New ENCOR Questions

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?

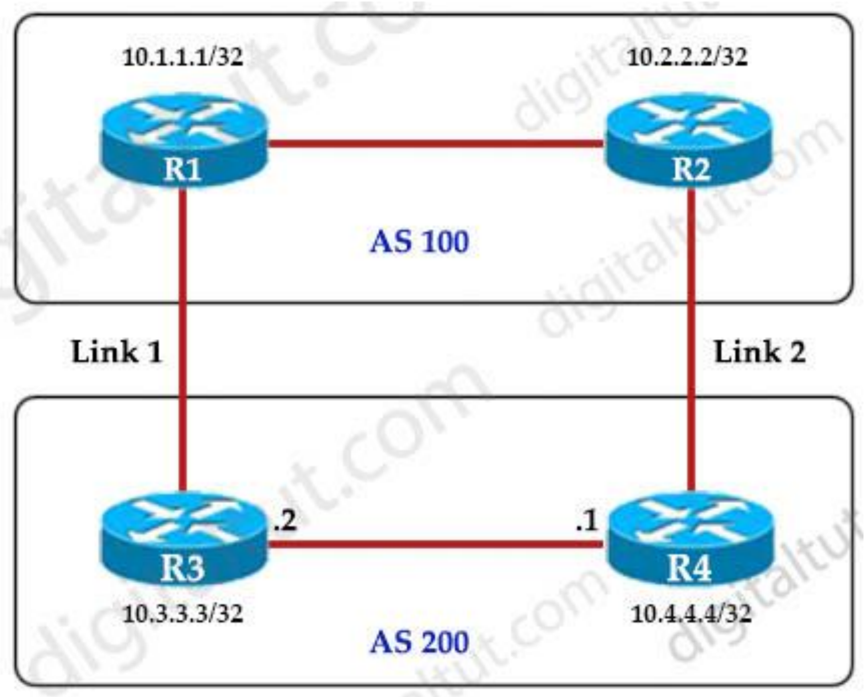
A. control-plane node
B. Identity Service Engine
C. RADIUS server
D. edge node

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
!
```

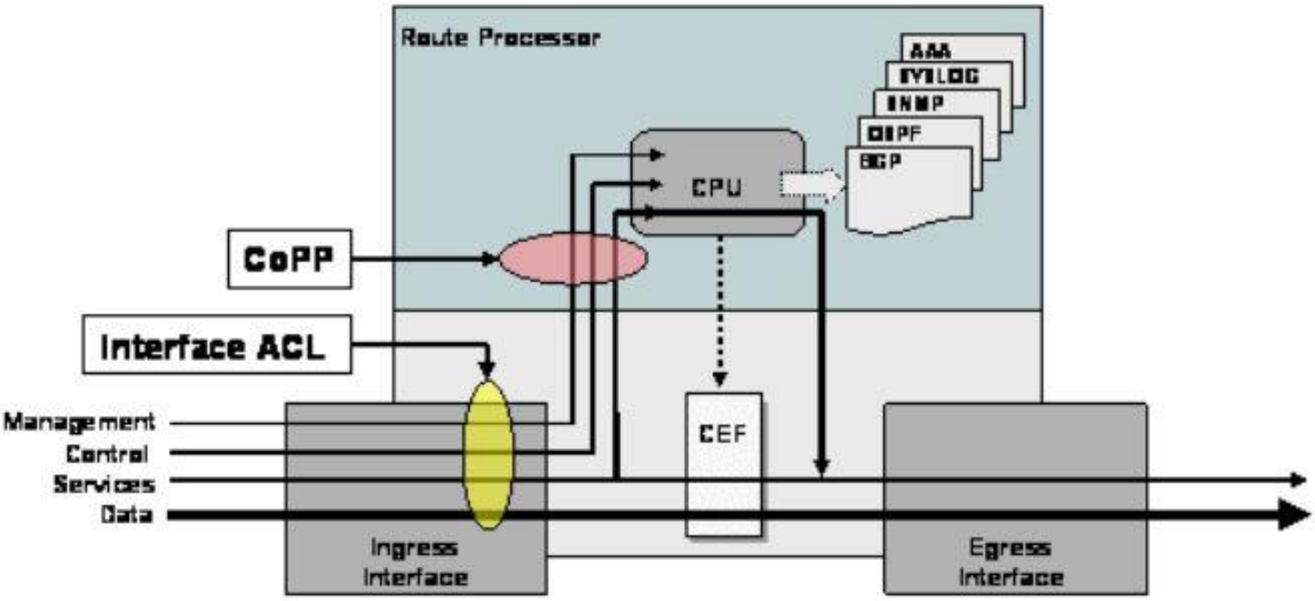
D.

```
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. But we cannot name the control-plane (like “transit”).

Question 5

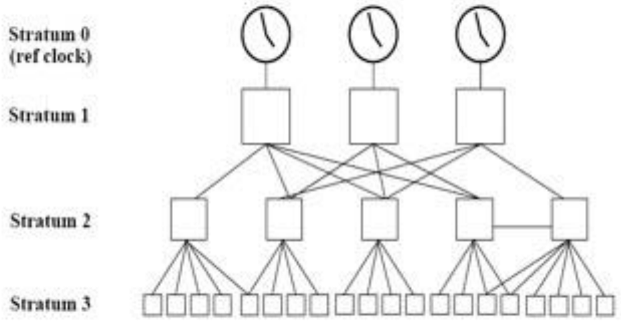
What NTP stratum level is a server that is connected directly to an authoritative time source?

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

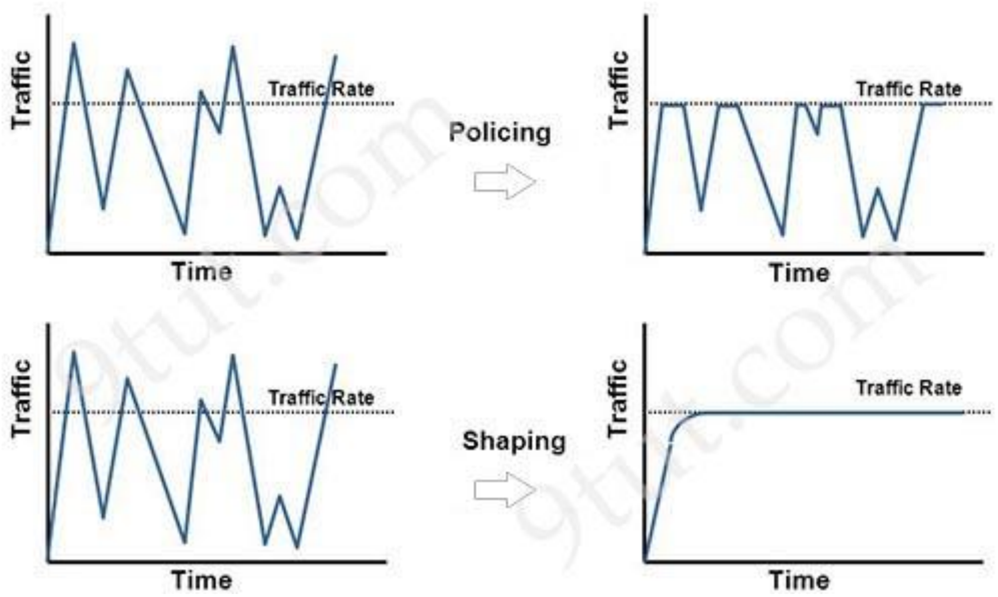
How does QoS traffic shaping alleviate network congestion?

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

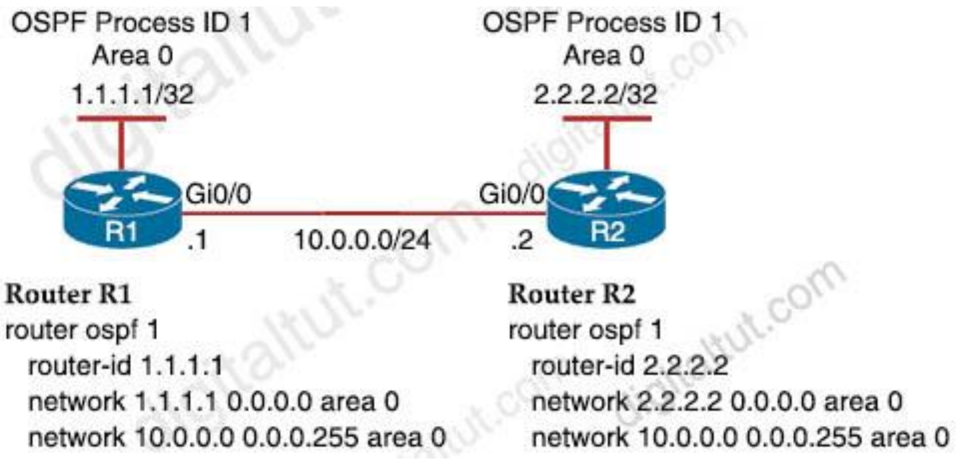
Answer: A

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.



