Refer to the exhibit. Which JSON syntax is derived from this data?

- {[{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': ['Running', 'Video games']}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': ['Napping', 'Reading']}]}
- {'Person': [{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': 'Running', 'Video games'}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': 'Napping', 'Reading'}]}
- {[{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': 'Running', 'Hobbies': 'Video games'}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': 'Napping', 'Hobbies': 'Reading'}]}
- {'Person': [{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': ['Running', 'Video games']}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': ['Napping', 'Reading']}]}

```
Router#show running-config | section line vty
line vty 0 4
 login local
line vty 5 15
 login local
!
Router#show running-config | include username
username cisco secret 5 $1$cM67$v7NQK0g2BGit77x88U1/00
```

Refer to the exhibit. Which action automatically enables privilege exec mode when logging in via SSH?

- Configure a password under the line configuration.
- Configure privilege level 15 under the line configuration.
- Configure the enable secret to be the same as the secret for user "Cisco".
- Configure user "cisco" with privilege level 15.

This is new question you can check the answer for this question

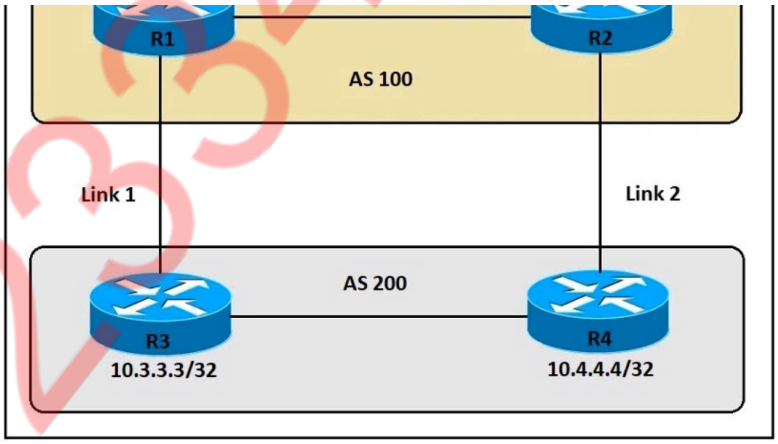
Which AP mode allows an engineer to scan configured channels for rogue access points?

- sniffer
- monitor
- bridge
- local

```
Router#sh run | b vty
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
```

Refer to the exhibit. Security policy requires all idle exec sessions to be terminated in 600 seconds. Which configuration achieves this goal?

- **line vty 0 15**
  exec-timeout 10 0
- **line vty 0 15**
  absolute-timeout 600
- **line vty 0 15**
  no exec-timeout
- **line vty 0 4**
  exec-timeout 600



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 accomplishes this task?

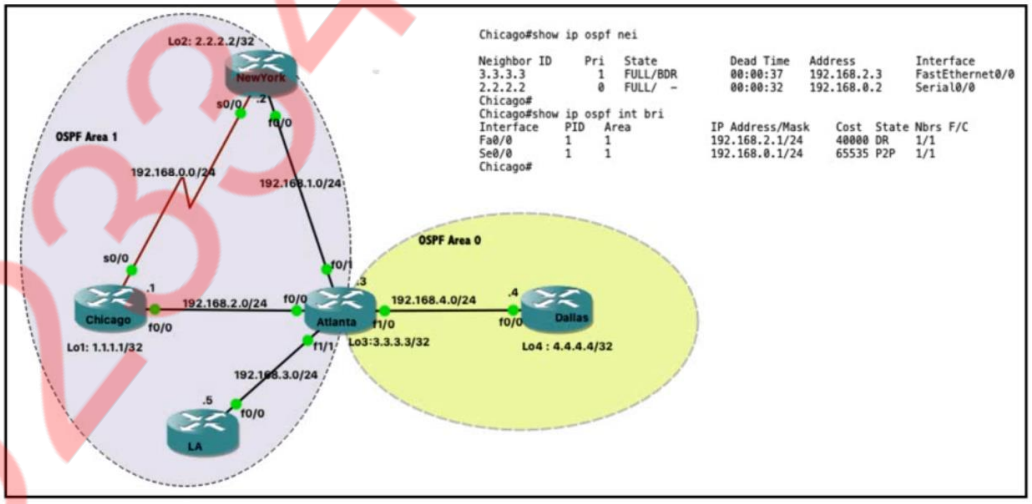
- R4(config-router)**neighbor 10.2.2.2 weight 200**
- R3(config-router)**neighbor 10.1.1.1 weight 200**
- R3(config-router)**bgp default local-preference 200**
- R4(config-router)**bgp default local-preference 200**

How does the RIB differ from the FIB?

- The RIB is used to create network topologies and routing tables. The FIB is a list of routes to particular network destinations.
- The FIB maintains network topologies and routing tables. The RIB is a list of routes to particular network destinations.
- [x] The RIB includes many routes to the same destination prefix. The FIB contains only the best route.
- The FIB includes many routes to a single destination. The RIB is the best route to a single destination.

