# Cisco.350-401.v2021-04-04.q96

| | |
|---|---|
| **Exam Code:** | 350-401 |
| **Exam Name:** | Implementing Cisco Enterprise Network Core Technologies (350-401 ENCOR) |
| **Certification Provider:** | Cisco |
| **Free Question Number:** | 96 |
| **Version:** | v2021-04-04 |
| **# of views:** | 1952 |
| **# of Questions views:** | 87791 |
| https://www.freecram.net/torrent/Cisco.350-401.v2021-04-04.q96.html | |

**NEW QUESTION: 1**
Which DNS lookup does an access point perform when attempting CAPWAP discovery?
**A.** CAPWAP-CONTROLLER local
**B.** CISCO-DNA-CONTROLLER local
**C.** CISCO-CAPWAP-CONTROLLER local
**D.** CISCO-CONTROLLER local
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 2**
A response code of 404 is received while using the REST API on Cisco UNA Center to POST to this URI.
/dna/intent/api/v1 /template-programmer/project
What does the code mean?
**A.** The client made a request a resource that does not exist.
**B.** The server has not implemented the functionality that is needed to fulfill the request.
**C.** The request accepted for processing, but the processing was not completed.
**D.** The POST/PUT request was fulfilled and a new resource was created, Information about the resource is in the response body.
**Answer: (SHOW ANSWER)**
The 404 (Not Found) error status code indicates that the REST API can't map the client's URI to a resource but may be available in the future. Subsequent requests by the client are permissible.

**NEW QUESTION: 3**
What is a Type 1 hypervisor?

**A.** runs on a virtual server and depends on an already installed operating system
**B.** runs directly on a physical server and includes its own operating system
**C.** runs directly on a physical server and depends on a previously installed operating system
**D.** run on a virtual server and includes its own operating system
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 4**
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: (SHOW ANSWER)**
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.

**NEW QUESTION: 5**
Which two security features are available when implementing NTP? (Choose two )
**A.** symmetric server passwords
**B.** dock offset authentication
**C.** broadcast association mode
**D.** encrypted authentication mechanism
**E.** access list-based restriction scheme
**Answer: (SHOW ANSWER)**
The time kept on a machine is a critical resource and it is strongly recommend that you use the security features of NTP to avoid the accidental or malicious setting of incorrect time. The two security features available are an access list-based restriction scheme and an encrypted authentication mechanism.

**NEW QUESTION: 6**
What are three valid HSRP states? (Choose three)
**A.** learning
**B.** speak
**C.** full
**D.** listen
**E.** INIT

**F.** established

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 7**

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

**A.** ARP probing

**B.** with OMP

**C.** with IP SLA

**D.** using BFD

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 8**

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

**A.** TLOC

**B.** RLOC

**C.** DNS

**D.** VTEP

**E.** EID

**Answer: (SHOW ANSWER)**

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:

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

**NEW QUESTION: 9**

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

**A.** traffic specification

**B.** SIP flow information

**C.** VoIP media session awareness

**D.** Wi-Fi multimedia

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 10**

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

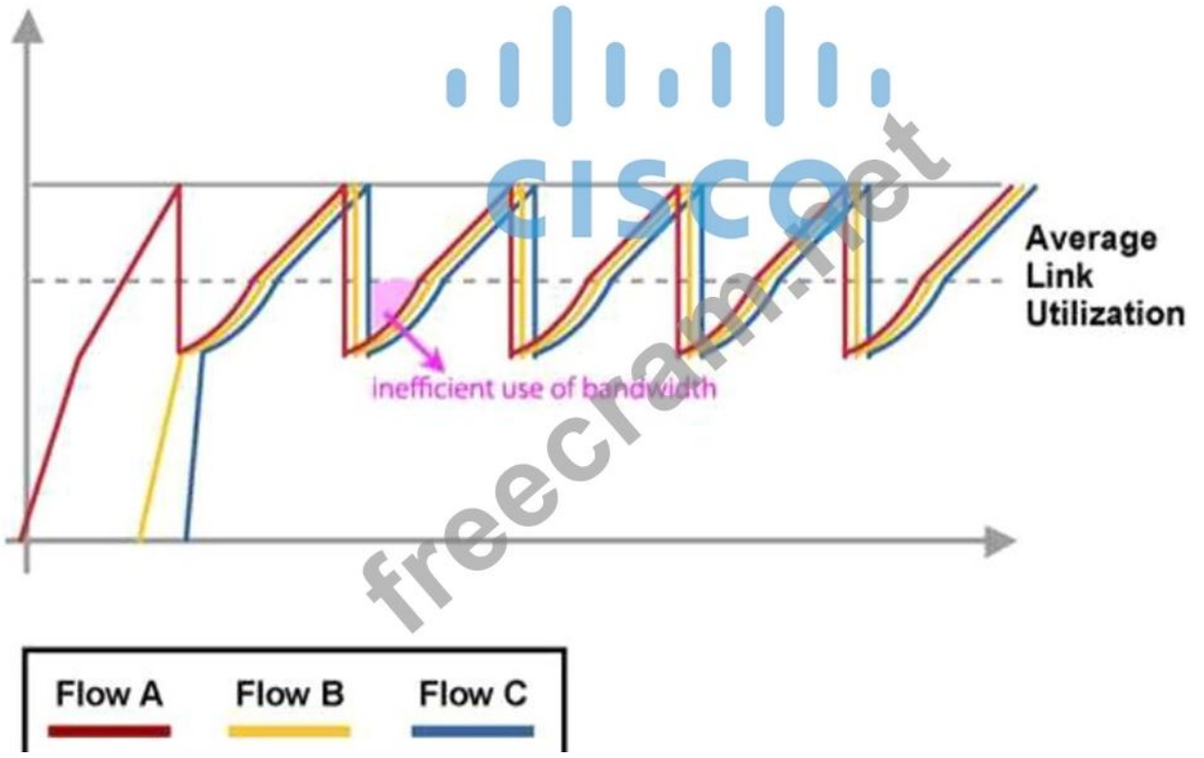
**D.** provides additional forwarding capacity to the fabric

**Answer: (SHOW ANSWER)**

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

Reference:

213525-sda-steps-to-configure-fusion-router.html




**NEW QUESTION: 11**

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

**A.** It supports unique virtual MAC addresses

**B.** Its virtual MAC is 0000.0C07.ACxx

**C.** Its multicast virtual MAC is 0000.5E00.01xx

**D.** It supports tracking

**E.** Its default configuration allows for pre-emption

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 12**

Refer to the exhibit.

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

Type                        : Remote Destination Session
Source RSPAN VLAN           : 50

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

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

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

**A.** SPAN session 2 only monitors egress traffic exiting port FastEthernet 0/14.

**B.** SPAN session 1 monitors activity on VLAN 50 of a remote switch

**C.** SPAN session 2 monitors all traffic entering and exiting port FastEthernet 0/15.

**D.** RSPAN session 1 is incompletely configured for monitoring

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 13**

Refer to the exhibit.


After an engineer configures an EtherChannel between switch SW1 and switch SW2, this error message is logged on switch SW2.

```
SW2#
09:45:32: %PM-4-ERR_DISABLE: channel-misconfig error detected on Gi0/0, putting Gi0/0 in err-disable state
09:45:32: %PM-4-ERR_DISABLE: channel-misconfig error detected on Gi0/1, putting Gi0/1 in err-disable state
```

Based on the output from SW1 and the log message received on Switch SW2, what action should the engineer take to resolve this issue?

**A.** Define the correct port members on the EtherChannel on switch SW1.

**B.** Connect the configuration error on interface Gi0/1 on switch SW1.

**C.** Correct the configuration error on interface Gi0/0 switch SW1.

**D.** Configure the same protocol on the EtherChannel on switch SW1 and SW2.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 14**
What is used to measure the total output energy of a Wi-Fi device?
**A.** dBi
**B.** EIRP
**C.** mW
**D.** dBm
**Answer: (SHOW ANSWER)**
Output power is measured in mW (milliwatts). answer 'dBi' milliwatt is equal to one thousandth (10-3) of a watt.

**NEW QUESTION: 15**
Drag and drop the LISP components from the left onto the function they perform on the right. Not all options are used.


**Answer:**

Explanation:
+ 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 no routable 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

**NEW QUESTION: 16**
At which Layer does Cisco DNA Center support REST controls?
**A.** Session layer
**B.** Northbound APIs
**C.** EEM applets or scripts
**D.** YMAL output from responses to API calls
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 17**

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

**A.** TACACS server

**B.** RADIUS server

**C.** PKI server

**D.** NTP server

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 18**

Which DHCP option helps lightweight APs find the IP address of a wireless LAN controller?

**A.** Option 150

**B.** Option 60

**C.** Option 43

**D.** Option 67

**Answer: (SHOW ANSWER)**

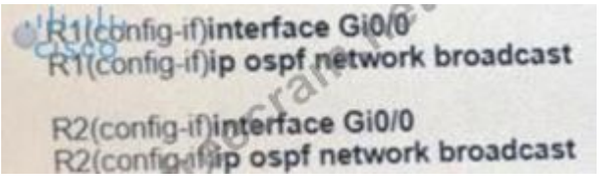
**NEW QUESTION: 19**

Refer to the exhibit.


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

A)


B)




C)


D)