Router R1

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

Router R2

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

A 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.

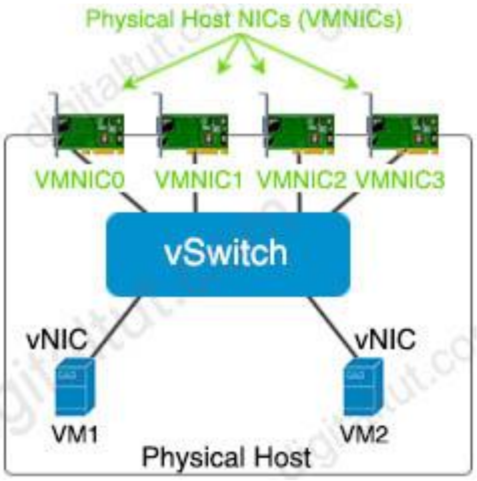
Another reason for broadcast radiation is using a trunk (to extend VLANs) from the network switch to the physical server.

——————————————————————————-

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

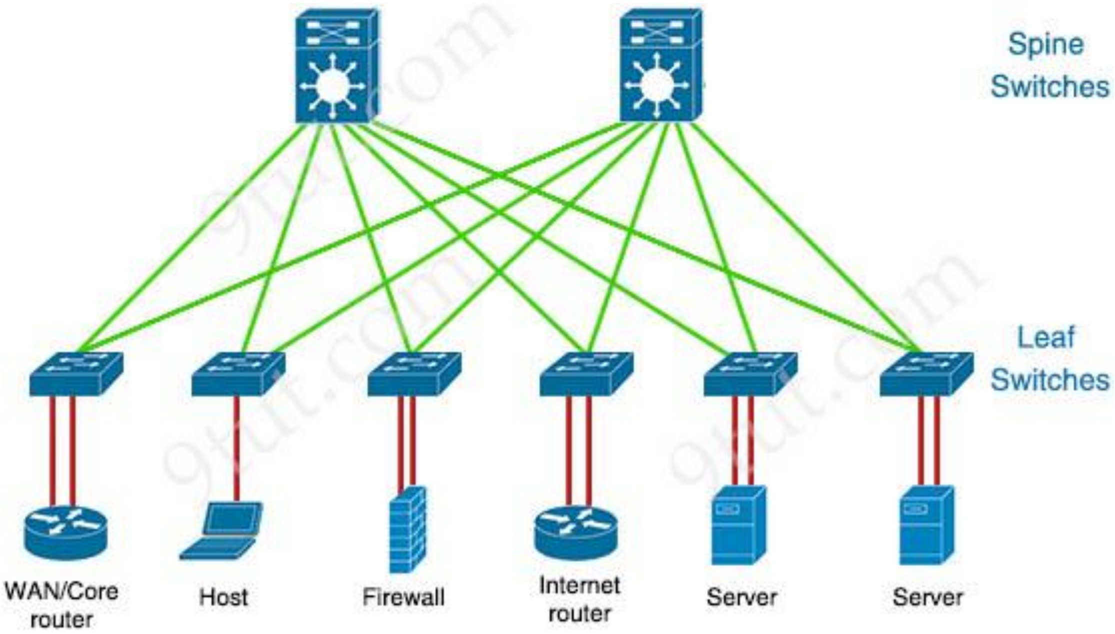
A company plans to implement intent-based networking in its campus infrastructure. Which design facilities a migrate from a traditional campus design to a programmer fabric designer?

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

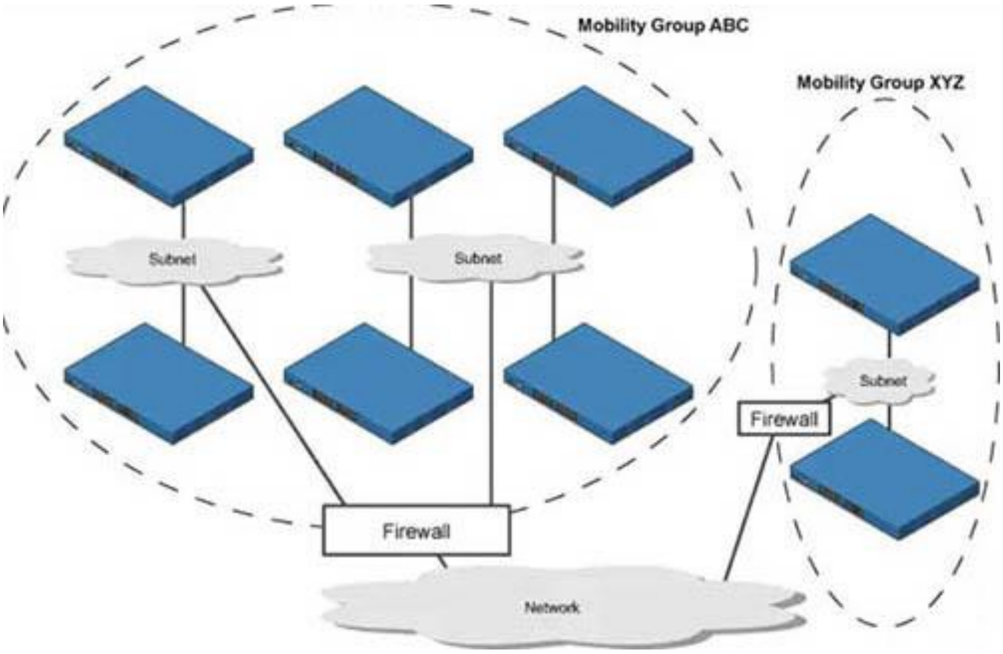
A prerequisite for configuring Mobility Groups is "All controllers must be configured with the same virtual interface IP address". If all the controllers within a mobility group are not using the same virtual interface, inter-controller roaming may appear to work, but the handoff does not complete, **and 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

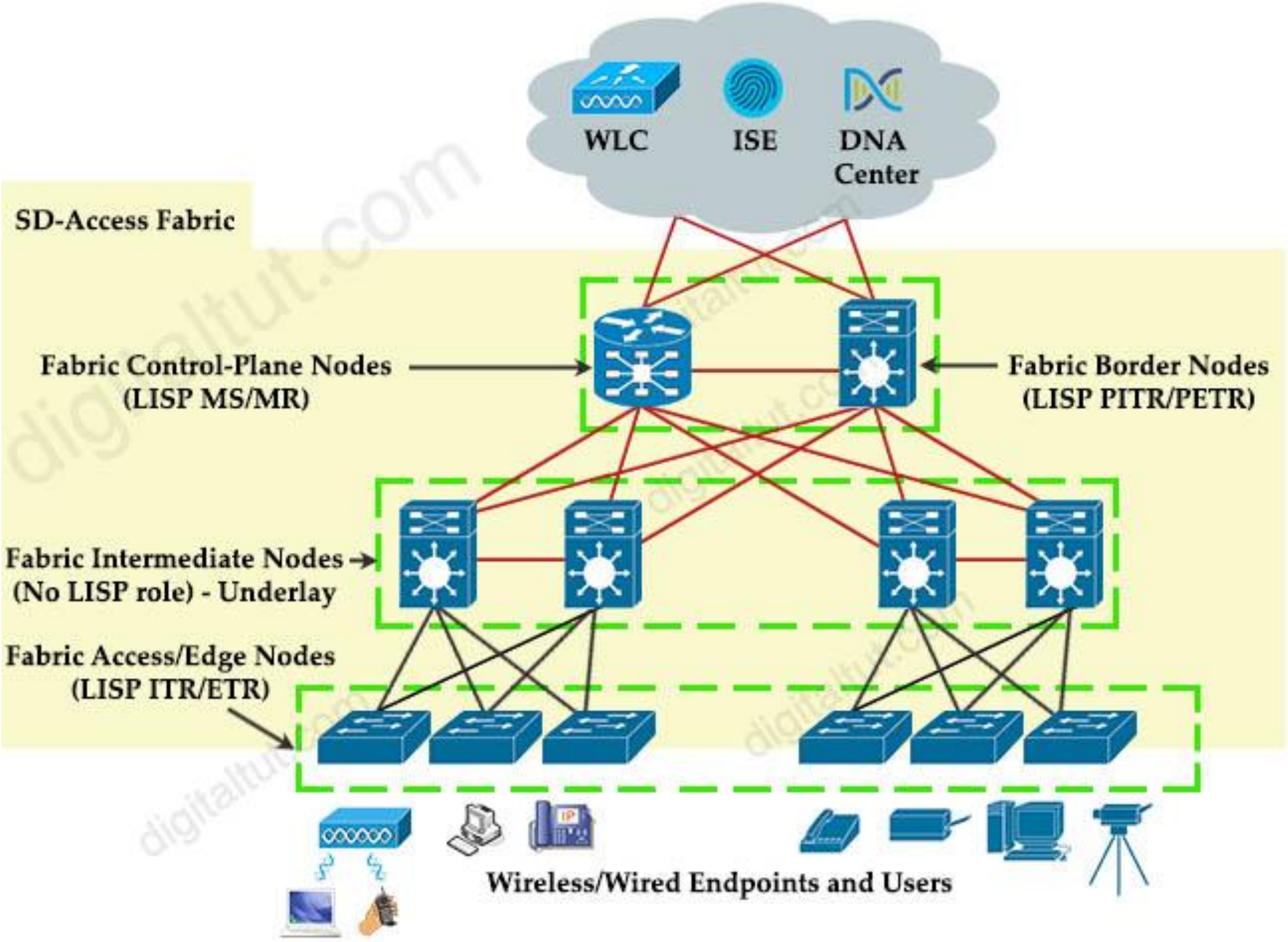
What are two device roles in Cisco SD-Access fabric? (Choose two)

