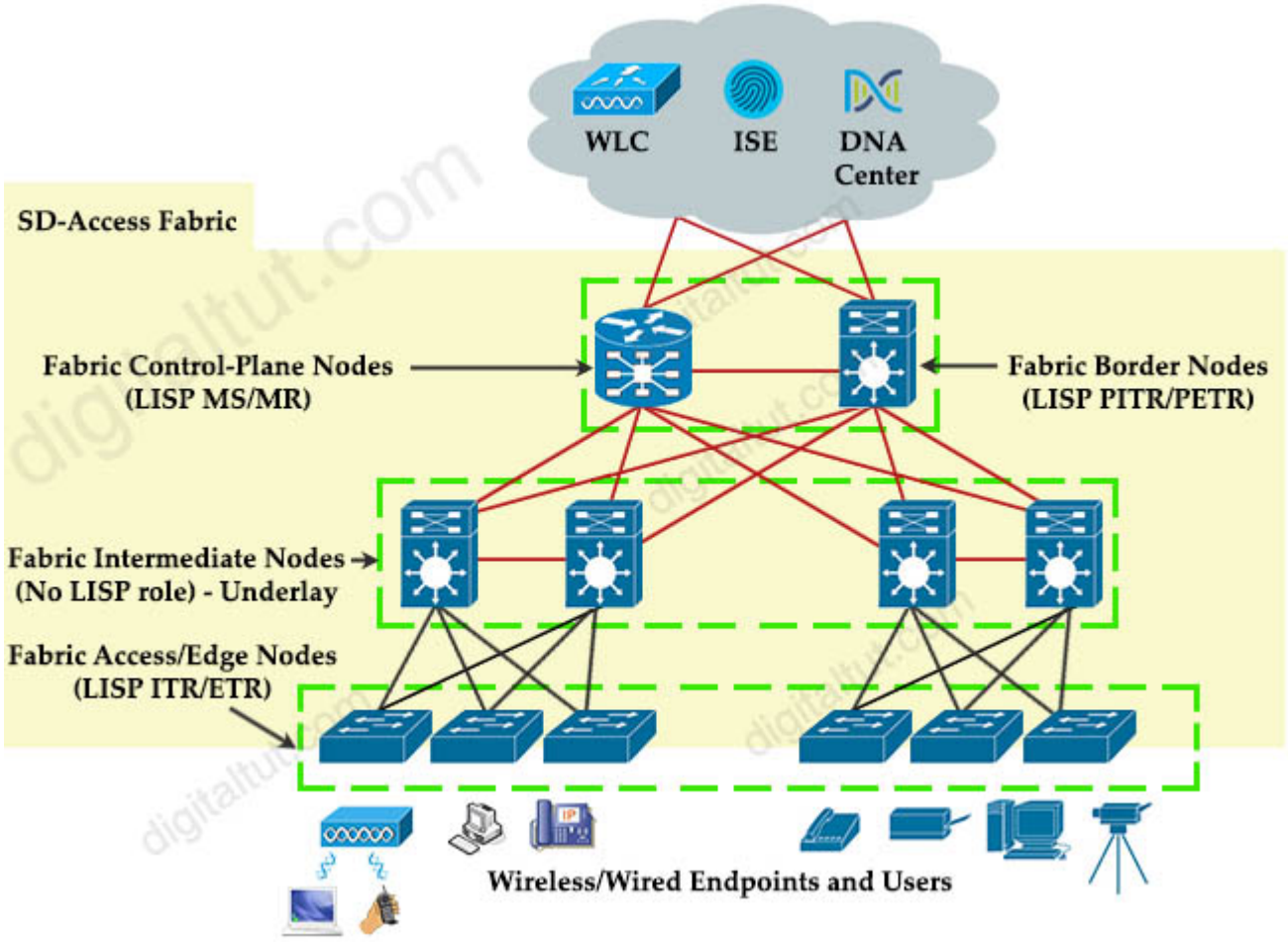
In an SD-Access solution what is the role of a fabric edge node?

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

Answer: B

Explanation

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



Question 30

Refer to the exhibit.