**A.** Option A

**B.** Option B

**C.** Option C

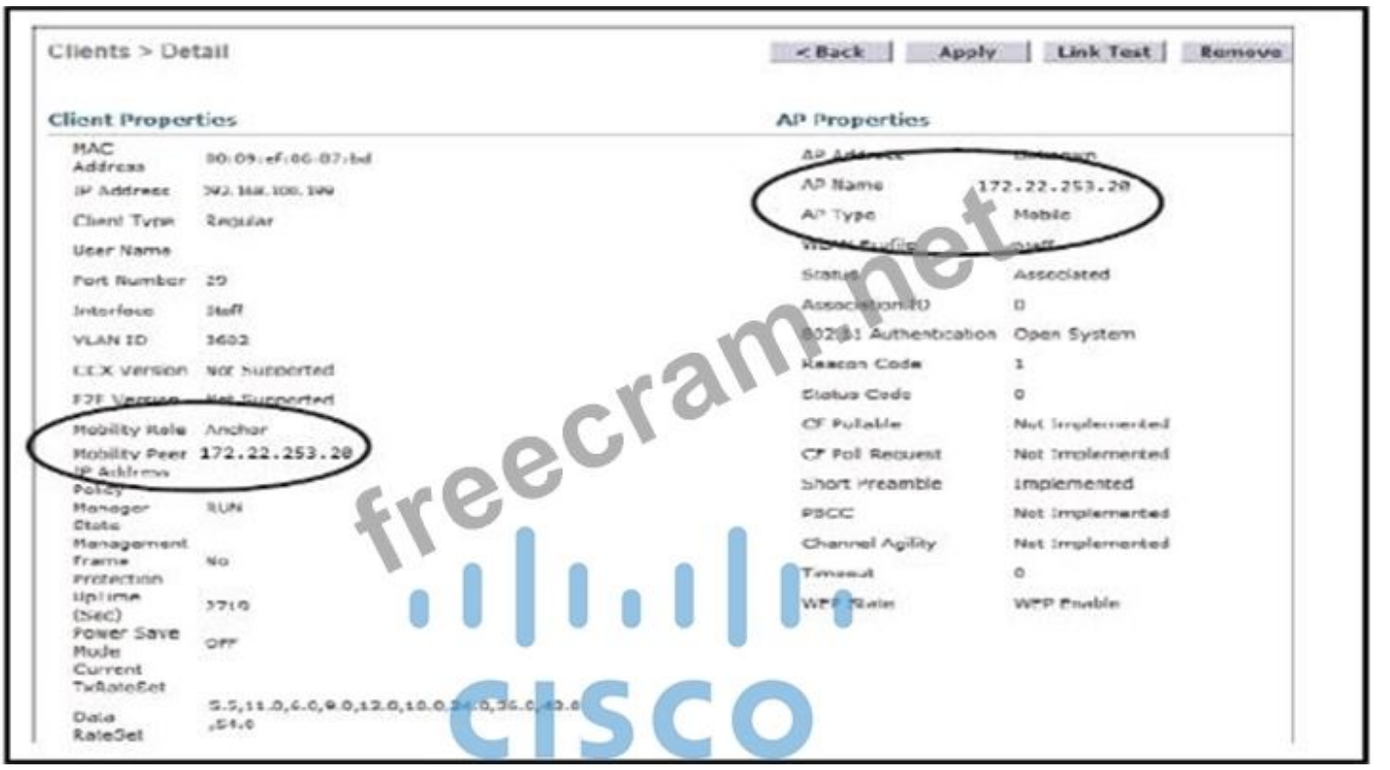
**D.** Option D

**Answer: (SHOW ANSWER)**

Broadcast and Non-Broadcast networks elect DR/BDR while Point-topoint/ 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.

**NEW QUESTION: 20**

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?

**A.** Indirect

**B.** Layer 2 intercontroller

**C.** Intracontroller

**D.** Layer 3 intercontroller

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 21**

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

**A.** Type 1 hypervisor runs directly on the physical hardware of the host machine without relying on the underlying OS.

**B.** Type 1 hypervisor enables other operating systems to run on it.

**C.** Type 1 hypervisor relics on the existing OS of the host machine to access CPU, memory, storage, and network resources.

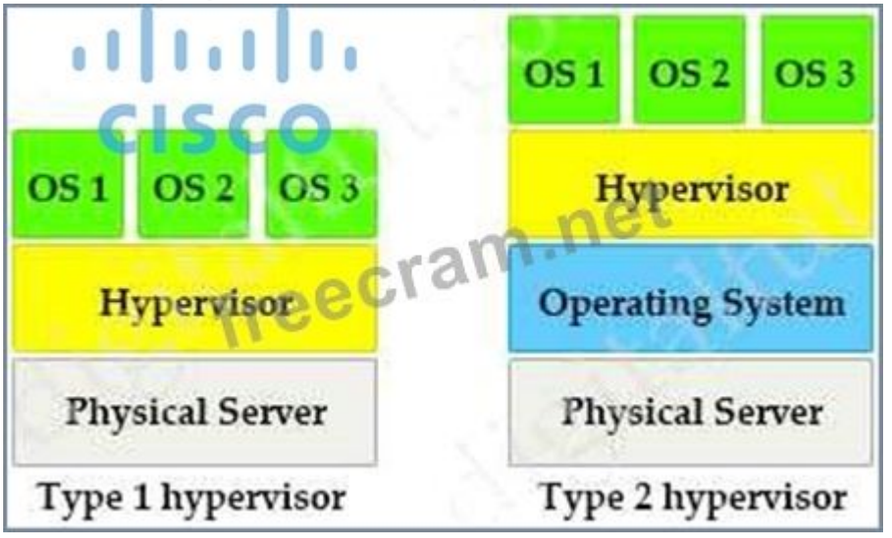
**D.** Type 1 hypervisor is the only type of hypervisor that supports hardware acceleration techniques.

**Answer: (SHOW ANSWER)**

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

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

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




**NEW QUESTION: 22**
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: (SHOW ANSWER)**
A complete Cisco DNA Center upgrade includes "System Update" and "Appplication Updates"




**NEW QUESTION: 23**

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: (SHOW ANSWER)**

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:

b_cg85/mobility_groups.html

**NEW QUESTION: 24**

Refer to the exhibit.


Which LISP component do routers in the public IP network use to

forward traffic between the two networks?

**A.** RLOC

**B.** map resolver

**C.** EID

**D.** map server

**Answer: A (LEAVE A REPLY)**

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:

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

**NEW QUESTION: 25**

What is the result of applying this access control list?

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

**A.** TCP traffic with the URG bit set is allowed

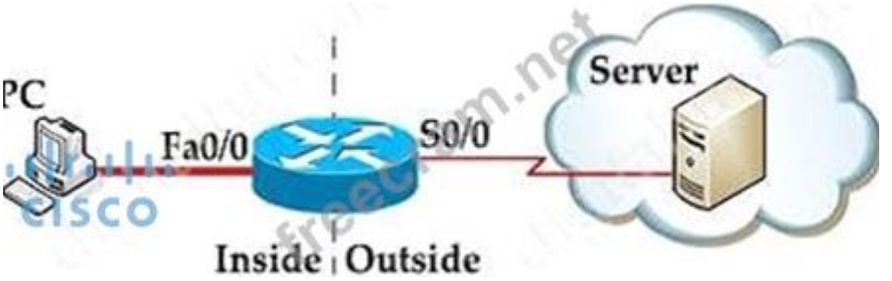
**B.** TCP traffic with the SYN bit set is allowed

**C.** TCP traffic with the ACK bit set is allowed

**D.** TCP traffic with the DF bit set is allowed

**Answer: (SHOW ANSWER)**

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




Suppose you only want to allow the hosts inside your company to telnet to an outside server but not vice versa, you can simply use an "established" access-list like this: access-list 100 permit tcp any any established access-list 101 permit tcp any any eq telnet ! interface S0/0 ip access-group 100 in ip access-group 101 out

**NEW QUESTION: 26**

Refer to the exhibit. An engineer is using XML in an application to send information to a RESTCONF-enabled device. After sending the request, the engineer gets this response message and a HTTP response code of 400. What do these responses tell the engineer?

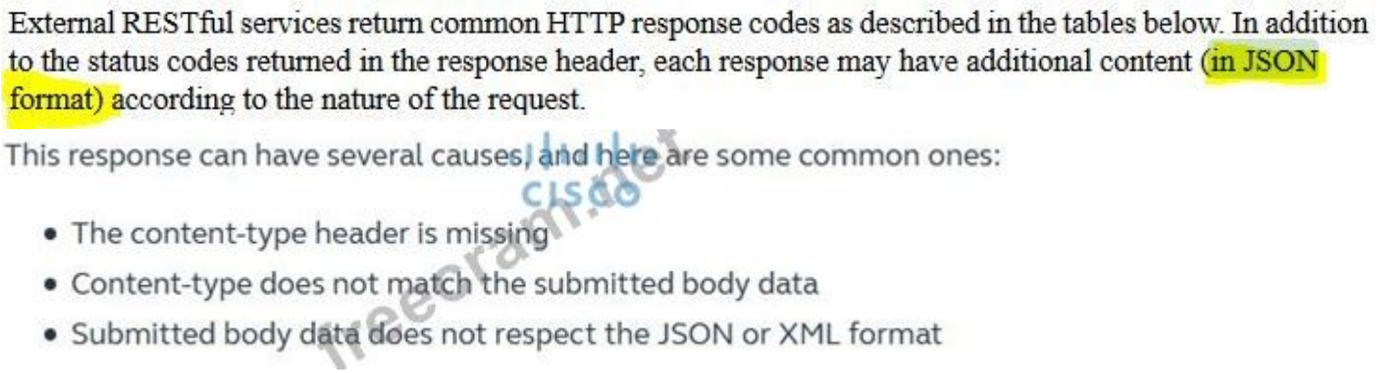
**A.** The Accept header sent was application/xml

**B.** POST was used instead of PUT to update

**C.** The Content-Type header sent was application/xml.

**D.** JSON body was used

**Answer: (SHOW ANSWER)**


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

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

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



**NEW QUESTION: 27**

Which statement about VXLAN is true?

**A.** VXLAN uses TCP 35 the transport protocol over the physical data cento network

**B.** VXLAN extends the Layer 2 Segment ID field to 24-bits. which allows up to 4094 unique Layer 2 segments over the same network.

**C.** VXLAN encapsulates a Layer 2 frame in an IP-UDP header, which allows Layer 2 adjacency across router boundaries.

**D.** VXLAN uses the Spanning Tree Protocol for loop prevention.

**Answer: (SHOW ANSWER)**

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

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

Reference:

lan-and-ethernet-virt.html

**NEW QUESTION: 28**

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: (SHOW ANSWER)**

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

**NEW QUESTION: 29**

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

**A.** hypervisor

**B.** pNIC

**C.** vSwitch

**D.** virtual router

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 30**

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

**A.** HEAD

**B.** REMOVE

**C.** PULL

**D.** PATCH

**E.** ADD

**F.** PUSH

**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 31**

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

**A.** It can support multiple customers on a single switch

**B.** It supports most routing protocols, including EIGRP, ISIS, and OSPF

**C.** It should be used when a customer's router is connected to an ISP over OSPF

**D.** It can increase the packet switching rate

**E.** It supports MPLS-VRF label exchange and labeled packets

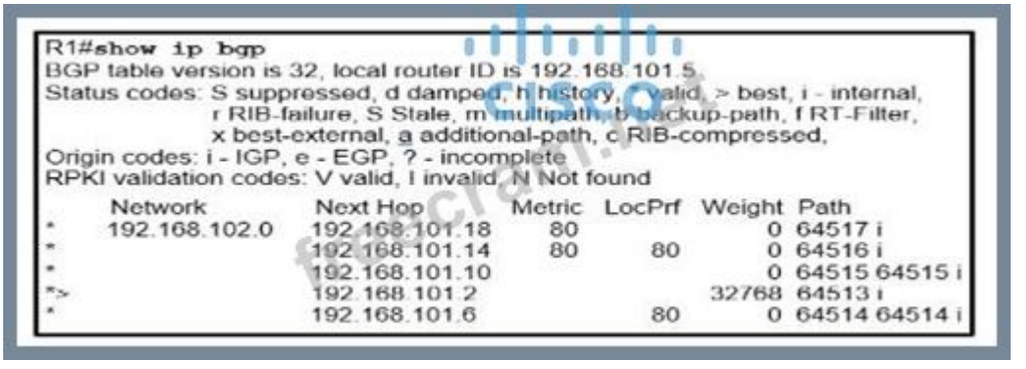
**Answer: (SHOW ANSWER)**

In VRF-Lite, Route distinguisher (RD) identifies the customer routing table and allows customers to be assigned overlapping addresses. Therefore it can support multiple customers with overlapping addresses -> Answer 'It can support multiple customers on a single switch' is correct. VRFs are commonly used for MPLS deployments, when we use VRFs without MPLS then we call it VRF lite -> Answer 'It supports MPLS-VRF label exchange and labeled packets' is not correct. VRF-Lite supports most populr routing protocols: BGP, OSPF, EIGRP, RIP, and static routing -> Answer 'It supports most routing protocols, including EIGRP, ISIS, and OSPF' is correct.