What is one benefit of implementing a VSS architecture?

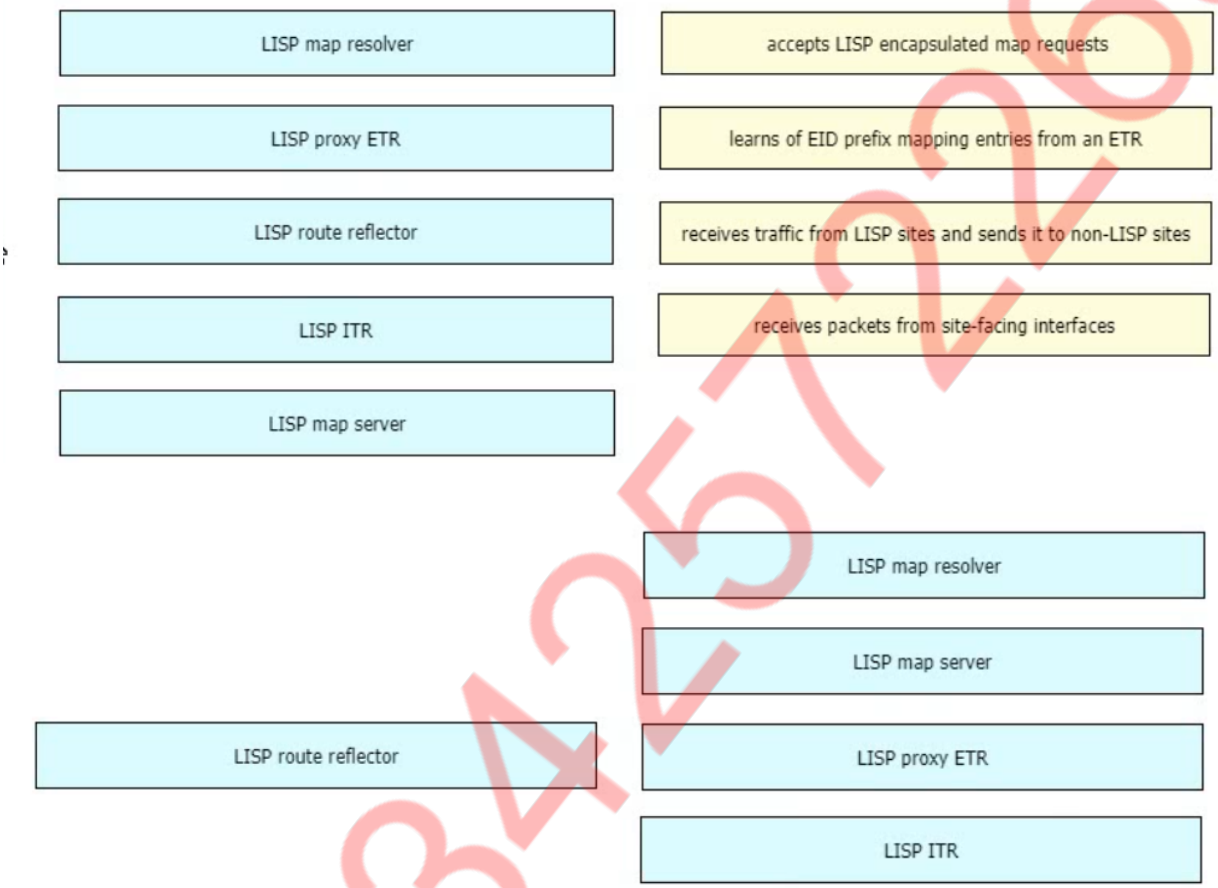
- [x] It provides a single point of management for improved efficiency.
- It uses a single database to manage configuration for multiple switches.
- It provides multiple points of management for redundancy and improved support.
- It uses GLBP to balance traffic between gateways.



Refer to the exhibit. Which router is the designated router on the segment 192.168.0.0/24?

- Router Chicago because it has a lower router ID.
- This segment has no designated router because it is a nonbroadcast network type.
- [x] This segment has no designated router because it is a p2p network type.
- Router NewYork because it has a higher router ID.

Drag and drop the LISP components from the left onto the functions they perform on the right. Not all options are used.



Which measurement is used from a post wireless survey to depict the cell edge of the access points?

- SNR
- Noise
- RSSI
- CCI

"HTTP/1.1 204 No Content" is returned when the **curl -i -X DELETE** command is issued. Which situation has occurred?

- The object could not be located at the URI path.
- The command succeeded in deleting the object.
- The object was located at the URI, but it could not be deleted.
- The URI was invalid.