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

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

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

Answer: C

Explanation

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

Question 31

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

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

Answer: B

Explanation

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

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

* NetFlow and the Lancope StealthWatch System
– Broad visibility
– **User and flow context analysis**
– Network behavior and anomaly detection
– Incident response and network forensics

* Cisco FirePOWER and FireSIGHT
– Real-time threat management
– Deeper contextual visibility for threats bypassing the perimeters
– URL control

* Advanced Malware Protection (AMP)
– Endpoint control with AMP for Endpoints
– Malware control with AMP for networks and content

* Content Security Appliances and Services
– Cisco Web Security Appliance (WSA) and Cloud Web Security (CWS)
– Dynamic threat control for web traffic
– Outbound URL analysis and data transfer controls
– Detection of suspicious web activity
– Cisco Email Security Appliance (ESA)
– Dynamic threat control for email traffic
– Detection of suspicious email activity

* Cisco Identity Services Engine (ISE)
– User and device identity integration with Lancope StealthWatch
– Remediation policy actions using pxGrid

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

Question 32

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

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

Answer: A

Explanation

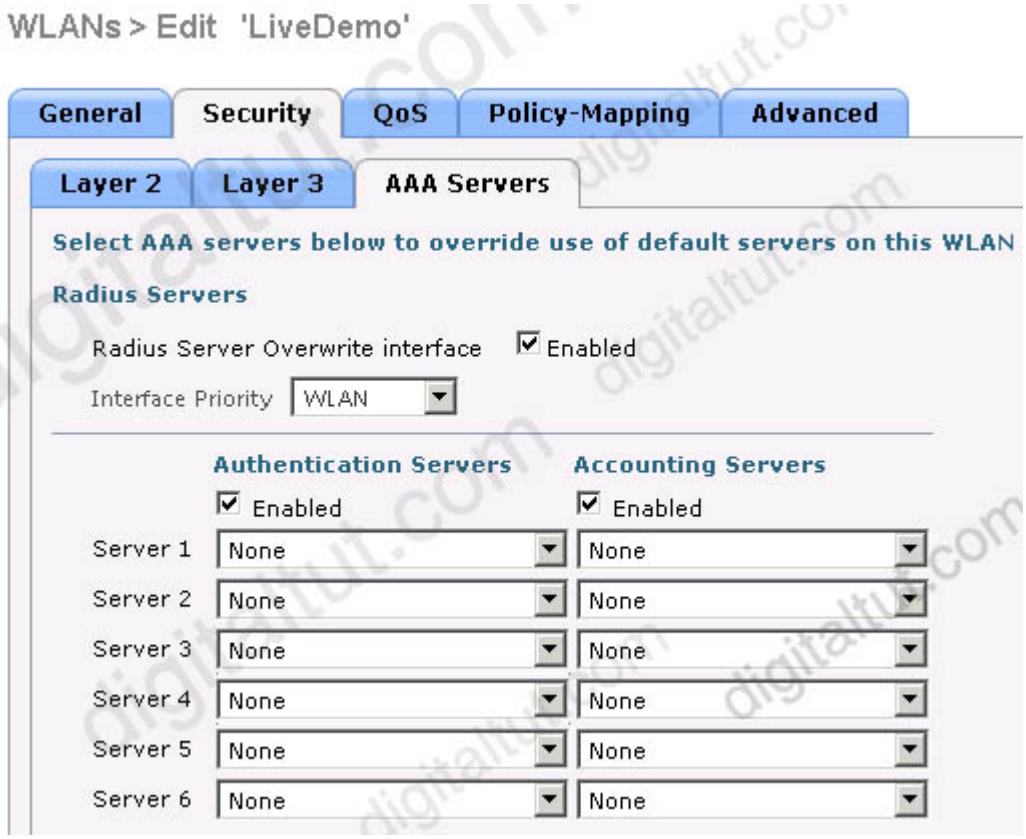
Ransomware are malicious software that locks up critical resources of the users. Ransomware uses well-established public/private key cryptography which leaves the only way of recovering the files being the payment of the ransom, or restoring files from backups.

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

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

Question 33

Refer to the exhibit.