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

Answer: C E

Explanation

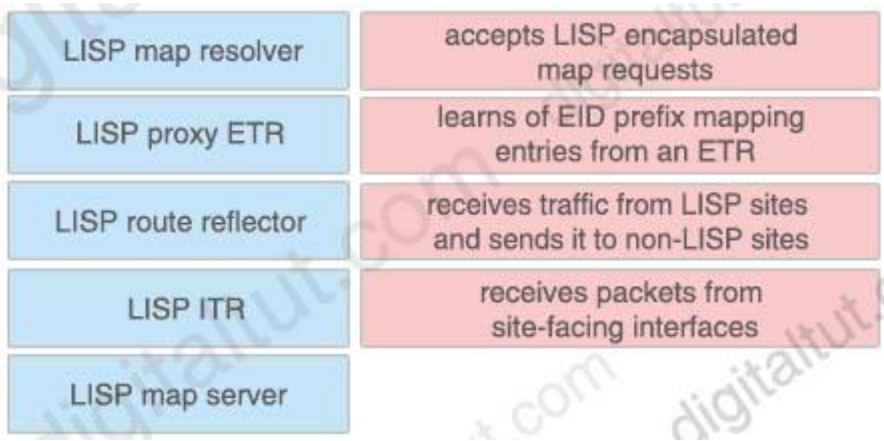
There are five basic device roles in the fabric overlay:
+ Control plane node: This node contains the settings, protocols, and mapping tables to provide the endpoint-to-location (EID-to-RLOC) mapping system for the fabric overlay.
+ **Fabric border node**: This fabric device (for example, core layer 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.


WLC
ISE
DNA Center
SD-Access Fabric
Fabric Control-Plane Nodes (LISP MS/MR)
Fabric Border Nodes (LISP PITR/PETR)
Fabric Intermediate Nodes (No LISP role) - Underlay
Fabric Access/Edge Nodes (LISP ITR/ETR)
IP
Wireless/Wired Endpoints and Users

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.

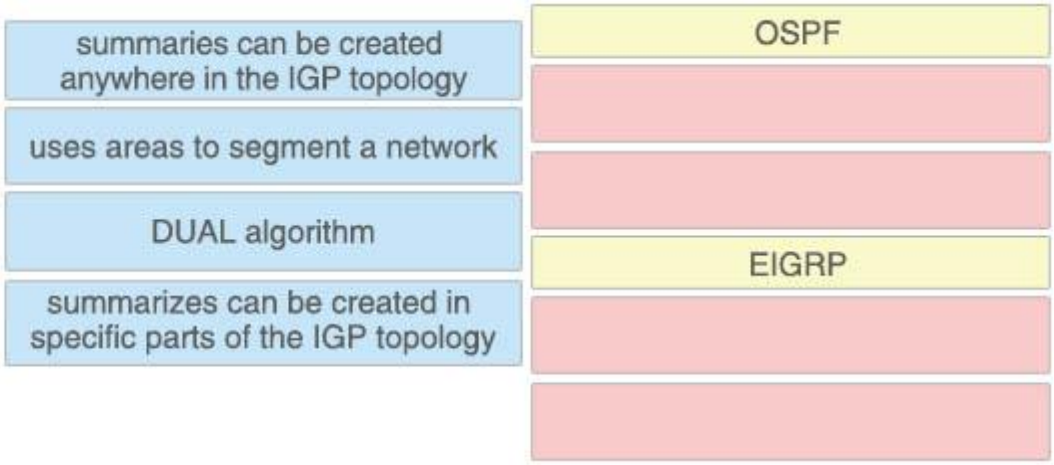
A LISP **proxy ETR** (PETR) implements ETR functions on behalf of non-LISP sites. A PETR is typically used when a LISP site needs to send traffic to non-LISP sites but the LISP site is connected through a service provider that does not accept nonroutable EIDs as packet sources. PETRs act just like ETRs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