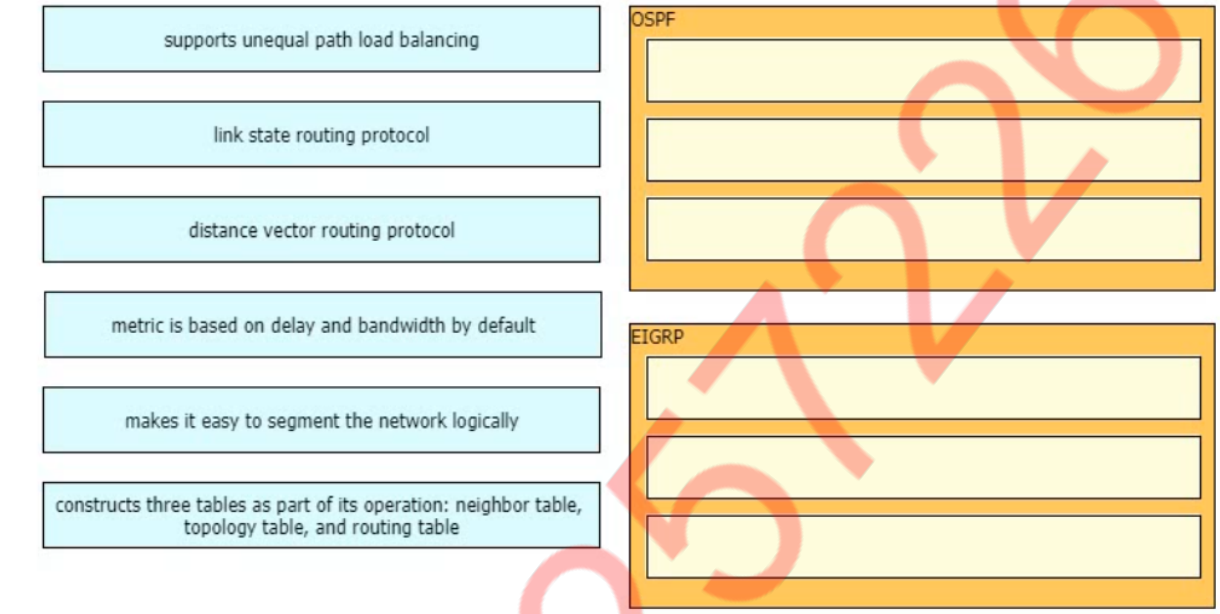
What is the difference between CEF and process switching?

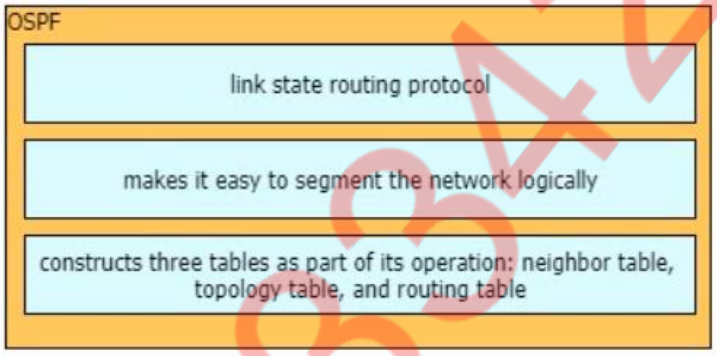
- Process switching is faster than CEF.
- CEF uses the FIB and the adjacency table to make forwarding decisions, whereas process switching punts each packet.
- CEF processes packets that are too complex for process switching to manage.
- CEF is more CPU-intensive than process switching.

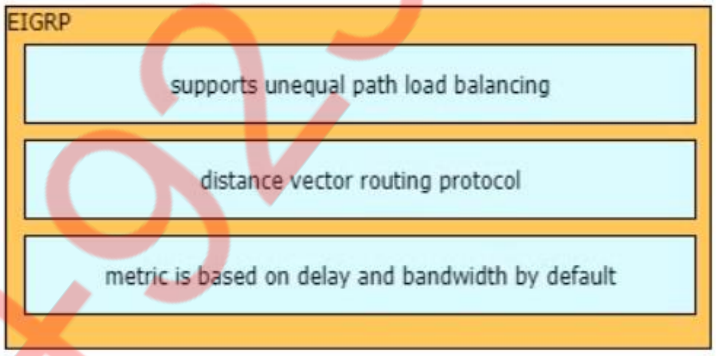
An engineer uses the Design workflow to create a new network infrastructure in Cisco DNA Center. How is the physical network device hierarchy structured?