**NEW QUESTION: 32**

Refer to the exhibit.




Which IP address becomes the active next hop for 192.168.102 0/24 when 192.168.101.2 fails?

**A.** 192.168.101.18

**B.** 192.168.101.6

**C.** 192.168.101.10

**D.** 192.168.101.14

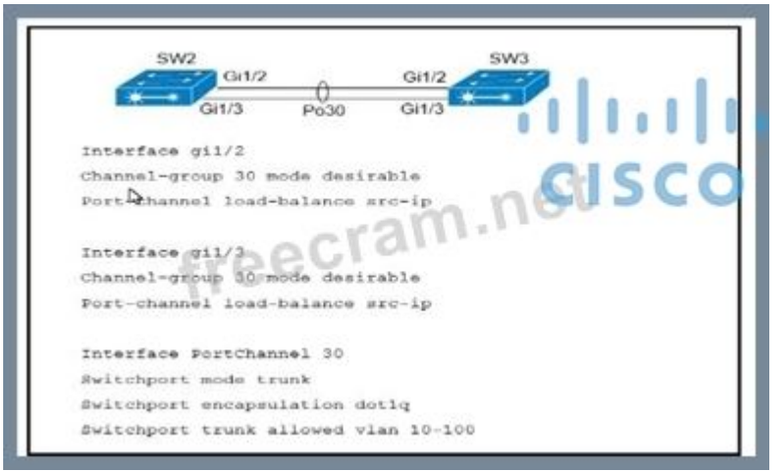
**Answer: (SHOW ANSWER)**

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

Path Selection Attributes: Weight > Local Preference > Originate > AS Path > Origin > MED > External > IGP Cost > eBGP Peering > Router ID BGP prefers the path with highest weight but the weights here are all 0 (which indicate all routes that are not originated by the local router) so we need to check the Local Preference. Answer

'192.168.101.18' path without LOCAL_PREF (LocPrf column) means it has the default value of 100.
Therefore we can find the two next best paths with the next hop of 192.168.101.18 and 192.168.101.10.
We have to move to the next path selection attribute: Originate. BGP prefers the path that the local router originated (which is indicated with the "next hop 0.0.0.0"). But none of the two best paths is self-originated.
The AS Path of the next hop 192.168.101.18 is shorter than the AS Path of the next hop 192.168.101.10 then the next hop 192.168.101.18 will be chosen as the next best path.

**NEW QUESTION: 33**
Refer to the exhibit.




A port channel is configured between SW2 and SW3. SW2 is not running a Cisco operating system. When all physical connections are mode, the port channel does not establish. Based on the configuration excerpt of SW3, what is the cause of the problem?
**A.** The port channel on SW2 is using an incompatible protocol.
**B.** The port-channel should be set to auto.
**C.** The port-channel interface lead balance should be set to src-mac
**D.** The port-channel trunk is not allowing the native VLAN.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 34**
What is the primary effect of the spanning-tree portfast command?
**A.** It enables BPDU messages
**B.** It minimizes spanning-tree convergence time
**C.** It immediately puts the port into the forwarding state when the switch is reloaded
**D.** It immediately enables the port in the listening state
**Answer: (SHOW ANSWER)**
Portfast feature should only be used on edge ports (ports directly connected to end stations). Neither edge ports or PortFast enabled ports generate topology changes when the link toggles so we cannot say Portfast reduces the STP convergence time.

PortFast causes a switch or trunk port to enter the spanning tree forwarding state immediately, bypassing the listening and learning states so answer 'It immediately puts the port into the forwarding state when the switch is reloaded ' is the best choice.

**NEW QUESTION: 35**

Refer to the exhibit.


Which privilege level is assigned to VTY users?

**A.** 1

**B.** 7

**C.** 13

**D.** 15

**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 36**

Refer to the exhibit.

Tunnel-Private-Group-Id(81): 15 Tunnel-Medium-Type(65): IEEE-802(6) Tunnel-Type(64): VLAN(13) A wireless client is connecting to FlexAP1 which is currently working standalone mode. The AAA authentication processis returning the following AVPs:

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

**A.** When the AP is in connected mode, the client will be placed in VLAN 15.

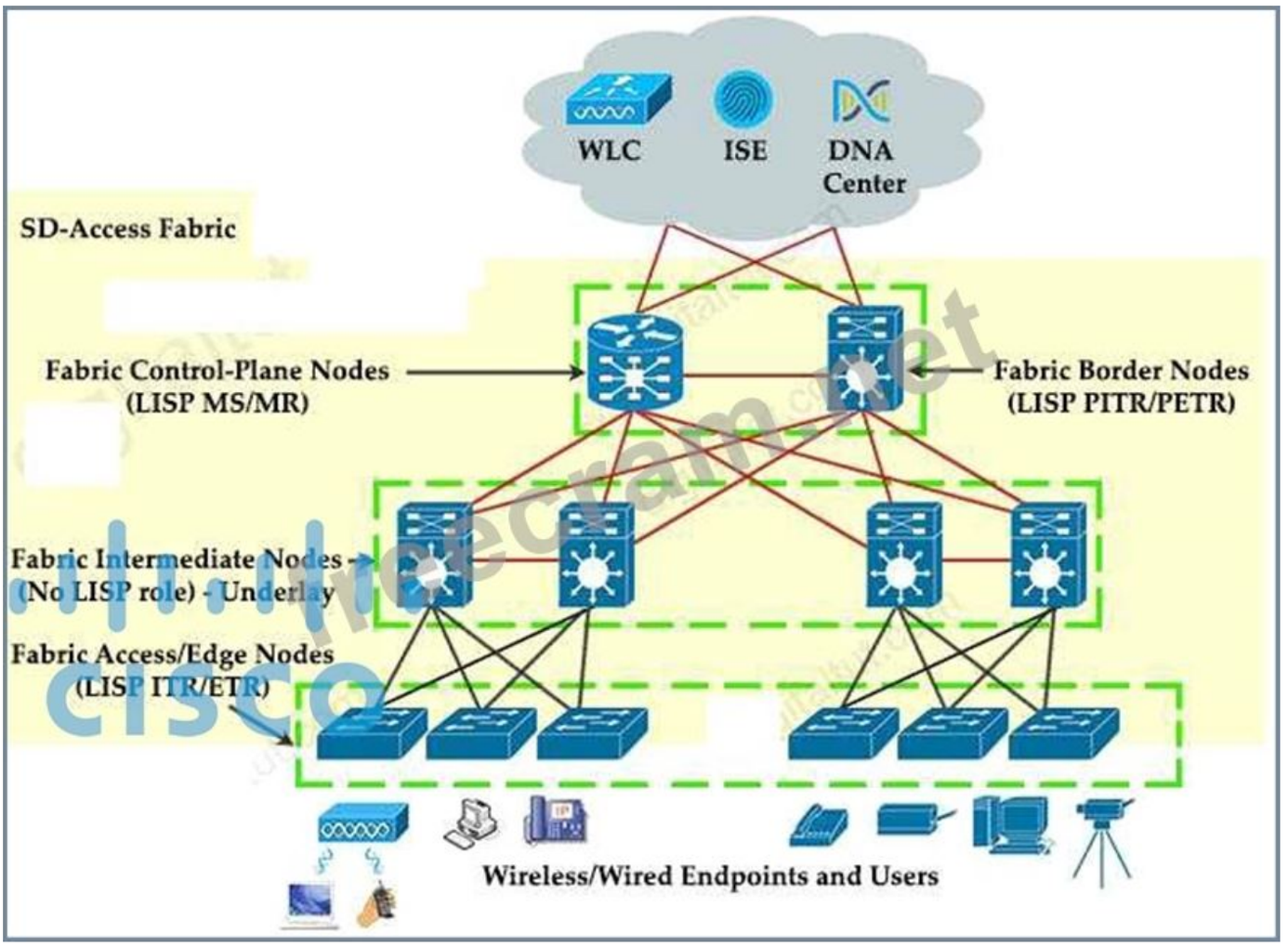
**B.** When the AP transitions to connected mode, the client will remain associated.

**C.** While the AP is in standalone mode, the client will be placed in VLAN 15.

**D.** When the AP is in connected mode, the client will be placed in VLAN 10.

**E.** When the AP is in connected mode, the client will be placed in VLAN 13.
**F.** While the AP is in standalone mode, the client will be placed in VLAN 13.
**G.** When the AP transitions to connected mode, the client will be de-authenticated.
**H.** While the AP is in standalone mode, the client will be placed in VLAN 10.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 37**
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 (LEAVE A REPLY)**
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.




**NEW QUESTION: 38**
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 (LEAVE A REPLY)**
Cisco IOS IP SLA Responder is a Cisco IOS Software component whose functionality is to respond to Cisco IOS IP SLA request packets. The IP SLA source sends control packets before the operation starts to establish a connection to the responder. Once the control packet is acknowledged, test packets are sent to the responder. The responder inserts a time-stamp when it receives a packet and factors out the destination processing time and adds time-stamps to the sent packets. This feature allows the calculation of unidirectional packet loss, latency, and jitter measurements with the kind of accuracy that is not possible with ping or other dedicated probe testing.
Reference:
0aecd806bfb52.html

The IP SLAs responder is a component embedded in the destination Cisco device that allows the system to anticipate and respond to IP SLAs request packets. The responder provides accurate measurements without the need for dedicated probes.
2/46sg/configuration/guide/Wrapper-46SG/swipsla.html
UDP Jitter measures the delay, delay variation(jitter), corruption, misorderingand packet lossby generating periodic UDP traffic. This operation always requires IP SLA responder.