summaries can be created anywhere in the IGP topology

uses areas to segment a network

DUAL algorithm

summarizes can be created in specific parts of the IGP topology

OSPF

EIGRP

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

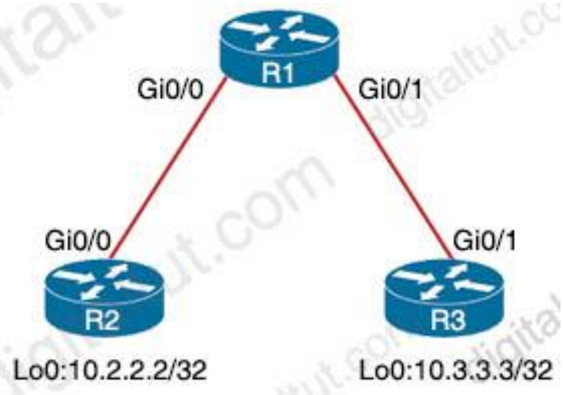
Explanation

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: D

Explanation

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

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

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

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

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

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

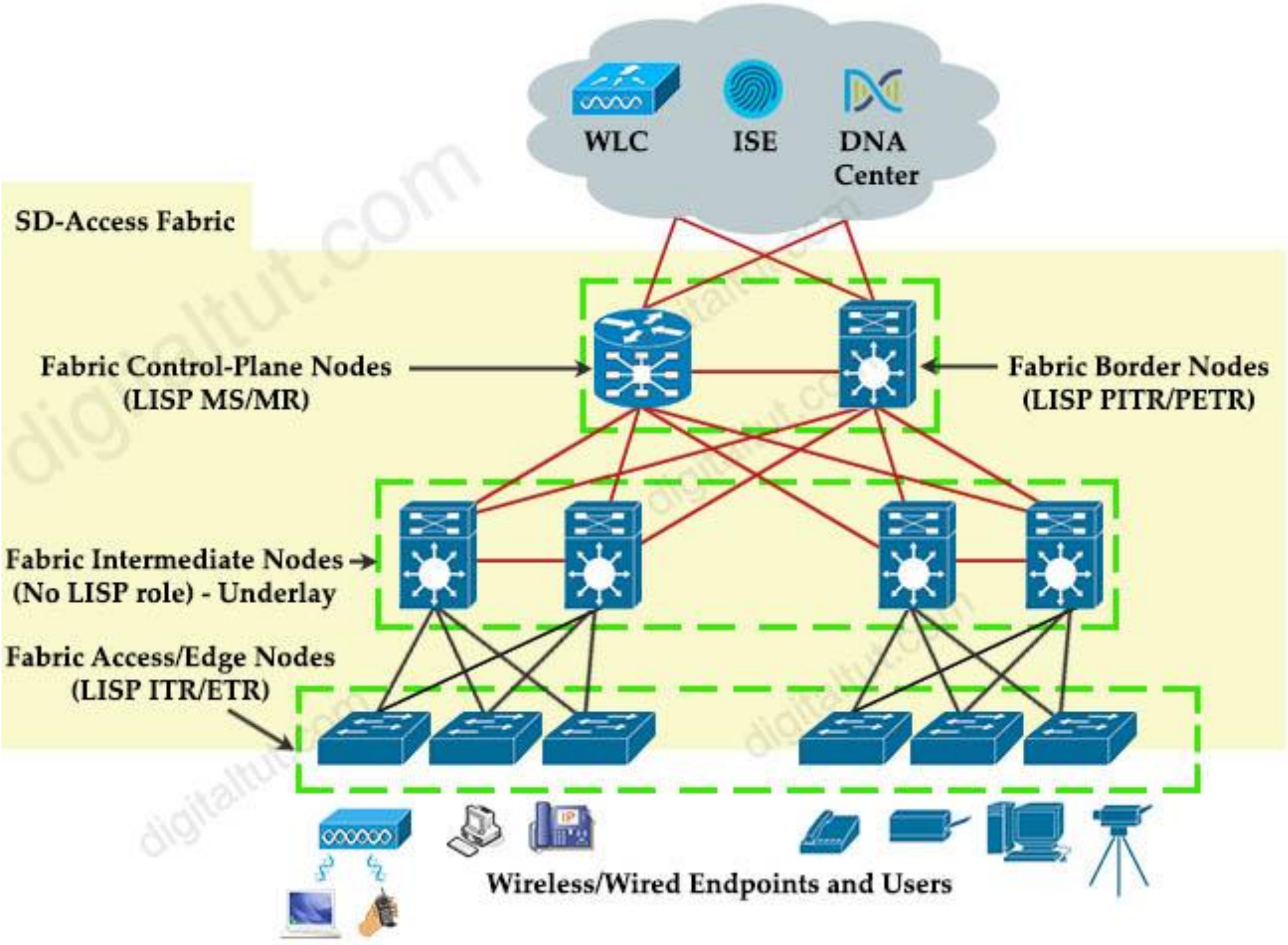
In an SD-Access solution what is the role of a fabric edge node?

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.



WLC
ISE
DNA Center
SD-Access Fabric
Fabric Control-Plane Nodes (LISP MS/MR)
Fabric Border Nodes (LISP PITR/PETR)
Fabric Intermediate Nodes (No LISP role) - Underlay
Fabric Access/Edge Nodes (LISP ITR/ETR)
Wireless/Wired Endpoints and Users

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

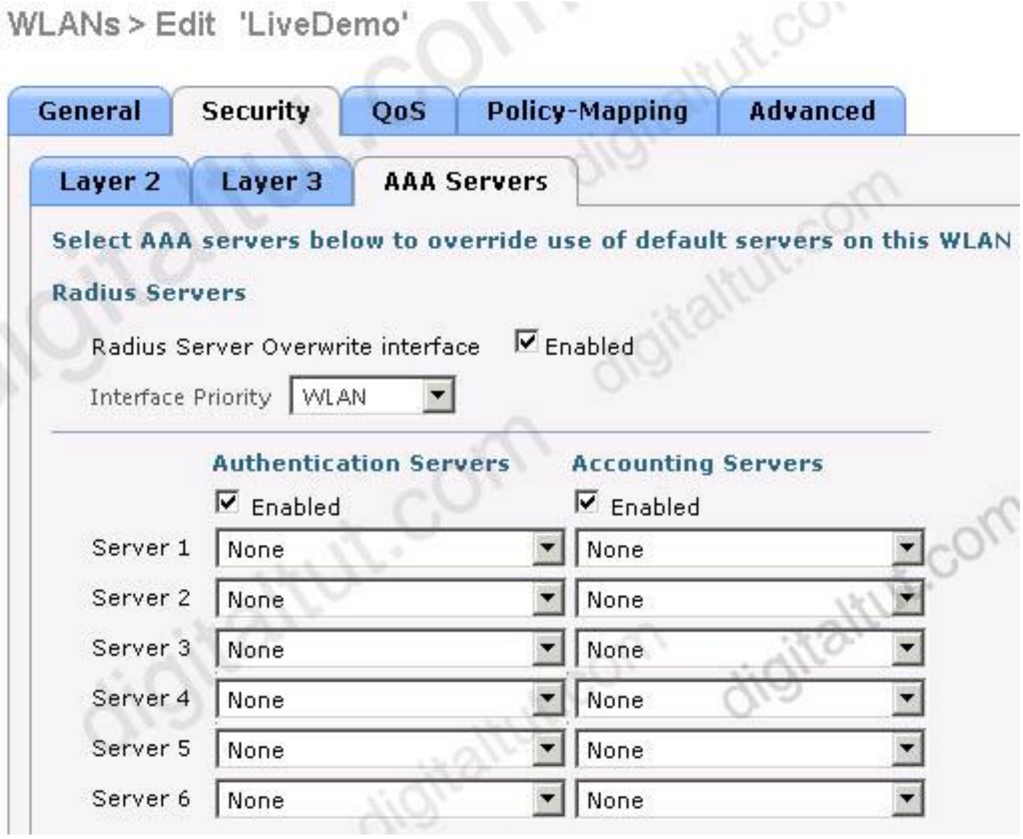
Ransomware are malicious software that locks up critical resources of the users. Ransomware uses well-established public/private key cryptography which leaves the only way of recovering the files being the payment of the ransom, or restoring files from backups.

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.



WLANs > Edit 'LiveDemo'

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

Radius Servers

Radius Server Overwrite interface ☑ Enabled

Interface Priority: WLAN

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

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

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

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

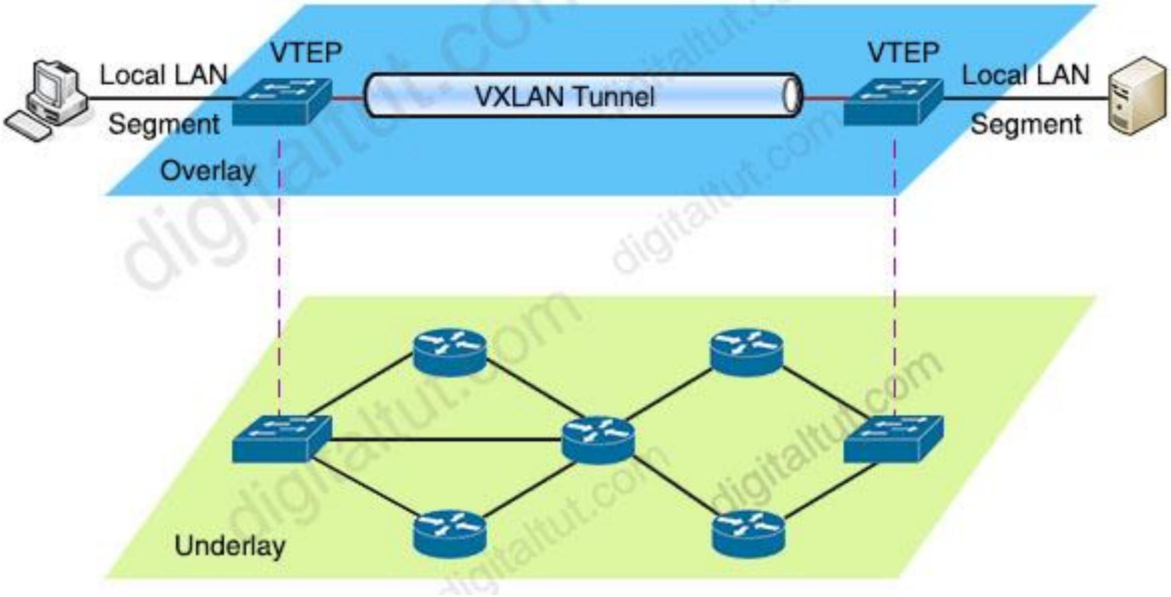
Which action is a function of VTEP in VXLAN?

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

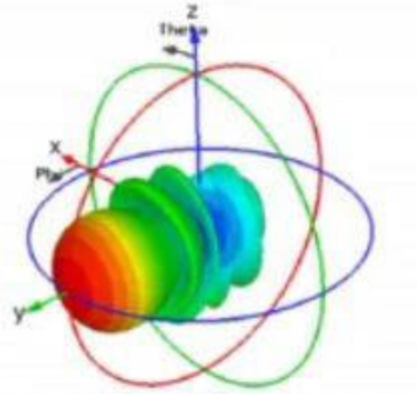
Explanation

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

Etherchannel Questions

https://www.digitaltut.com/etherchannel-questions

Question 1

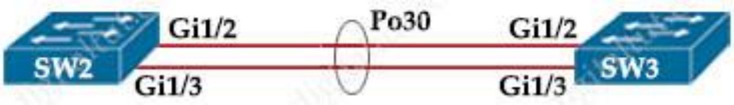
Which PAgP mode combination prevents an Etherchannel from forming?