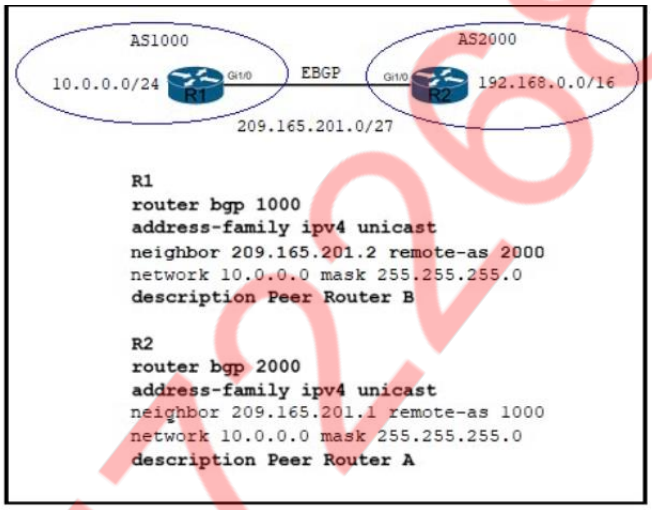
- by location
- by role
- by organization
- by hostname naming convention

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







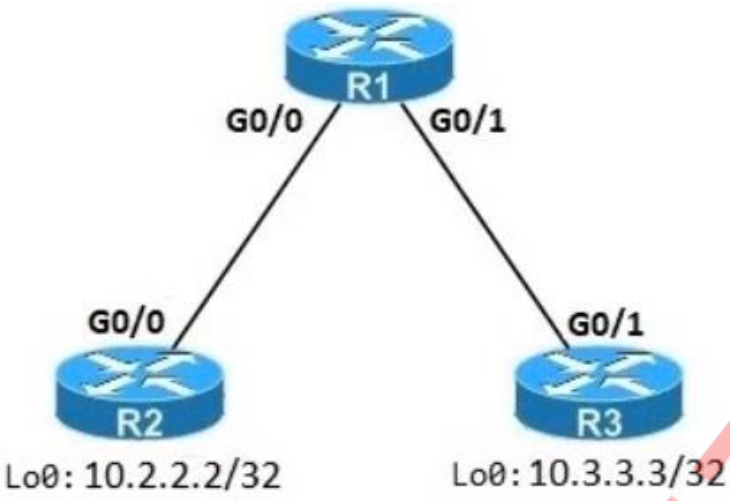


Refer to the exhibit. Which two commands are needed to allow for full reachability between AS 1000 and AS 2000? (Choose two.)

- [ ] R1
  no network 10.0.0.0 mask 255.255.255.0
- [ ] R1
  network 192.168.0.0 mask 255.255.0.0
- [x] R2
  network 209.165.201.0 mask 255.255.192.0
- [ ] R2
  network 192.168.0.0 mask 255.255.0.0
- [x] R2
  no network 10.0.0.0 mask 255.255.255.0

What are two benefits of YANG? (Choose two.)

- [ ] It enforces configuration semantics.
- [ ] It collects statistical constraint analysis information.
- [x] It enforces configuration constraints.
- [ ] It enables multiple leaf statements to exist within a leaf list.
- [x] It enforces the use of a specific encoding format for NETCONF.



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 set accomplishes this task?

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

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

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

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

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

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

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

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

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

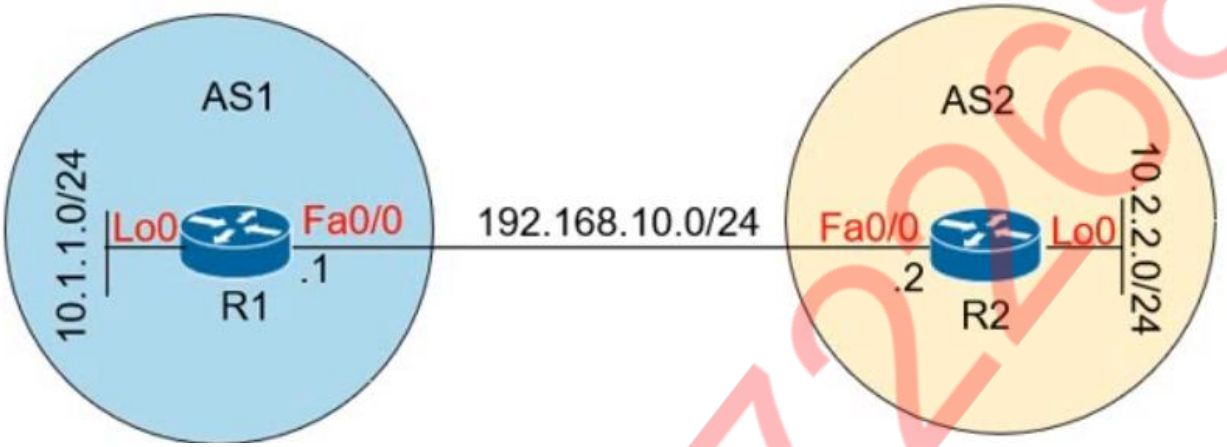
- R3(config)#**time-range WEEKEND**
  R3(config-time-range)#**periodic Saturday Sunday 00:00 to 23:59**

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

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

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

- Layer 3
- inter-xTR
- auto anchor
- fast roam



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?

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**

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**

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**

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**

Which encryption hashing algorithm does NTP use for authentication?