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

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

Answer: A

Question 34

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 35

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

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

Answer: A

Explanation

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

Question 36

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 37

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

Explanation

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

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

Question 38

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

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

Answer: B

Explanation

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

Question 39

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 40

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

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

Answer: A

Explanation

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

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

Question 41

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

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

Answer: B

Explanation

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

Question 42

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

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

Answer: C

Explanation

The Cisco DNA Center open platform for intent-based networking provides 360-degree extensibility across multiple components, including:
+ **Intent-based APIs** leverage the controller to enable business and IT applications to deliver intent to the network and to reap network analytics and insights for IT and business innovation. These enable APIs that allow Cisco DNA Center to receive input from a variety of sources, both internal to IT and from line-of-business applications, related to application policy, provisioning, software image management, and assurance.
…

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

Question 43

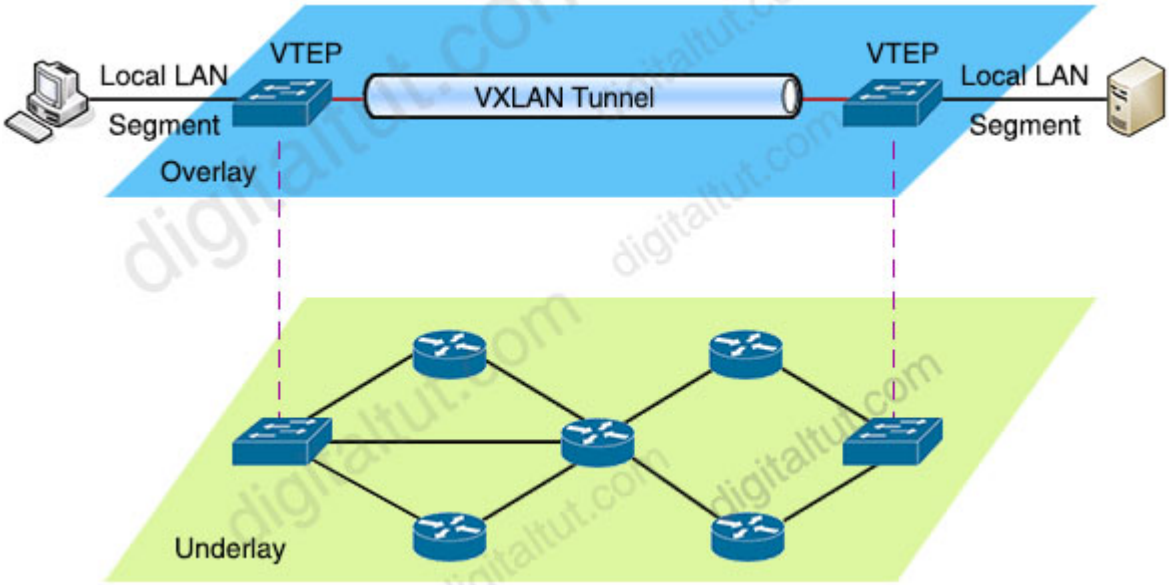
Which action is a function of VTEP in VXLAN?

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

Answer: C

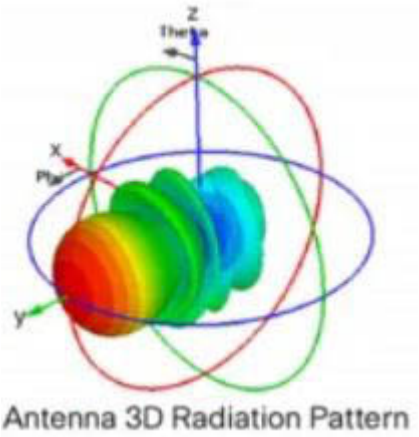
Explanation

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



Question 44

Which type of antenna does the radiation pattern represent?



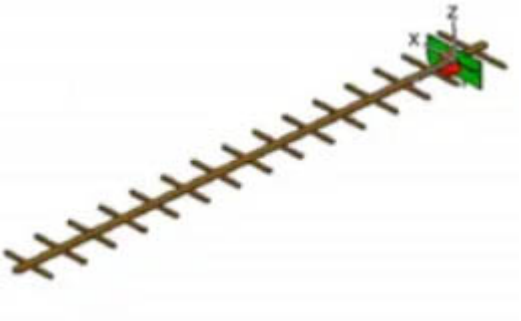
Antenna 3D Radiation Pattern

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

Answer: A

Explanation

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



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

========== This is the end of the update ==========

Comments

1. Ant
   June 23rd, 2020

   Thanks DigitalTut. The questions are 10.. there will be another update in the next few days, with other Q&A ? In according with rumors here, the new questions are 18 or plus.

   Thanks again !

2. Nhardz
   June 23rd, 2020