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

Answer: A

Question 2

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



```
interface gi1/2
 channel-group 30 mode desirable
 port-channel load-balance src-ip

interface gi1/3
 channel-group 30 mode desirable
 port-channel load-balance src-ip

interface PortChannel 30
 switchport mode trunk
 switchport encapsulation dot1q
 switchport trunk allowed vlan 10-100
```

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

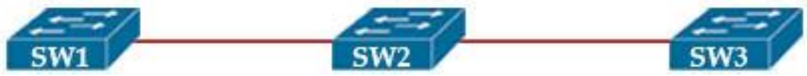
Answer: A

Trunking Questions

https://www.digitaltut.com/trunking-questions

Question 1

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

Question 2

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                 : MyDomain.com
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xCC 0x77 0x02 0x40 0x93 0xB5 0xC1 0xA2
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00

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


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

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

SD-WAN & SD-Access Solutions

https://www.digitaltut.com/sd-wan-sd-access-solutions

Question 1

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

Question 2

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

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

Answer: B

Question 3

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

Question 4

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

Question 5

Which statement about a fabric access point is true?

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

Answer: C

Question 6

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

Question 7

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

Question 8

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

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

Answer: D

QoS Questions

https://www.digitaltut.com/qos-questions

Question 1

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 2

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

Question 3

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

Question 4

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

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

Answer: A

Switching Mechanism Questions

https://www.digitaltut.com/switching-mechanism-questions

Question 1

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

Question 2

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

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: D E

Question 3

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

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

Answer: D

Question 4

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

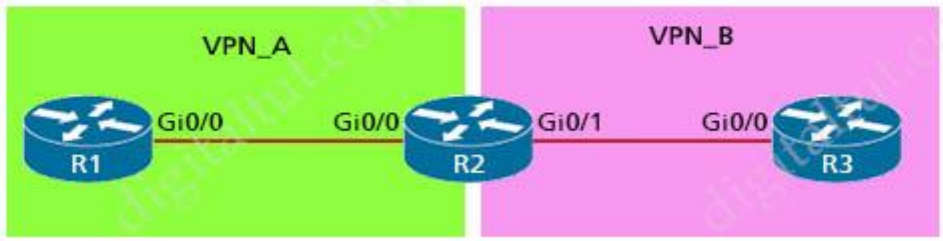
Answer: D

Virtualization Questions

https://www.digitaltut.com/virtualization-questions

Question 1

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



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

Answer: B

Question 2

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

Question 3

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: B E

Question 4

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

Question 5

What are two benefits 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: B D

Question 6

Which statement describes the IP and MAC allocation requirements for virtual machines on type 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

Question 7

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 8

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)

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

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: D E

LISP & VXLAN Questions

https://www.digitaltut.com/lisp-vxlan-questions

Question 1

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

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

Answer: A

Question 2

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

Question 3

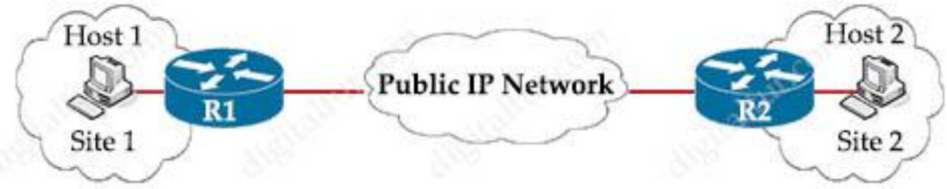
Into which two pieces of information does the LISP protocol split the device identity? (Choose two)

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

Answer: A B

Question 4

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 5

Which statement about VXLAN is true?

A. VXLAN uses TCP 35 the transport protocol over the physical data center 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

EIGRP & OSPF Questions

https://www.digitaltut.com/eigrp-ospf-questions

Question 1

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

Question 2

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

Question 3

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

Answer: C

Question 4

Which EIGRP feature allows the use of leak maps?

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

Answer: D

Question 5

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: A B

Question 6

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: A

Question 7

Which 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

Question 8

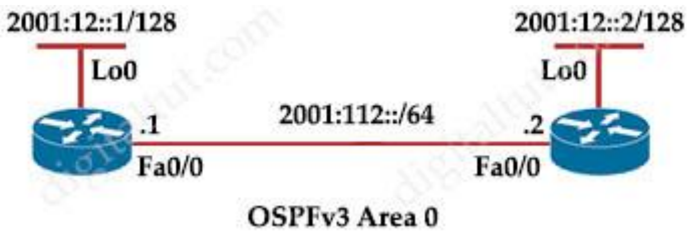
Which feature is supported by EIGRP but is not supported by OSPF?

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

Answer: C

Question 9

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

Question 10

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

BGP Questions

https://www.digitaltut.com/bgp-questions-7

Question 1

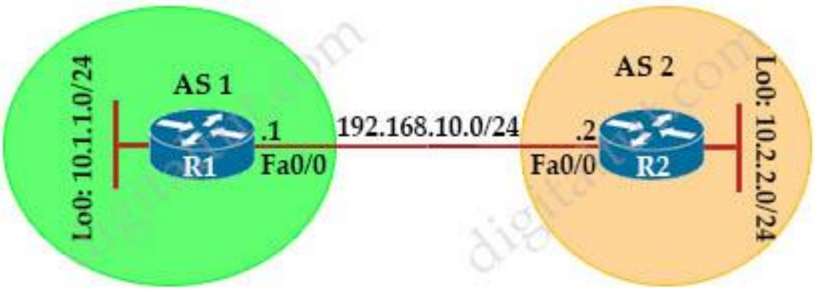
A local router shows an EBGP neighbor in the Active state. Which statement is true about the local router?

A. The local router has active prefix in the forwarding table firom 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

Question 2

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

Question 3

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

   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                        0 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

Question 4

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

Wireless Questions

https://www.digitaltut.com/wireless-questions

Question 1

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

Question 2

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: B D

Question 3

Which statement about Cisco EAP-FAST is true?

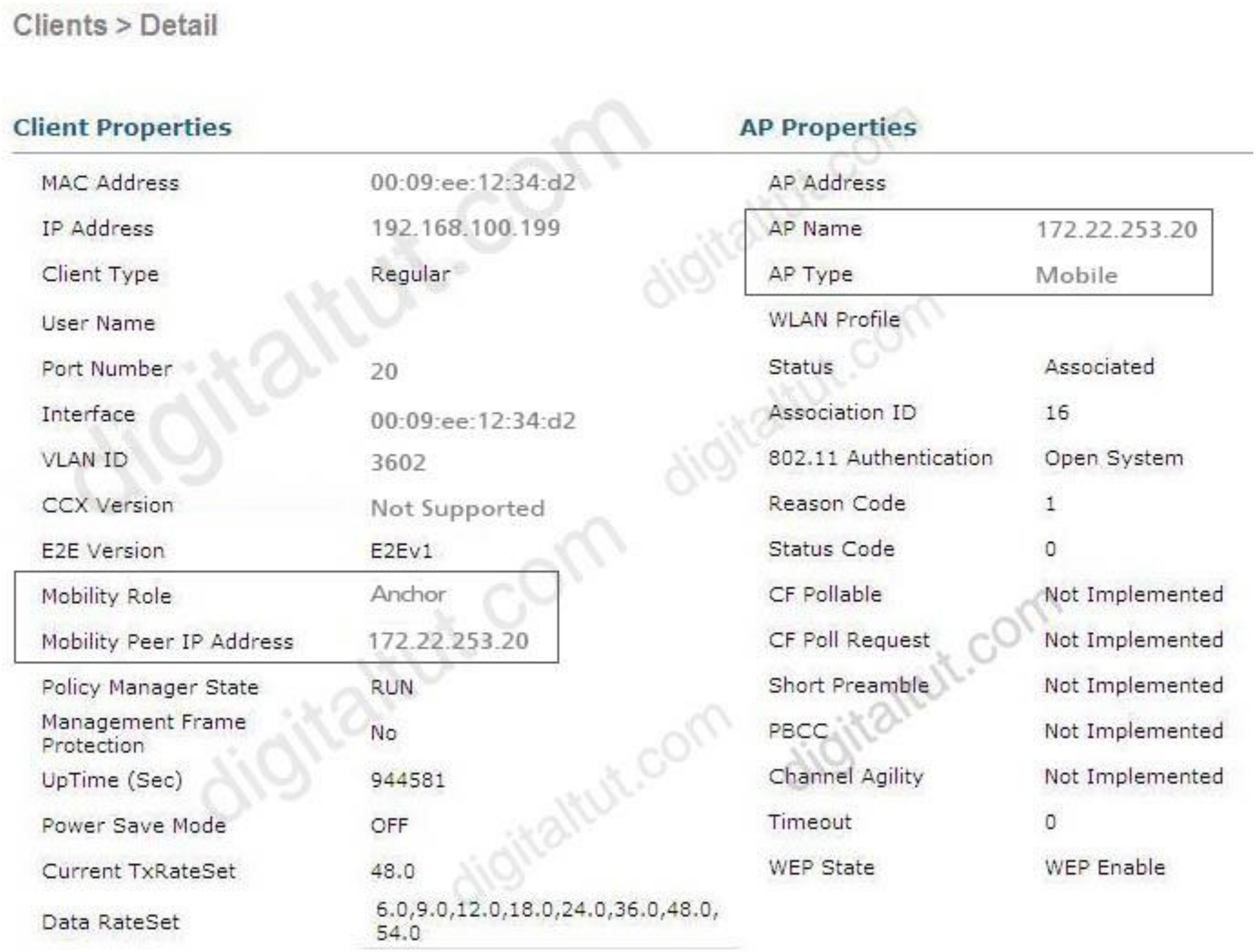
A. It does not require a RADIUS server certificate
B. It requires a client certificate