**NEW QUESTION: 39**
Which statement about an RSPAN session configuration is true?
**A.** A fitter mutt be configured for RSPAN Regions
**B.** Only one session can be configured at a time
**C.** A special VLAN type must be used as the RSPAN destination.
**D.** Only incoming traffic can be monitored
**Answer: (SHOW ANSWER)**
in all participating switches -> This VLAN can be considered a special VLAN type -> Answer 'A special VLAN type must be used as the RSPAN destination' is correct.
Reference:
elease/12-2_55_se/configuration/guide/3750xscg/swspan.html
We can configure multiple RSPAN sessions on a switch at a time, then continue configuring multiple RSPAN sessions on the other switch without any problem -> Answer 'Only one session can be configured at a time' is not correct.
This is how to configure Remote SPAN (RSPAN) feature on two switches. Traffic on FastEthernet0/1 of Switch 1 will be sent to Fa0/10 of Switch2 via VLAN 40.
+ Configure on both switches
Switch1,2(config)#vlan 40
Switch1,2(config-vlan)#remote-span
+ Configure on Switch1
Switch1(config)# monitor session 1 source interface FastEthernet 0/1
Switch1(config)# monitor session 1 destination remote vlan 40
+ Configure on Switch2
Switch2(config)#monitor session 5 source remote vlan 40
Switch2(config)# monitor session 5 destination interface FastEthernet 0/10

**NEW QUESTION: 40**
A GRE tunnel is down with the error message %TUN-5-RECUR DOWN:
**Tunnel0 temporarily disabled due to recursive routing error.**
Which two options describe possible causes of the error? (Choose two)
**A.** There is link flapping on the tunnel
**B.** Incorrect destination IP addresses are configured on the tunnel
**C.** The tunnel mode and tunnel IP address are misconfigured
**D.** There is instability in the network due to route flapping

**E.** The tunnel destination is being routed out of the tunnel interface

**Answer: (SHOW ANSWER)**

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

+ A misconfiguration that causes the router to try to route to the tunnel destination address using the tunnel interface itself (recursive routing)

+ A temporary instability caused by route flapping elsewhere in the network Reference: eigrp/22327-gre-flap.html

**NEW QUESTION: 41**

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'

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

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

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



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

**Answer: (SHOW ANSWER)**

Reference:

a1.html

**NEW QUESTION: 42**

In a Cisco SD-Access wireless architecture, which device manages endpoint ID to Edge Node bindings?

**A.** fabric wireless controller

**B.** fabric control plane node

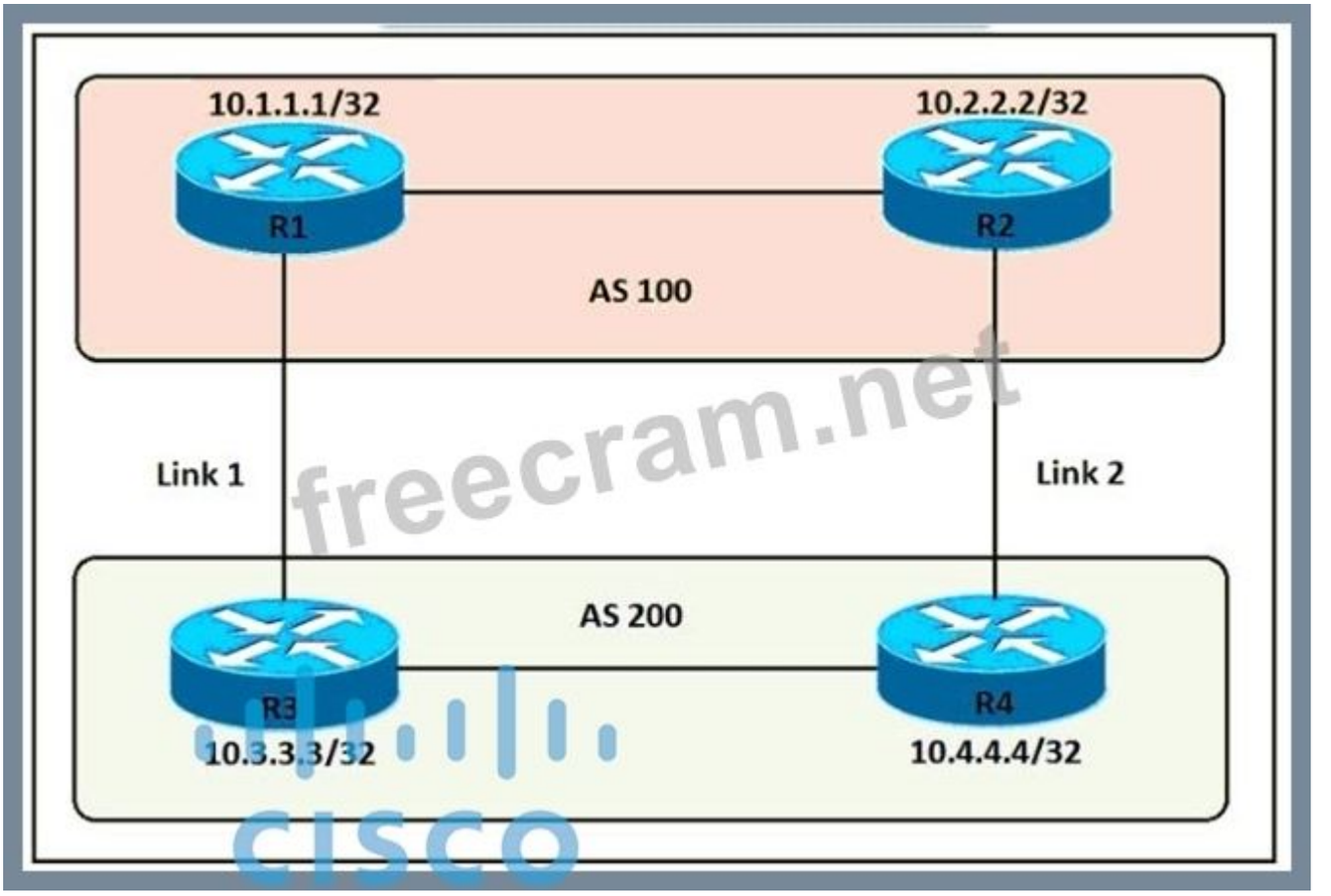
**C.** fabric border node

**D.** fabric edge node.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 43**

Refer to the exhibit.