- SSL
- MD5
- AES128
- AES256

Which exhibit displays a valid JSON file?

```
{
    "hostname": "edge_router_1",
    "interfaces": [
        "GigabitEthernet1/1",
        "GigabitEthernet1/2",
        "GigabitEthernet1/3"
    ]
}
```

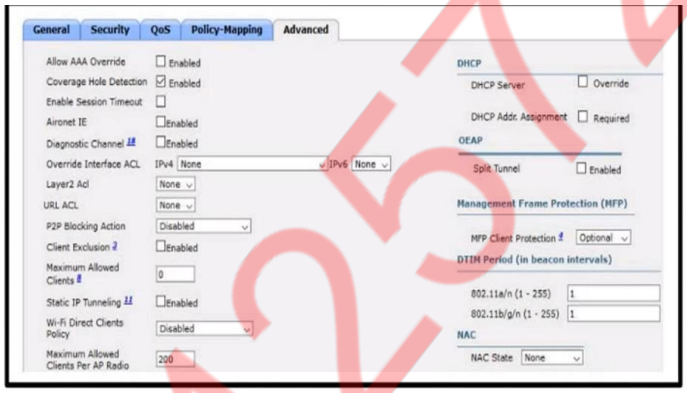
```
{
    "hostname": "edge_router_1"
    "interfaces": [
        "GigabitEthernet1/1"
        "GigabitEthernet1/2"
        "GigabitEthernet1/3"
    ]
}
```

```
{
    "hostname": "edge_router_1",
    "interfaces": {
        "GigabitEthernet1/1",
        "GigabitEthernet1/2",
        "GigabitEthernet1/3",
    },
}
```

```
{
    "hostname": "edge_router_1"
    "interfaces": {
        "GigabitEthernet1/1"
```

What is the function of the LISP map resolver?

- to send traffic to non-LISP sites when connected to a service provider that does not accept nonroutable EIDs as packet sources
- to connect a site to the LISP-capable part of a core network, publish the EID-to-RLOC mappings for the site, and respond to map-request messages
- to decapsulate map-request messages from ITRs and forward the messages to the MS
- to advertise routable non-LISP traffic from one address family to LISP sites in a different address family



Refer to the exhibit. An engineer is investigating why guest users are able to access other guest user devices when the users are connected to the customer guest WLAN. What action resolves this issue?

- implement Wi-Fi direct policy
- implement split tunneling
- implement P2P blocking
- implement MFP client protection

```
Switch2#
01:25:08: %PM-4-ERR_DISABLE: channel-misconfig error detected on
Fa0/23, putting Fa0/23 in err-disable
state
01:25:08: %PM-4-ERR_DISABLE: channel-misconfig error detected on
Fa0/24, putting Fa0/24 in err-disable
state
Switch2#


Switch1#show etherchannel summary

!output omitted

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------
1      Po2(SD)         LACP      Fa1/0/23(D)


Switch2#show etherchannel summary

!output omitted

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------
1      Po1(SD)           -        Fa0/23(D)   Fa0/24(D)
```

Refer to the exhibit. An engineer is configuring an EtherChannel between Switch1 and Switch2 and notices the console message on Switch2. Based on the output, which action resolves this issue?

- Configure the same EtherChannel protocol on both switches.
- Configure the same port channel interface number on both switches.
- Configure more member ports on Switch1.
- Configure less member ports on Switch2.

Which deployment option of Cisco NGFW provides scalability?

- inline tap
- high availability
- clustering
- tap

Which two threats does AMP4E have the ability to block? (Choose two.)

- [x] Microsoft Word macro attack
- [x] ransomware
- [ ] SQL injection
- [ ] DDoS
- [ ] email phishing

An engineer is troubleshooting the AP join process using DNS. Which FQDN must be resolvable on the network for the access points to successfully register to the WLC?

- wlchostname.domain.com
- cisco-capwap-controller.domain.com
- ap-manager.domain.com
- primary-wlc.domain.com

```
with manager.connect(host=192.168.0.1, port=22,
                     username='admin', password='password1', hostkey_verify=True,
                     device_params={'name':'nexus'}) as m:
```

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

- It opens a tunnel and encapsulates the login information, if the host key is correct.
- It creates an SSH connection using the SSH key that is stored, and the password is ignored.
- It opens an ncclient connection to a Cisco Nexus device and maintains it for the duration of the context.
- It creates a temporary connection to a Cisco Nexus device and retrieves a token to be used for API calls.