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

Answer: A

Question 4

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



Clients > Detail

Client Properties

MAC Address	00:09:ee:12:34:d2
IP Address	192.168.100.199
Client Type	Regular
User Name	
Port Number	20
Interface	00:09:ee:12:34:d2
VLAN ID	3602
CCX Version	Not Supported
E2E Version	E2Ev1
Mobility Role	Anchor
Mobility Peer IP Address	172.22.253.20
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	944581
Power Save Mode	OFF
Current TxRateSet	48.0
Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0, 54.0

AP Properties

AP Address	
AP Name	172.22.253.20
AP Type	Mobile
WLAN Profile	
Status	Associated
Association ID	16
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Enable

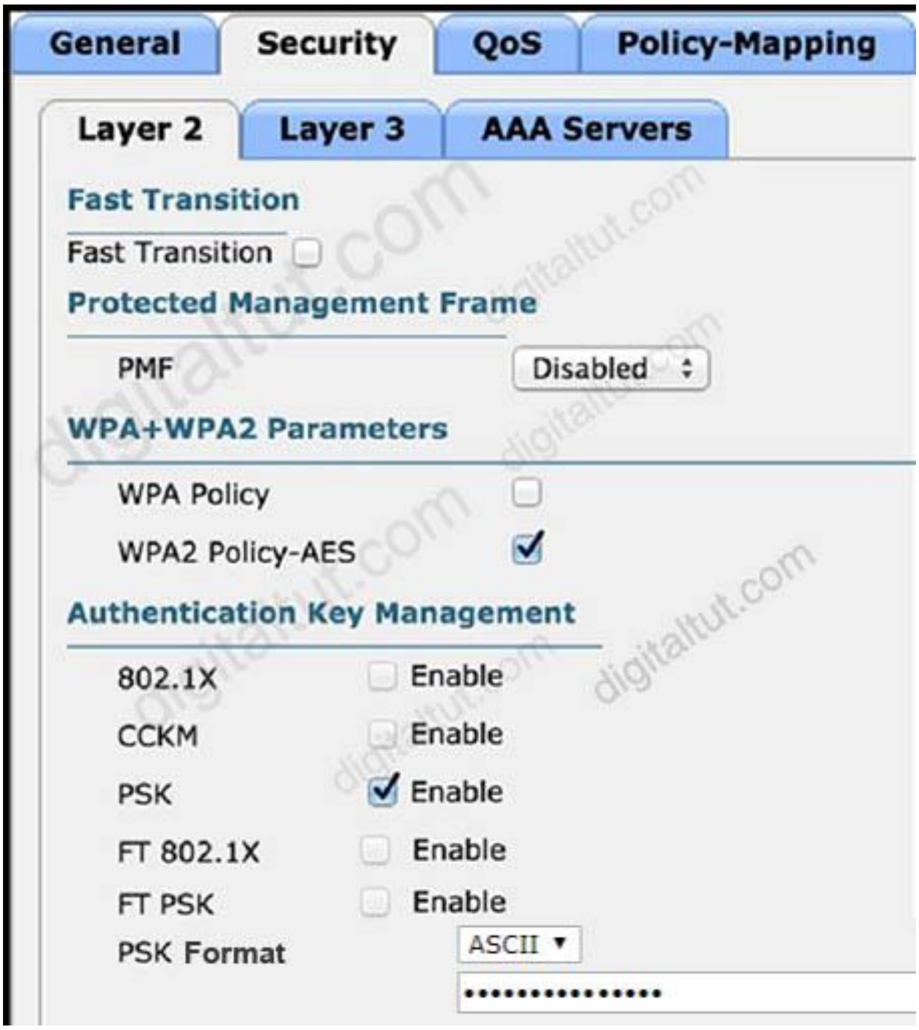
digitaltut.com

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

Answer: B

Question 5

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



Fast Transition

Fast Transition □

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy-AES ☑

Authentication Key Management

802.1X □ Enable

CCKM □ Enable

PSK ☑ Enable

FT 802.1X □ Enable

FT PSK □ Enable

PSK Format ASCII

•••••••••••••••

digitaltut.com

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

Answer: A

Question 6

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: A C

Question 7

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

Question 8

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: D E

Question 9

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

Question 10

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

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

Answer: B

Question 11

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

Question 12

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 13

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

Question 14

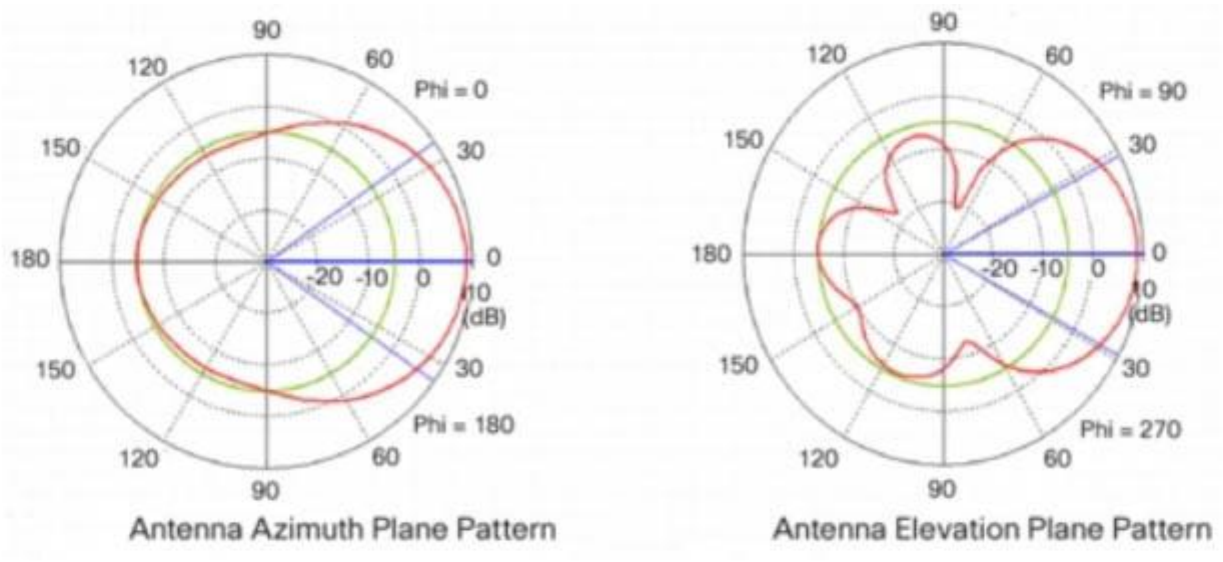
Which two methods are used by an AP that is trying to discover a wireless LAN controller? (Choose two)

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: B D

Question 15

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



Antenna Azimuth Plane Pattern

Antenna Elevation Plane Pattern

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

Answer: A

HSRP & VRRP Questions

https://www.digitaltut.com/hsrp-vrrp-questions

Question 1

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: A D

Question 2

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

Question 3

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 4

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

Question 5

What are three valid HSRP states? (Choose three)

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

Answer: A B E

Question 6

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

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

Answer: B E

Network Assurance Questions

https://www.digitaltut.com/network-assurance-questions

Question 1

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

Question 2

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

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

Answer: D

Question 3

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: B C

Question 4

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 5

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: D E

Question 6

Which statement about an RSPAN session configuration is true?