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

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

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

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

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

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

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

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

R4(config)#router bgp 200
```

**A.** Option D

**B.** Option C

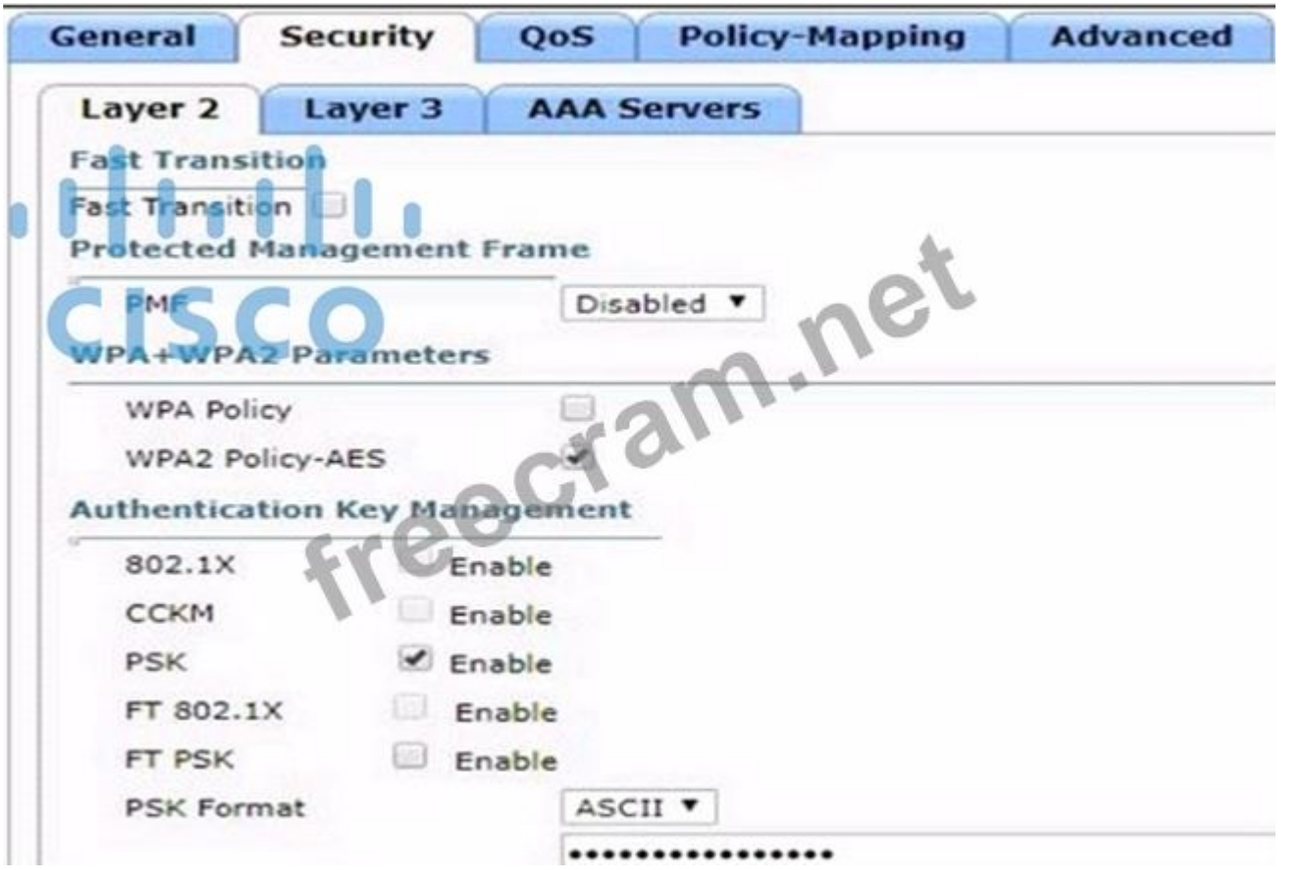
**C.** Option A

**D.** Option B

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 44**

Refer to the exhibit.




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

**A.** RADIUS token

**B.** username and password

**C.** certificate

**D.** text string

**Answer: (SHOW ANSWER)**

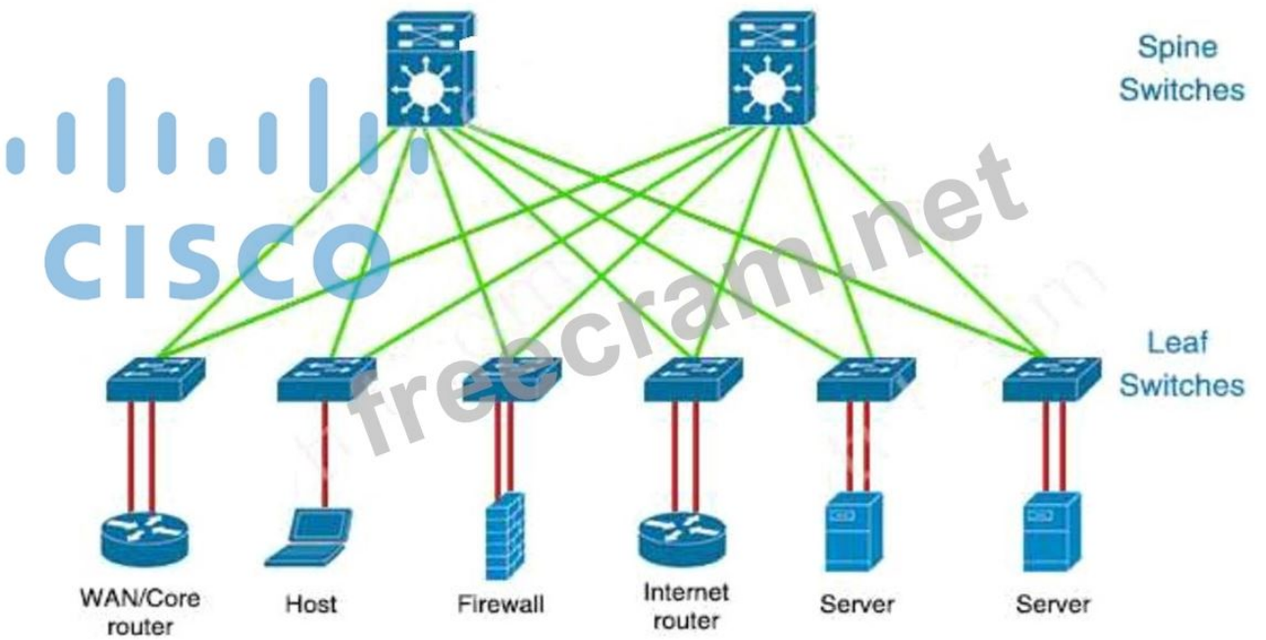
**NEW QUESTION: 45**

An engineer is configuring GigabitEthernet1/0/0 for VRRP. When the router has the highest priority In group 5, It must assume the master role. Which command set should the engineer add to the configuration to accomplish this task?


**A.** Option D

**B.** Option A
**C.** Option B
**D.** Option C
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 46**
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 (LEAVE A REPLY)**
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).



**NEW QUESTION: 47**
What function does vxlan perform in an SD-Access deployment?
**A.** systems management and orchestration
**B.** control plane forwarding
**C.** data plane forwarding
**D.** policy plane forwarding
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 48**
Which component handles the orchestration plane of the Cisco SD-WAN?
**A.** vSmart
**B.** vManage
**C.** vBond
**D.** vEdge
+ 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.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 49**
Which IPv6 migration method relies on dynamic tunnels that use the 2002::/16 reserved address space?
**A.** GRE
**B.** 6RD
**C.** 6to4
**D.** ISATAP
**Answer: (SHOW ANSWER)**
6to4 tunnel is a technique which relies on reserved address space 2002::/16 (you must remember this range). These tunnels determine the appropriate destination address by combining the IPv6 prefix with the globally unique destination 6to4 border router's IPv4 address, beginning with the 2002::/16 prefix, in this format:
2002:border-router-IPv4-address::/48
For example, if the border-router-IPv4-address is 64.101.64.1, the tunnel interface will have an IPv6 prefix of 2002:4065:4001:1::/64, where 4065:4001 is the hexadecimal equivalent of

64.101.64.1. This technique allows IPv6 sites to communicate with each other over the IPv4 network without explicit tunnel setup but we have to implement it on all routers on the path.

**NEW QUESTION: 50**

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



**A.** HTTP Status Code 200

**B.** HTTP Status Code 302

**C.** HTTP Status Code 401

**D.** HTTP Status Code: 504

**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 51**

What is the purpose of an RP in PIM?

**A.** ensure the shortest path from the multicast source to the receiver.

**B.** send join messages toward a multicast source SPT

**C.** secure the communication channel between the multicast sender and receiver.

**D.** receive IGMP joins from multicast receivers.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 52**

Refer to the exhibit.


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

**A.** RSPAN traffic is sent to VLANs 222 and 223.

**B.** An error is flagged for configuring two destinations.

**C.** RSPAN traffic is split between VLANs 222 and 223.

**D.** The RSPAN VLAN is replaced by VLAN 223.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 53**

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

**A.** It uses an API call to interrogate the devices and register the returned data.

**B.** It creates device packs through the use of an SDK

**C.** It obtains MIBs from each vendor that details the APIs available.

**D.** It imports available APIs for the non-Cisco device in a CSV format.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 54**

How does SSO work with HSRP to minimize network disruptions?

**A.** It enables HSRP to elect another switch in the group as the active HSRP switch.

**B.** It ensures fast failover in the case of link failure.

**C.** It enables data forwarding along known routes following a switchover, white the routing protocol reconverges.

**D.** It enables HSRP to failover to the standby RP on the same device.

**Answer: (SHOW ANSWER)**

SSO enables the standby RP to take over if the active RP fails.

**NEW QUESTION: 55**

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

**A.** it determines if the hardware Is compatible to form the StackWise Virtual domain.

**B.** It determines which switch becomes active or standby.

**C.** It discovers the StackWise domain and brings up SVL interfaces.

**D.** It rejects any unidirectional link traffic forwarding.

**Answer: (SHOW ANSWER)**

The Link Management Protocol (LMP) is activated on each link of the StackWise Virtual links as soon as the links are established. LMP ensure the integrity of SVL links and monitors and maintains the health of the links. The redundancy role of each switch is resolved by the StackWise Discovery Protocol (SDP). It ensures that the hardware and software versions are compatible to form the SVL and determines which switch becomes active or standby from a control plane perspective.

**NEW QUESTION: 56**

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

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

Which action reduces the user impact?

**A.** increase the AP heartbeat timeout

**B.** increase BandSelect

**C.** enable coverage hole detection

**D.** increase the dynamic channel assignment interval

**Answer: (SHOW ANSWER)**
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.

**NEW QUESTION: 57**
What is used to validate the authenticity of the client and is sent in HTTP requests as a JSON object?
**A.** SSH
**B.** HTTPS
**C.** JVVT
**D.** TLS
**Answer: (SHOW ANSWER)**
https://developer.atlassian.com/server/crowd/json-requests-and-responses/

**NEW QUESTION: 58**
Refer to the exhibit.
(YOUR CONNECTION IS NOT PRIVATE WARNING )
An engineer is designing a guest portal on Cisco ISE using the default configuration. During the testing phase, the engineer receives a warning when displaying the guest portal. Which issue is occurring?
**A.** The server that is providing the portal has a self-signed certificate
**B.** The connection is using an unsupported protocol
**C.** The connection is using an unsupported browser
**D.** The server that is providing the portal has an expired certificate
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 59**
An engineer uses the Design workflow to create a new network infrastructure in Cisco DNA Center. How is the physical network device hierarchy structured?
**A.** by location
**B.** by role
**C.** by organization
**D.** by hostname naming convention
**Answer: (SHOW ANSWER)**


**NEW QUESTION: 60**

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

**A.** VSPAN

**B.** IPSPAN

**C.** RSPAN

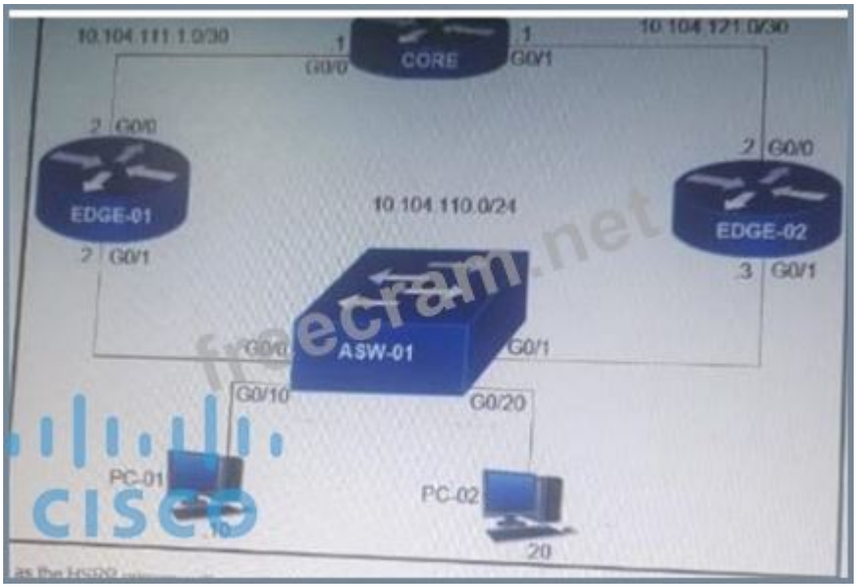
**D.** ERSPAN

**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 61**

Refer to the exhibit.




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

**A.** standby 10 priority

**B.** standby 10 preempt

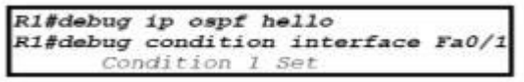
**C.** standby 10 timers

**D.** standby 10 track

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 62**

Refer to the exhibit.




Which statement about the OPSF debug output is true?

**A.** The output displays all OSPF messages which router R1 has sent to received on interface Fa0/1.

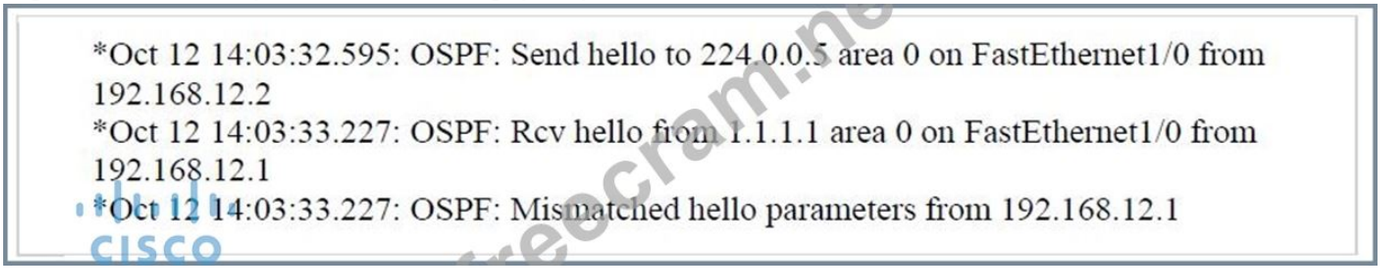
**B.** The output displays all OSPF messages which router R1 has sent or received on all interfaces.

**C.** The output displays OSPF hello messages which router R1 has sent received on interface Fa0/1.

**D.** The output displays OSPF hello and LSACK messages which router R1 has sent or received.

**Answer: (SHOW ANSWER)**

This combination of commands is known as "Conditional debug" and will filter the debug output based on your conditions. Each condition added, will behave like an 'And' operator in Boolean logic. Some examples of the "debug ip ospf hello" are shown below:




**NEW QUESTION: 63**

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

**A.** adaptive R

**B.** 802.11V

**C.** 802.11k

**D.** over the DS

**Answer: A (LEAVE A REPLY)**

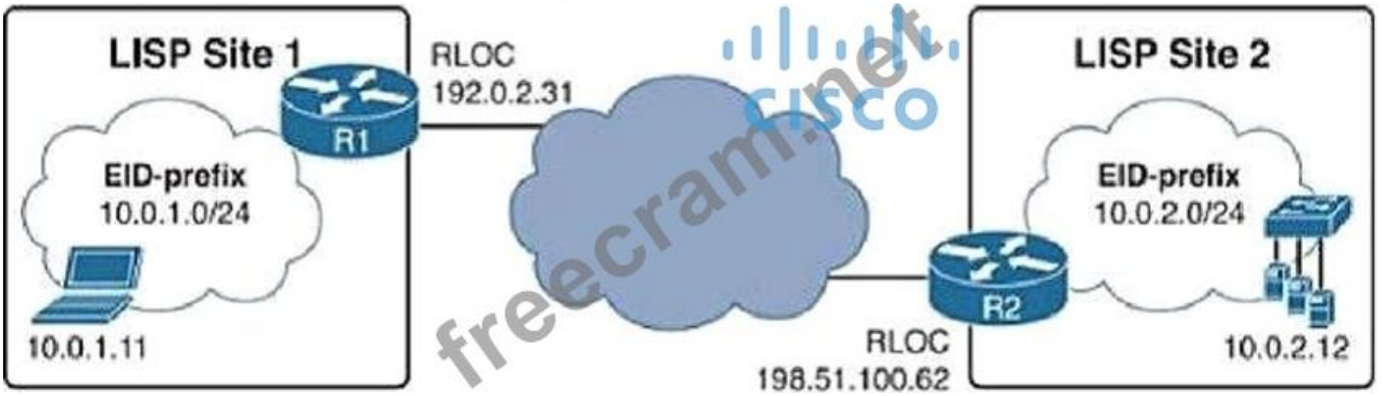
**NEW QUESTION: 64**

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

**A.** LISP learns the next hop

**B.** OTP uses LISP encapsulation to obtain routes from neighbors

**C.** OTP uses LISP encapsulation for dynamic multipoint tunneling
**D.** OTP maintains the LISP control plane
**Answer: (SHOW ANSWER)**
The EIGRP Over the Top solution can be used to ensure connectivity between disparate EIGRP sites. This feature uses EIGRP on the control plane and Locator ID Separation Protocol (LISP) encapsulation on the data plane to route traffic across the underlying WAN architecture. EIGRP is used to distribute routes between customer edge (CE) devices within the network, and the traffic forwarded across the WAN architecture is LISP encapsulated.
EIGRP OTP only uses LISP for the data plane, EIGRP is still used for the control plane.
Therefore we cannot say OTP uses LISP encapsulation for dynamic multipoint tunneling as this requires encapsulating both data and control plane traffic -> Answer 'OTP uses LISP encapsulation for dynamic multipoint tunneling' is not correct.
In OTP, EIGRP serves as the replacement for LISP control plane protocols (therefore EIGRP will learn the next hop, not LISP -> Answer 'LISP learns the next hop' is not correct). Instead of doing dynamic EID-to-RLOC mappings in native LISP-mapping services, EIGRP routers running OTP over a service provider cloud create targeted sessions, use the IP addresses provided by the service provider as RLOCs, and exchange routes as EIDs. Let's take an example:




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

**NEW QUESTION: 65**

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

**A.** MR

**B.** PITR

**C.** ALT

**D.** MS

**E.** PETR

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 66**

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

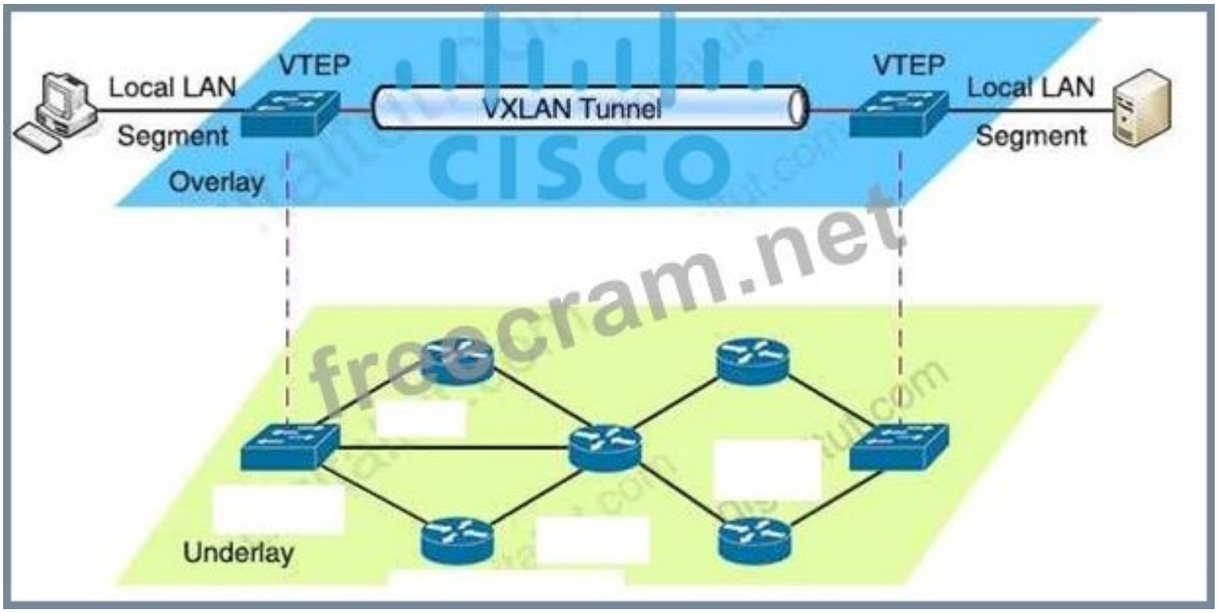
**C.** encapsulating and de-encapsulating VXLAN Ethernet frames

**D.** tunneling traffic from IPv4 to IPv6 VXLANs

**Answer: (SHOW ANSWER)**

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

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




**NEW QUESTION: 67**

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

**A.** DHCP

**B.** VXLAN

**C.** SXP

**D.** LISP

**Answer: (SHOW ANSWER)**

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

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

**NEW QUESTION: 68**

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

**A.** uses flexible NetFlow

**B.** classifies traffic based on advanced application recognition

**C.** assigns a VLAN to the endpoint

**D.** classifies traffic based an the contextual identity of the endpoint rather than its IP address

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 69**

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.

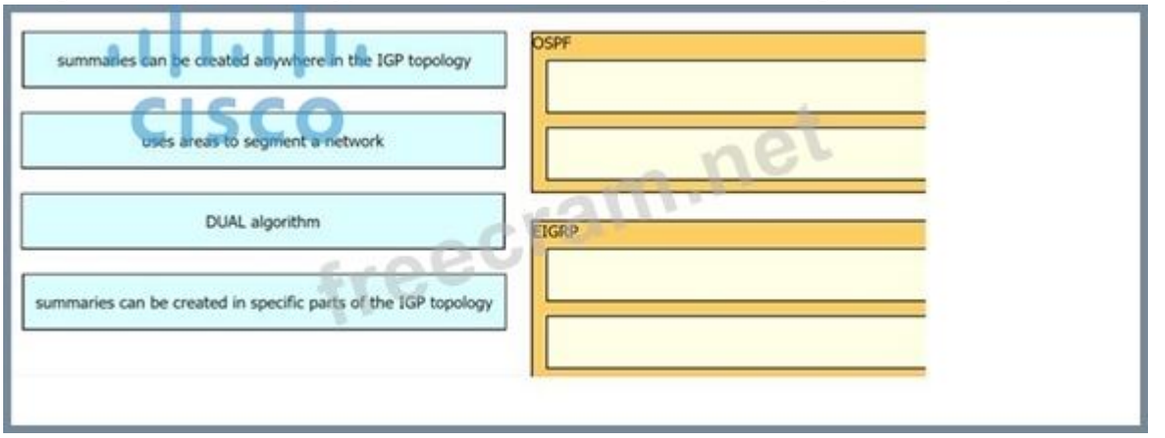
**D.** It manages the data plane.

**Answer: (SHOW ANSWER)**

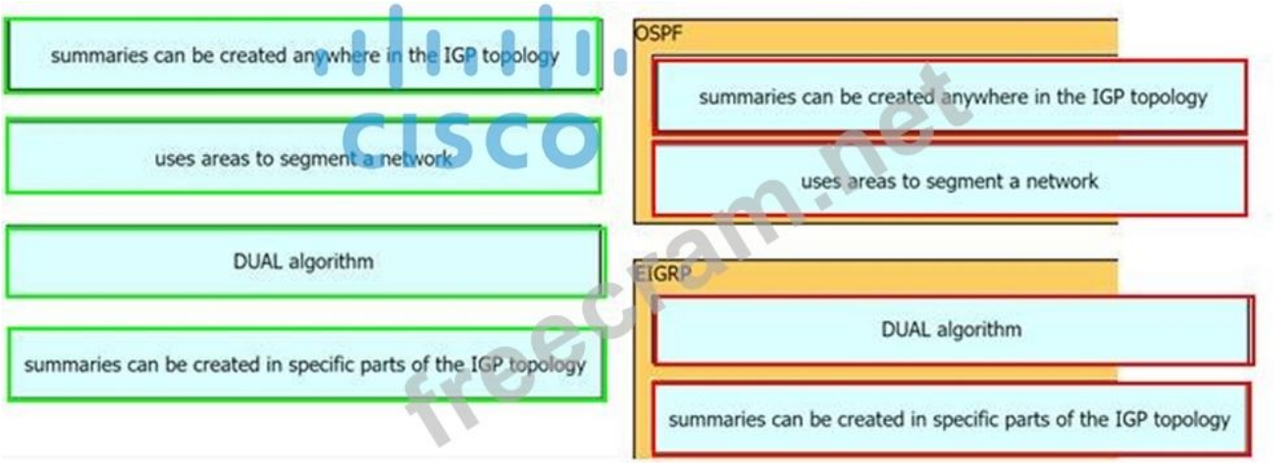
Control plane (vSmart) builds and maintains the network topology and make decisions on the traffic flows. The vSmart controller disseminates control plane information between WAN Edge devices, implements control plane policies and distributes data plane policies to network devices for enforcement.

**NEW QUESTION: 70**

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




**Answer:**




**NEW QUESTION: 71**
How does the EIGRP metric differ from the OSPF metric?
**A.** The EIGRP metric is calculated based on bandwidth only. The OSPF metric is calculated on delay only.
**B.** The EIGRP metric is calculated based on delay only. The OSPF metric is calculated on bandwidth and delay.
**C.** The EIGRP metric Is calculated based on bandwidth and delay. The OSPF metric is calculated on bandwidth only.
**D.** The EIGRP metric Is calculated based on hop count and bandwidth. The OSPF metric is calculated on bandwidth and delay.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 72**
Refer to the exhibit.