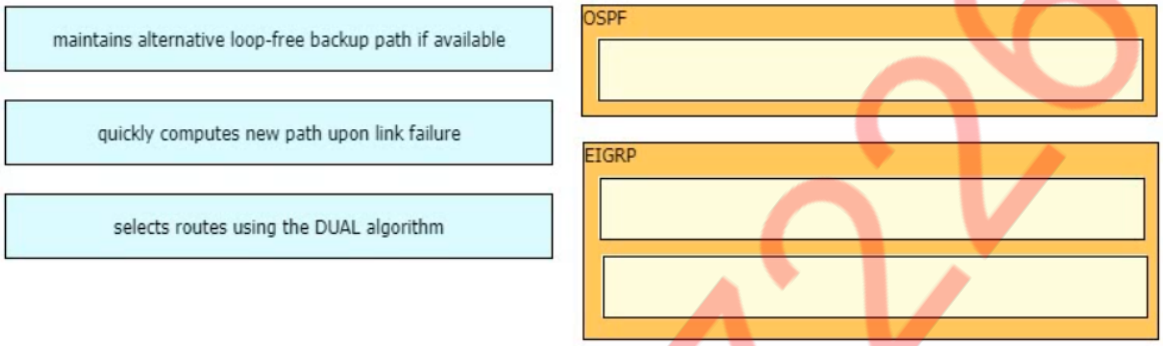
Which control plane protocol is used between Cisco SD-WAN routers and vSmart controllers?

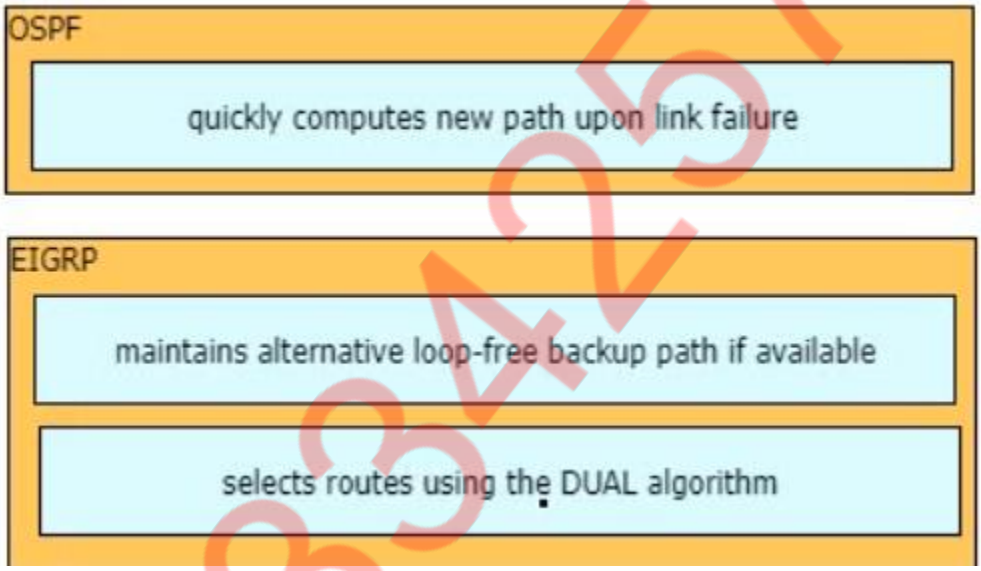
- TCP
- OMP
- UDP
- BGP

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

- It is used for HTTP and HTTPS requests.
- It is provided using NGINX acting as a proxy web server.
- It is not supported on Cisco devices.
- It requires certificates for authentication.

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





An engineer must configure an ACL that permits packets which include an ACK in the TCP header. Which entry must be included in the ACL?

- **access-list 10 permit ip any any eq 21 tcp-ack**
- **access-list 110 permit tcp any any eq 21 tcp-ack**
- **access-list 10 permit tcp any any eq 21 established**
- **access-list 110 permit tcp any any eq 21 established**

At which layer does Cisco DNA Center support REST controls?

- EEM applets or scripts
- northbound APIs
- YAML output from responses to API calls
- session layer

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

- classifies traffic based on the contextual identity of the endpoint rather than its IP address
- classifies traffic based on advanced application recognition
- assigns a VLAN to the endpoint
- uses flexible NetFlow

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

- **event manager applet ondemand**
  event register
  action 1.0 syslog priority critical msg 'This is a message from ondemand'
- **event manager applet ondemand**
  event none
  action 1.0 syslog priority critical msg 'This is a message from ondemand'
- **event manager applet ondemand**
  action 1.0 syslog priority critical msg 'This is a message from ondemand'
- **event manager applet ondemand**
  event manual
  action 1.0 syslog priority critical msg 'This is a message from ondemand'

```
Router#show ip ospf interface
GigabitEthernet0/1.40 is up, line protocol is up
  Internet Address 10.3.5.254/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.29, Interface address 10.3.5.254
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 172.16.30.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.29, Interface address 172.16.30.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 172.16.11.29/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 172.16.11.27, Interface address 172.16.11.27
  Backup Designated router (ID) 172.16.11.30, Interface address 172.16.11.30
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
```

Refer to the exhibit. A network engineer configures OSPF and reviews the router configuration. Which interface or interfaces are able to establish OSPF adjacency?