A. A fitter 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

Question 7

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

Question 8

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 9

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

Security Questions

https://www.digitaltut.com/security-questions-2

Question 1

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
 stoppbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stoppbits 1
line vty 0 4
 password 7 03384737389E938
 login
line vty 5 15
 password 7 03384737389E938
 login
```

```
!
end

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

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

Answer: A

Question 2

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

Question 3

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

Question 4

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

Question 5

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

Question 6

The login method is configured on the VTY lines of a router with these parameters.
– The first method for authentication is TACACS
– If TACACS is unavailable, login is allowed without any provided credentials

Which configuration accomplishes this task?

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

R1#sh run | section vty
line vty 0 4
password 7 0202039485748

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

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

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

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

R1#sh run | section vty
line vty 0 4
password 7 0202039485748
```

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

R1#sh run | section vty
line vty 0 4

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

Answer: C

Question 7

Which NGFW mode block flows crossing the firewall?

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

Answer: D

Question 8

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

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

Answer: D

Access-list Questions

https://www.digitaltut.com/access-list-questions

Question 1

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

A. Permit 10.0.0.0 0.0.0.1
B. Permit 10.0.0.1 0.0.0.0
C. Permit 10.0.0.1 0.0.0.254
D. Permit 10.0.0.0 255.255.255.254

Answer: C

Question 2

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 GigabitEthemet0/0 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 209.165.200.255 255.255.255.0
 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 3

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

Answer: C

Question 4

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

A. Deny tcp any any eq 80
Permit tcp any any gt 21 lt 444

B. Permit tcp any any neq 80

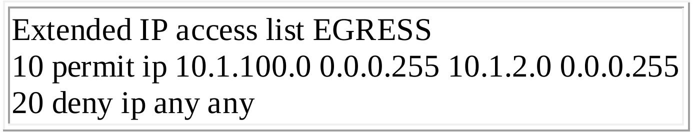
C. Permit tcp any any range 22 443
Deny tcp any any eq 80

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

Answer: C

Question 5

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



```
Extended IP access list EGRESS
10 permit ip 10.1.100.0 0.0.0.255 10.1.2.0 0.0.0.255
20 deny ip any any
```

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

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

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

```
C. config t
ip access-list extended EGRESS2
permit ip 10.1.10.0 0.0.0.295 10.1.2.0 0.0.0.299
permit ip 10.1.100.0 0.0.0.299 10.1.2.0 0.0.0.299
deny ip any any
!
interface g0/1
no ip access-group EGRESS out
ip access-group EGRESS2 out
```

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

Answer: B

Automation Questions

https://www.digitaltut.com/automation-questions

Question 1

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

Question 2

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

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

Answer: A

Question 3

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

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

Answer: A D

Question 4

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 5

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

Question 6

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 go entry-val 75 poll-interval
5”
```

A. It issues email when the value is greater than 75% for five polling cydes
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

Question 7

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

Question 8

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

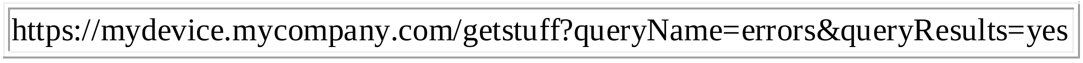
```
event manager applet LARGECONFIG
  event cli pattern "show running-config" sync yes
  action 1.0 puts "Warning! This device has a VERY LARGE configuration
        and may take some time to process"
  action 1.1 puts nonewline "Do you wish to continue [Y/N]"
  action 1.2 gets response
  action 1.3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

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

Answer: A D

Question 9

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 10

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

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

Answer: C E

Question 11

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

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

Answer: B

Question 12

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

Automation Questions 2

https://www.digitaltut.com/automation-questions-2

Question 1

Which statements are used for error handling in Python?

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

Answer: B

Question 2

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

```
PYTHON CODE
import requests
import json

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

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

print(response['ins_api']['outputs'][output']['body']['kickstart_ver_str'])
===========================================================================
HTTP JSON Response:
{
 "ins_api": {
  "type": "cli_show",
  "version":"1.0",
  "sid":"eoc",
  "outputs":{
   "output":{
    "input":"show version",
    "msg":"Success",
    "code":"200",
    "body":{
     "bios_ver_str":"07.61",
     "kickstart_ver_str":"7.0(3)I7(4)",
     "bios_cmpl_time":"04/08/2017",
     "kick_file_name":"bootflash:///nxos.7.0.3.I7.4.bin",
     "kick_cmpl_time":"6/14/1970 09:49:04",
     "chassis_id": "Nexus9000 93180YC-EX chassis",
     "cpu_name": "Intel(R) Xeon(R) CPU @1.80GHz",
     "memory": 24633488,
     "mem_type":"kB",
     "rr_usecs":134703,
     "rr_ctime":"Sun Mar 10 15:41:46 2019",
     "rr_reason": "Reset Requested by CLI command reload",
     "rr_sys_ver":"7.0(3)I7(4)",
     "rr_service":"",
     "manufacturer": "Cisco Systems, Inc",
     "TABLE_package_list": {
      "ROW_package_list": {
       "package_id": {}
      }
     }
    }
   }
  }
 }
}
```

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

Answer: D

Question 3

Which data modeling language is commonly used by NETCONF?

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

Answer: C

Question 4

A response code of 404 is received while using the REST API on Cisco UNA Center to POST to this URL

/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

Question 5

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

Question 6

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

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

Answer: C

Question 7

What do Cisco DNA southbound APIs provide?

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

Answer: A

Question 8

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’

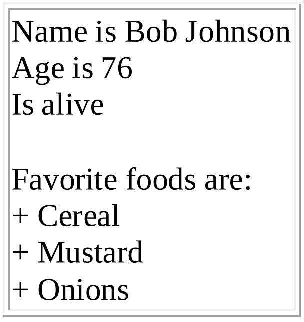
C. event manager applet boom
event syslog pattern ‘UP’
action 1.0 puts ‘logging directly to console’

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

Answer: C

Question 9

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



Name is Bob Johnson
Age is 76
Is alive

Favorite foods are:
+ Cereal
+ Mustard
+ Onions

A. Name: Bob, Johnson, Age: 76, Alive: true, Favourite Foods. [Cereal, “Mustard”, “Onions}}
B. Name”, “Bob Johnson”, “Age”, 76, “Alive”, true, “favourite Foods”, [“Cereal, “Mustard”, Onions”}}
C. Name’, ‘Bob Johnson,’ ‘Age’, 76, ‘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”:76,”alive”:true,”favorite foods”:[“Cereal”,”Mustard”,”Onions”]}

Answer: E

Question 10

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

Question 11

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

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

Miscellaneous Questions

https://www.digitaltut.com/miscellaneous-questions-2

Question 1

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: D E

Question 2

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

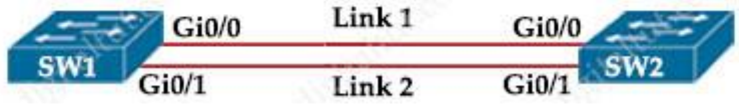
```
access-list 1 permit 10.1.1.0 0.0.0.31
ip nat pool CISCO 209.165.201.1 209.165.201.30 netmask 255.255.255.224
ip nat inside source list 1 pool CISCO
```

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: A E

Question 3

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 G0/1 on SW2, but the port remains blocked.



```
SW2#show spanning-tree
 VLAN0010
   Spanning tree enabled protocol ieee
   Root ID      Priority  24596
                 Address   0018.7363.4300
                Cost      2
                Port      13 (GigabitEthernet0/0)
                Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

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

```
Interface  Role  Sts  Cost Prio.Nbr  Type
---------- ----  ---- ---- --------  ----
Gi0/0      Root  FWD  4    128.1     P2p
Gi0/1      Atln  BLK  4    32.2      P2p
```

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

Question 4

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

Question 5

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: B F

Question 6

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

Question 7

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: C D

Question 8

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

Question 9

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

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

Tunnel0 temporarily disabled due to recursive routing error.