```
line vty 0 4
 session-timeout 30
 exec-timeout 120 0
 session-limit 30
 login local
line vty 5 15
 session-timeout 30
 exec-timeout 30 0
 session-limit 30
 login local
```

Only administrators from the subnet 10.10.10.0/24 are permitted to have access to the router. A secure protocol must be used for the remote access and management of the router instead of clear-text protocols. Which configuration achieves this goal?

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

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



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

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



**A.** Option A

**B.** Option B

**C.** Option C

**D.** Option D

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 73**

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

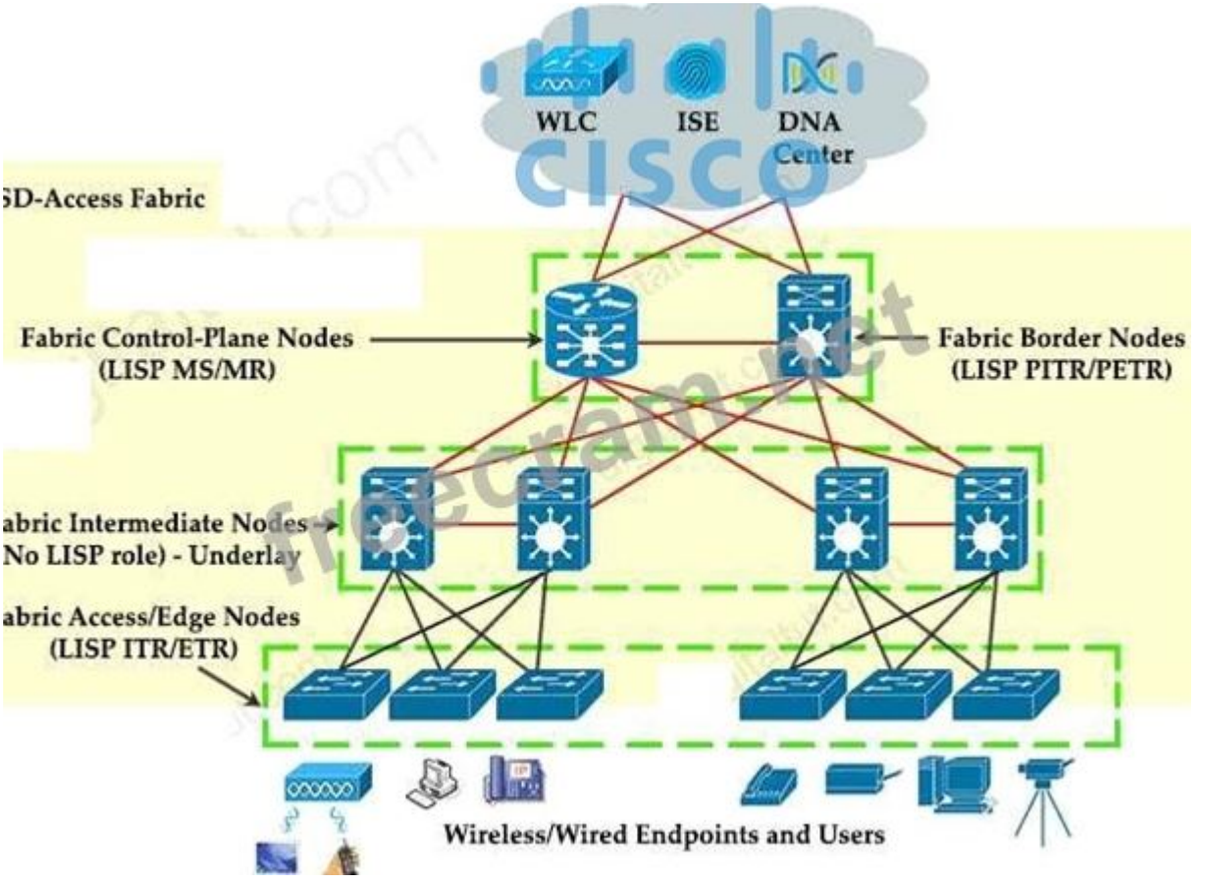
**B.** to connect wired endpoint to the SD-Access fabric

**C.** to advertise fabric IP address space to external network

**D.** to connect the fusion router to the SD-Access fabric

**Answer: B (LEAVE A REPLY)**

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




**NEW QUESTION: 74**
Which characteristic distinguishes Ansible from Chef?
**A.** Ansible uses Ruby to manage configurations. Chef uses YAML to manage configurations.
**B.** The Ansible server can run on Linux, Unix or Windows. The Chef server must run on Linux or Unix.
**C.** Ansible lacs redundancy support for the master server. Chef runs two masters in an active/active mode.
**D.** Ansible pushes the configuration to the client. Chef client pulls the configuration from the server.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 75**
Witch two actions provide controlled Layer 2 network connectivity between virtual machines running on the same hypervisor? (Choose two.)
**A.** Use a single trunk link to an external Layer2 switch.
**B.** Use a virtual switch running as a separate virtual machine.
**C.** Use VXLAN fabric after installing VXLAN tunneling drivers on the virtual machines.
**D.** Use a single routed link to an external router on stick.
**E.** Use a virtual switch provided by the hypervisor.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 76**
What is the function of the fabric control plane node In a Cisco SD-Access deployment?
**A.** It holds a comprehensive database that tracks endpoints and networks in the fabric.
**B.** It is responsible for policy application and network segmentation in the fabric.
**C.** It provides Integration with legacy nonfabric-enabled environments.
**D.** It performs traffic encapsulation and security profiles enforcement in the fabric.
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 77**
Refer to the exhibit.


Which two statements about the EEM applet configuration are true? (Choose two.)
**A.** The EEM applet runs after the CLI command is executed
**B.** The running configuration is displayed only if the letter Y is entered at the CLI
**C.** The EEM applet runs before the CLI command is executed
**D.** The EEM applet requires a case-insensitive response
**Answer: (SHOW ANSWER)**
When you use the sync yes option in the event cli command, the EEM applet runs before the CLI command is executed. The EEM applet should set the _exit_status variable to indicate whether the CLI command should be executed (_exit_status set to one) or not (_exit_status set to zero). With the sync no option, the EEM applet is executed in background in parallel with the CLI command.

**NEW QUESTION: 78**
Refer to the exhibit.


An engineer must block all traffic from a router to its directly connected subnet 209.165.200.0/24. The engineer applies access control list EGRESS in the outbound direction on the GigabitEthernet0/0 interface of the router However, the router can still ping hosts on the 209.165.200.0/24 subnet. Which explanation of this behavior is true?

**A.** 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.

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

**C.** Only standard access control lists can block traffic from a source IP address.

**D.** The access control list must contain an explicit deny to block traffic from the router.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 79**

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: (SHOW ANSWER)**

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

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

Answer 'security group tag ACL assigned to each router on a network' is not correct either as it says "assigned to each router").

**NEW QUESTION: 80**
Which JSON syntax is valid?

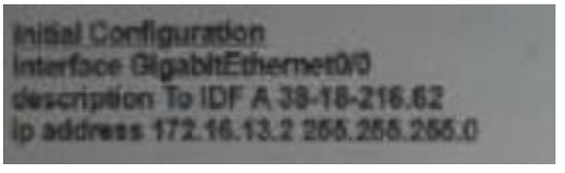

**A.** Option A
**B.** Option B
**C.** Option C
**D.** Option D
**Answer: (SHOW ANSWER)**
This JSON can be written as follows:
{
'switch': {
'name': 'dist1',
'interfaces': ['gig1', 'gig2', 'gig3']
}
}

**NEW QUESTION: 81**
What is the main function of VRF-lite?
**A.** To connect different autonomous systems together to share routes
**B.** To route IPv6 traffic across an IPv4 backbone
**C.** To allow devices to use labels to make Layer 2 Path decisions
**D.** To segregate multiple routing tables on a single device
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 82**
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: (SHOW ANSWER)**
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
+ Flex Connect, formerly known as Hybrid Remote Edge AP (HREAP), mode: allows data traffic to be switched locally and not go back to the controller. The Flex Connect AP can perform standalone client authentication and switch VLAN traffic locally even when it's disconnected to the WLC (Local Switched). Flex Connect 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.

**NEW QUESTION: 83**
An engineer must configure interface GigabitEthernet0/0 for VRRP group 10. When the router has the highest priority in the group, it must assume the master role. Which command set must be added to the initial configuration to accomplish this task?




**A.** vrrp 10 ip 172.16.13.254
vrrp 10 preempt
**B.** standby 10 ip 172.16.13.254
standby 10 priority 120
**C.** vrrp group 10 ip 172.16.13 254.255.255.255.0
vrrp group 10 priority 120
**D.** standby 10 ip 172.16.13.254 255.255.255.0
standby 10 preempt
**Answer: (SHOW ANSWER)**
By default, a preemptive scheme is enabled. A backup high-priority virtual router that becomes available takes over for the backup virtual router that was elected to become the virtual router master.

**NEW QUESTION: 84**

Based on this interface configuration, what is the expected state of OSPF adjacency?