- only GigabitEthernet0/1
- only GigabitEthernet0/0
- GigabitEthernet0/0 and GigabitEthernet0/1
- GigabitEthernet0/1 and GigabitEthernet0/1.40

How are the different versions of IGMP compatible?

- IGMPv2 is compatible only with IGMPv2.
- IGMPv3 is compatible only with IGMPV1.
- IGMPv2 is compatible only with IGMPv1.
- IGMPv3 is compatible only with IGMPv3.

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

- **logging host 10.2.3.4 vrf mgmt transport tcp port 6514**
- **logging host 10.2.3.4 vrf mgmt transport udp port 6514**
- **logging host 10.2.3.4 vrf mgmt transport tcp port 514**
- **logging host 10.2.3.4 vrf mgmt transport udp port 514**

A server running Linux is providing support for virtual machines along with DNS and DHCP services for a small business. Which technology does this represent?

- container
- Type 2 hypervisor
- hardware pass-thru
- Type 1 hypervisor

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?

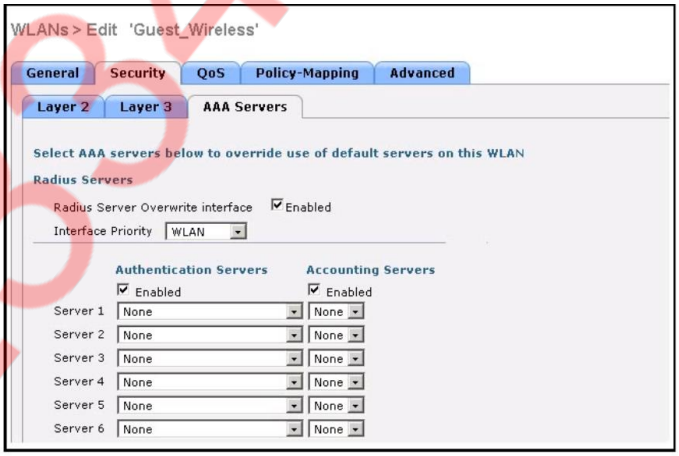
- RADIUS server
- ISE server
- local WLC
- anchor WLC

Which two results occur if Cisco DNA Center loses connectivity to devices in the SD-Access fabric? (Choose two.)

- [ ] All devices reload after detecting loss of connection to Cisco DNA Center.
- [ ] Already connected users are unaffected, but new users cannot connect.
- [ ] Users lose connectivity.
- [x] User connectivity is unaffected.
- [x] Cisco DNA Center is unable to collect monitoring data in Assurance.

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

- (•) It creates device packs through the use of an SDK.
- ( ) It uses an API call to interrogate the devices and register the returned data.
- ( ) It obtains MIBs from each vendor that details the APIs available.
- ( ) It imports available APIs for the non-Cisco device in a CSV format.



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

- ( ) any interface configured on the WLC
- (•) the interface specified on the WLAN configuration
- ( ) the controller management interface
- ( ) the controller virtual interface

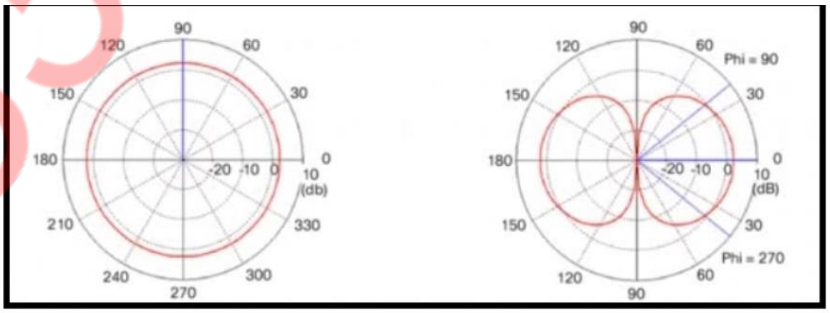
An engineer runs the code against an API of Cisco DNA Center, and the platform returns this output. What does the response indicate?

```
import requests
import sys
import urllib3

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

def main():
   device_uri = "https://192.168.1.1/dna/system/api/v1/auth/token"
   http_result = requests.get(device_uri, auth=("root", "test406225306!"))
   print(http_result)
   if http_result.status_code != requests.codes.ok:
      print("Call failed! Review get_token() . ")
      sys.exit()
   print(http_result.json()["Token"])

if _name_ == "_main_":
   sys.exit(main())
```

Output

```
$ python get_token.py
<Response [405]>
Call failed! Review get_token ().
```

- The authentication credentials are incorrect.
- The URI string is incorrect.
- The Cisco DNA Center API port is incorrect.
- The HTTP method is incorrect.



Refer to the exhibit. Which type of antenna is shown on the radiation patterns?