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

A. 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

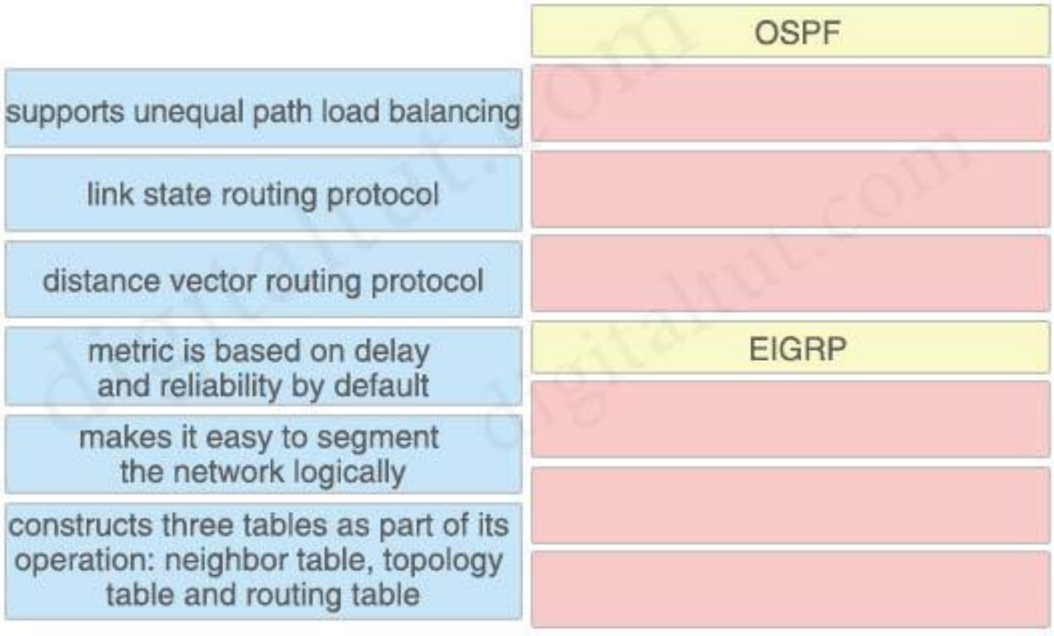
Answer: C E

Drag Drop Questions

https://www.digitaltut.com/drag-drop-questions

Question 1

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



supports unequal path load balancing

link state routing protocol

distance vector routing protocol

metric is based on delay and reliability by default

makes it easy to segment the network logically

constructs three tables as part of its operation: neighbor table, topology table and routing table

OSPF

EIGRP

Answer:

OSPF:
+ link state routing protocol
+ makes it easy to segment the network logically
+ constructs three tables as part of its operation: neighbor table, topology table and routing table

EIGRP:
+ supports unequal path load balancing
+ distance vector routing protocol
+ metric is based on delay and reliability by default (?)

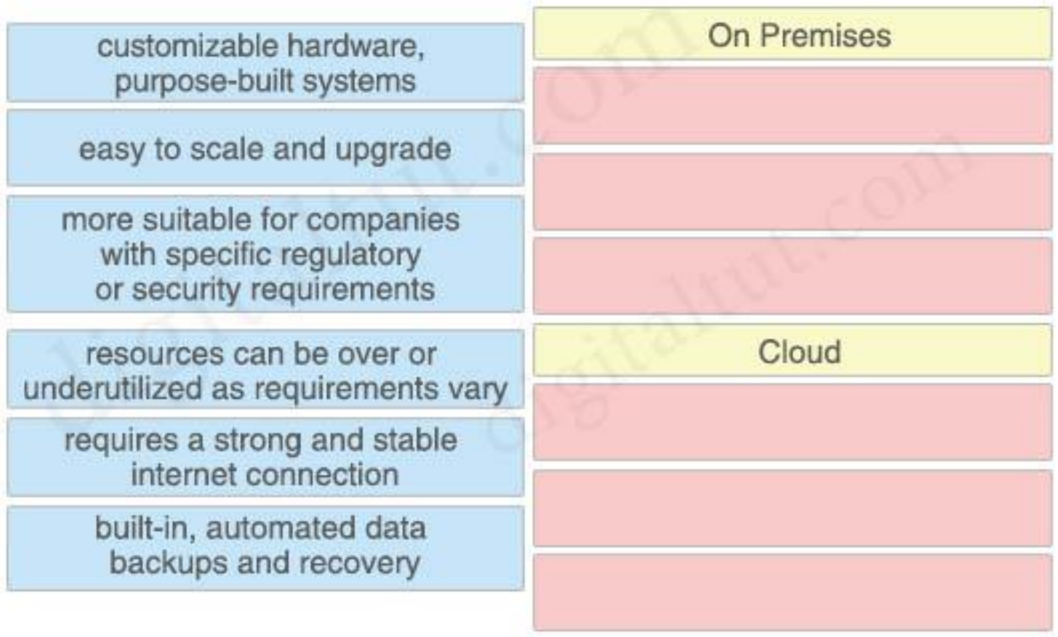
Explanation

Maybe there is something wrong with the answer "metric is based on delay and reliability by default" as OSPF metric is only dependent on the interface bandwidth & reference bandwidth while EIGRP metric is dependent on bandwidth and delay by default. But only EIGRP metric is based on delay so "EIGRP" is a better answer.

Both OSPF and EIGRP have three tables to operate: neighbor table (store information about OSPF/EIGRP neighbors), topology table (store topology structure of the network) and routing table (store the best routes).

Question 2

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



customizable hardware, purpose-built systems

easy to scale and upgrade

more suitable for companies with specific regulatory or security requirements

resources can be over or underutilized as requirements vary

requires a strong and stable internet connection

built-in, automated data backups and recovery

On Premises

Cloud

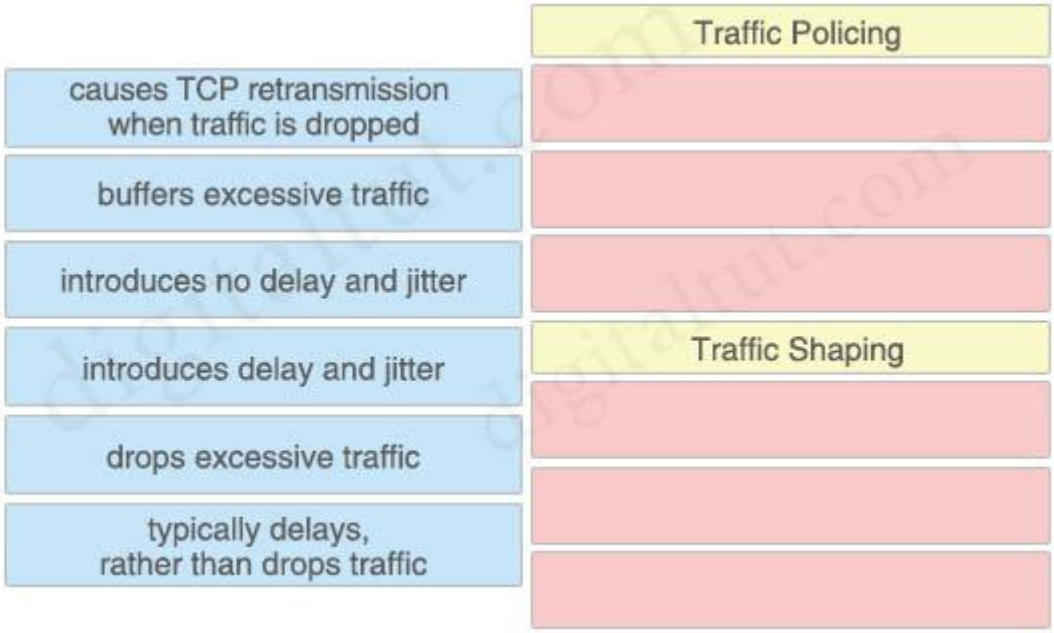
Answer:

On Premises:
+ resources can be over or underutilized as requirements vary
+ customizable hardware, purpose-built systems
+ more suitable for companies with specific regulatory or security requirements

Cloud:
+ easy to scale and upgrade
+ requires a strong and stable internet connection
+ built-in, automated data backups and recovery

Question 3

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



causes TCP retransmission when traffic is dropped

buffers excessive traffic

introduces no delay and jitter

introduces delay and jitter

drops excessive traffic

typically delays, rather than drops traffic

Traffic Policing

Traffic Shaping

digitaltut.com

Answer:

Traffic Policing:
+ introduces no delay and jitter
+ drops excessive traffic
+ causes TCP retransmission when traffic is dropped

Traffic Shaping:
+ buffers excessive traffic
+ introduces delay and jitter
+ typically delays, rather than drops traffic