```
R1:
interface GigabitEthernet0/1
 ip address 192.0.2.1 255.255.255.252
 ip ospf 1 area 0
 ip ospf hello-interval 2
 ip ospf cost 1
end

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



**A.** Full on both routers

**B.** not established

**C.** 2WAY/DROTHER on both routers

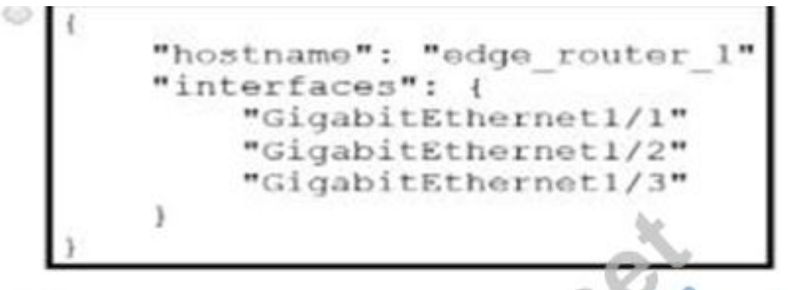
**D.** FULL/BDR on R1 and FULL/BDR on R2

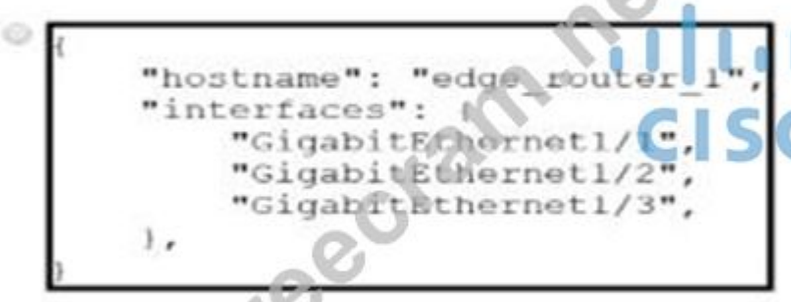
**Answer: (SHOW ANSWER)**

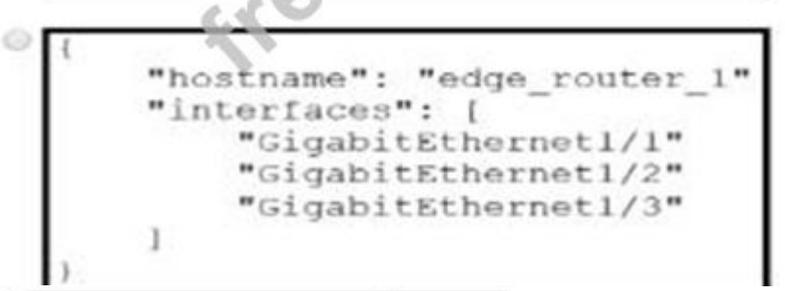
On Ethernet interfaces the OSPF hello intervl is 10 second by default so in this case there would be a Hello interval mismatch -> the OSPF adjacency would not be established.

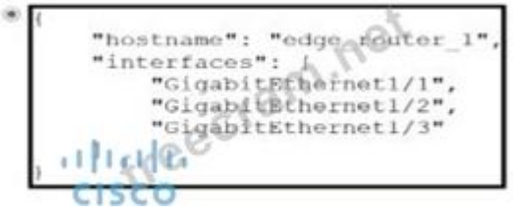
**NEW QUESTION: 85**

Which exhibit displays a valid JSON file?




**A.** Option A

**B.** Option D

**C.** Option C

**D.** Option B

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 86**

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

**A.** CDP

**B.** SNMP

**C.** LLDP

**D.** ping

**E.** NETCONF

**F.** a specified range of IP addresses

**Answer: (SHOW ANSWER)**

There are three ways for you to discover devices:

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

**NEW QUESTION: 87**

Which PAgP mode combination prevents an Etherchannel from forming?

**A.** auto/auto

**B.** desirable/desirable

**C.** auto/desirable

**D.** desirable

**Answer: (SHOW ANSWER)**

There are two PAgP modes:

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

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

| PAgP | Desirable | Auto |
|---|---|---|
| **Desirable** | Yes | Yes |
| **Auto** | Yes | **No** |

**NEW QUESTION: 88**

Refer to the exhibit.

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

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

What are two effects of this configuration? (Choose two.)

**A.** If R1 goes down, R2 becomes active but reverts to standby when R1 comes back online.

**B.** R1 becomes the active router.

**C.** If R2 goes down, R1 becomes active but reverts to standby when R2 comes back online.

**D.** R1 becomes the standby router.

**E.** If R1 goes down. R2 becomes active and remains the active device when R1 comes back online.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 89**

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

**A.** body

**B.** HTTP method

**C.** URI

**D.** header

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 90**

Which QoS mechanism will prevent a decrease in TCP performance?

**A.** Shaper

**B.** Rate-Limit

**C.** Policer

**D.** Fair-Queue

**E.** WRED

**F.** LLQ

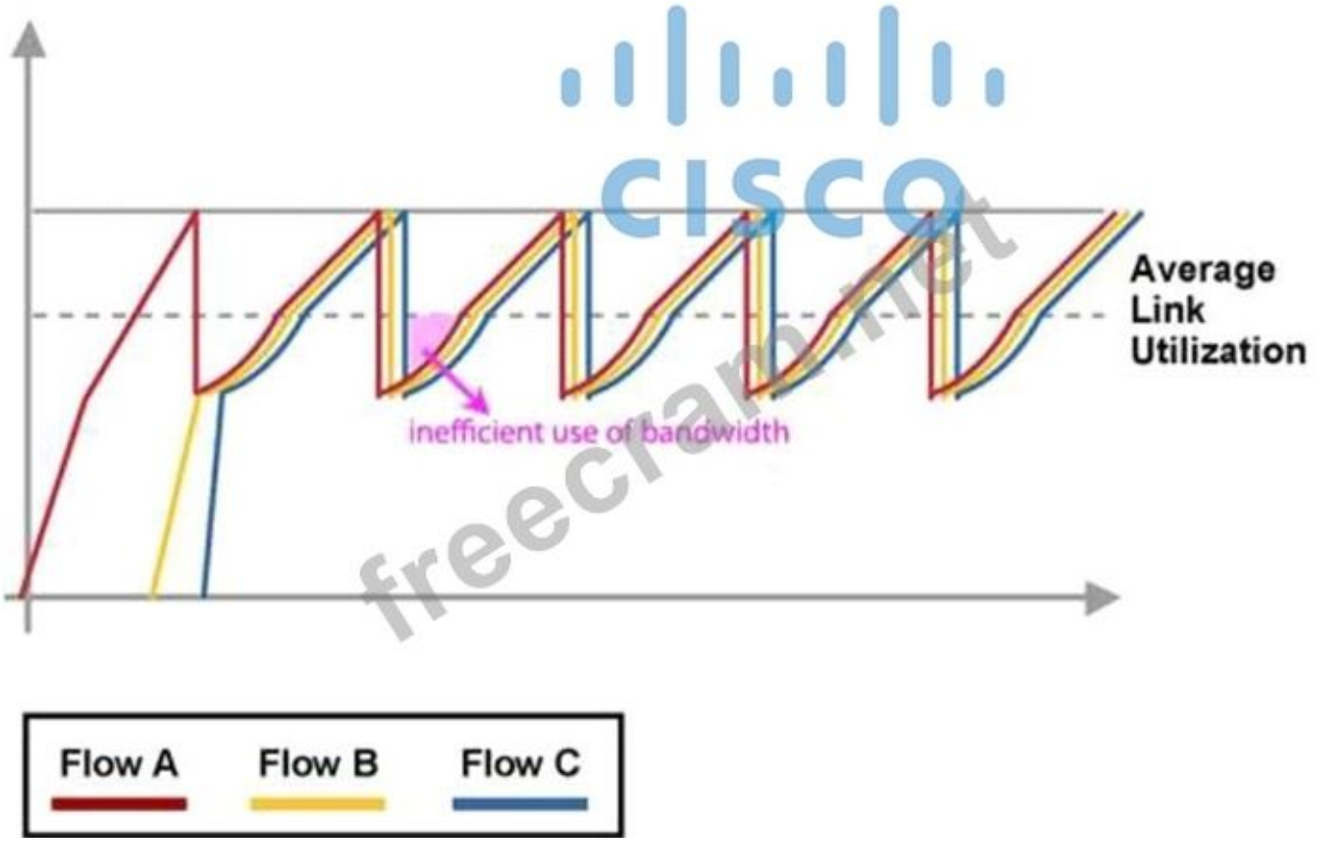
Explanation

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

The average queue size is calculated.

2. If the average is less than the minimum queue threshold, the arriving packet is queued.

3. If the average is between the minimum queue threshold for that type of traffic and the maximum threshold for the interface, the packet is either dropped or queued, depending on the packet drop probability for that type of traffic.
4. If the average queue size is greater than the maximum threshold, the packet is dropped.
WRED reduces the chances of tail drop (when the queue is full, the packet is dropped) by selectively dropping packets when the output interface begins to show signs of congestion (thus it can mitigate congestion by preventing the queue from filling up). By dropping some packets early rather than waiting until the queue is full, WRED avoids dropping large numbers of packets at once and minimizes the chances of global synchronization. Thus, WRED allows the transmission line to be used fully at all times.
WRED generally drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, the higher the priority of a packet, the higher the probability that the packet will be delivered.
**Answer: (SHOW ANSWER)**
Reference:
mt/qos-conavd-15-mt-book/qos-conavd-cfg-wred.html
WRED is only useful when the bulk of the traffic is TCP/IP traffic. With TCP, dropped packets indicate congestion, so the packet source will reduce its transmission rate. With other protocols, packet sources may not respond or may resend dropped packets at the same rate. Thus, dropping packets does not decrease congestion.
16/qos-conavd-xe-16-book/qos-conavd-oview.html
Note: Global synchronization occurs when multiple TCP hosts reduce their transmission rates in response to congestion. But when congestion is reduced, TCP hosts try to increase their transmission rates again simultaneously (known as slow-start algorithm), which causes another congestion. Global synchronization produces this graph:

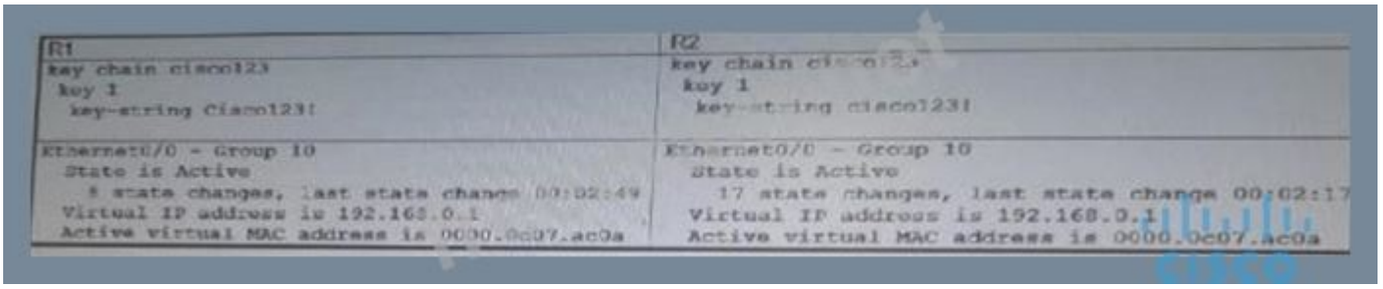



**NEW QUESTION: 91**
Which component of the Cisco Cyber Threat Defense solution provides user and flow context analysis?
**A.** Cisco Firepower and FireSIGHT
**B.** Cisco Stealth watch system
**C.** Advanced Malware Protection
**D.** Cisco Web Security Appliance
**Answer: B (LEAVE A REPLY)**
The goal 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:
/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf



**NEW QUESTION: 92**
Refer to the exhibit.




An engineer is installing a new pair of routers in a redundant configuration. Which protocol ensures that traffic is not disrupted in the event of a hardware failure?
**A.** HSRPv2
**B.** VRRP
**C.** HSRPv1
**D.** GLBP
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 93**
Which data modeling language is commonly used by NETCONF?
**A.** REST
**B.** YANG
**C.** HTML
**D.** XML
**Answer: (SHOW ANSWER)**
Cisco IOS XE supports the Yet Another Next Generation (YANG) data modeling language. YANG can be used with the Network Configuration Protocol (NETCONF) to provide the desired solution of automated and programmable network operations. NETCONF(RFC6241) is an XML-based protocol that client applications use to request information from and make configuration changes to the device. YANG is primarily used to model the configuration and state data used by NETCONF operations.
Reference:
6-5/configuration_guide/prog/b_165_prog_9500_cg/data_models.pdf

**NEW QUESTION: 94**
Which feature is supported by EIGRP but is not supported by OSPF?
**A.** equal-cost load balancing
**B.** route filtering
**C.** unequal-cost load balancing
**D.** route summarization
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 95**
In an SD-WAN deployment, which action in the vSmart controller responsible for?
**A.** handle, maintain, and gather configuration and status for nodes within the SD-WAN fabric
**B.** distribute policies that govern data forwarding performed within the SD-WAN fabric
**C.** gather telemetry data from vEdge routers
**D.** onboard vEdge nodes into the SD-WAN fabric
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 96**
What is the difference between CEF and process switching?
**A.** CEF processes packets that are too complex for process switching to manage.
**B.** CEF is more CPU-intensive than process switching.
**C.** CEF uses the FIB and the adjacency table to make forwarding decisions, whereas process switching punts each packet.
**D.** Process switching is faster than CEF.
**Answer: C (LEAVE A REPLY)**

CEF uses a FIB to make IP destination prefix-based switching decisions.