- patch
- omnidirectional
- Yagi
- dipole

```
Tunnel100 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.200.1/24
  MTU 17912 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive set (10 sec), retries 3
  Tunnel source 209.165.202.129 (GigabitEthernet0/1)
   Tunnel Subblocks:
     src-track:
        Tunnel100 source tracking subblock associated with GigabitEthernet0/1
         Set of tunnels with source GigabitEthernet0/1, 1 members (includes iterators), on interface <OK>
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
```

Refer to the exhibit. A network engineer configures a GRE tunnel and enters the **show interface tunnel** command. What does the output confirm about the configuration?

- (•) The tunnel mode is set to the default.
- ( ) Interface tracking is configured.
- ( ) The physical interface MTU is 1476 bytes.
- ( ) The keepalive value is modified from the default value.

What is one fact about Cisco SD-Access wireless network deployments?

- ( ) The WLC is part of the fabric underlay.
- ( ) The wireless client is part of the fabric overlay.
- (•) The access point is part of the fabric overlay.
- ( ) The access point is part of the fabric underlay.

An engineer is describing QoS to a client. Which two facts apply to traffic policing? (Choose two.)

- [x] Policing should be performed as close to the source as possible.
- [ ] Policing typically delays the traffic, rather than drops it.
- [x] Policing drops traffic that exceeds the defined rate.
- [ ] Policing adapts to network congestion by queuing excess traffic.
- [ ] Policing should be performed as close to the destination as possible.

```
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
```

Refer to the exhibit. An engineer must modify the access control list EGRESS to allow all IP traffic from subnet 10.1.10.0/24 to 10.1.2.0/24. The access control list is applied in the outbound direction on router interface GigabitEthernet 0/1. Which configuration command set will allow this traffic without disrupting existing traffic flows?

(•) 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

( ) config t
ip access-list extended EGRESS2
permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
permit ip 10.1.100.0 0.0.0.255 10.1.2.0 0.0.0.255
deny ip any any
!
interface g0/1
no ip access-group EGRESS out
ip access-group EGRESS2 out

( ) 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

( ) 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

What is the centralized control policy in a Cisco SD-WAN deployment?

( ) list of ordered statements that define user access policies

(•) set of statements that defines how routing is performed

( ) set of rules that governs nodes authentication within the cloud

( ) list of enabled services for all nodes within the cloud

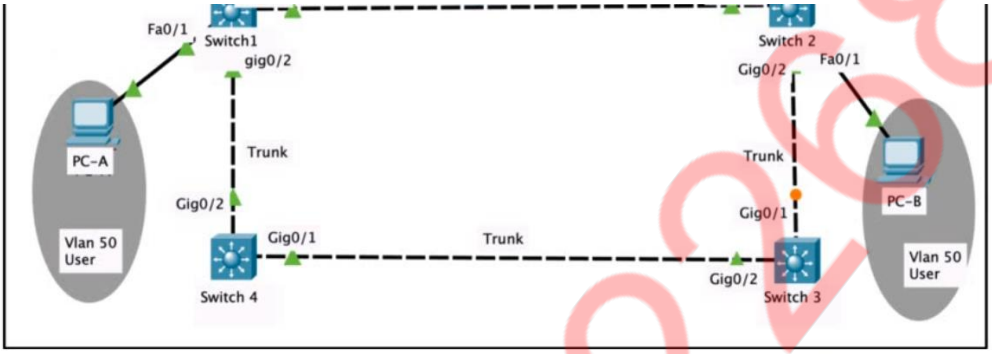
Which component of the Cisco Cyber Threat Defense solution provides user and flow context analysis?

( ) Cisco Firepower and FireSIGHT

(•) Cisco Stealthwatch system

( ) Advanced Malware Protection

( ) Cisco Web Security Appliance



Refer to the exhibit. Rapid PVST+ is enabled on all switches. Which command set must be configured on Switch1 to achieve the following results on port fa0/1?

- When a device is connected, the port transitions immediately to a forwarding state.
- The interface should not send or receive BPDUs.
- If a BPDU is received, it continues operating normally.

○ Switch1(config)# **interface f0/1**
Switch1(config-if)# **spanning-tree portfast**
Switch1(config-if)# **spanning-tree bpduguard enable**

◉ Switch1(config)# **spanning-tree portfast bpdufilter default**
Switch1(config)# **interface f0/1**
Switch1(config-if)# **spanning-tree portfast**

○ Switch1(config)# **spanning-tree portfast bpduguard default**
Switch1(config)# **interface f0/1**
Switch1(config-if)# **spanning-tree portfast**

○ Switch1(config)# **interface f0/1**
Switch1(config-if)# **spanning-tree portfast**

Which characteristic distinguishes Ansible from Chef?

○ The Ansible server can run on Linux, Unix or Windows. The Chef server must run on Linux or Unix.

○ Ansible uses Ruby to manage configurations. Chef uses YAML to manage configurations.

◉ Ansible pushes the configuration to the client. Chef client pulls the configuration from the server.

○ Ansible lacks redundancy support for the primary server. Chef runs two primary servers in active/active mode.

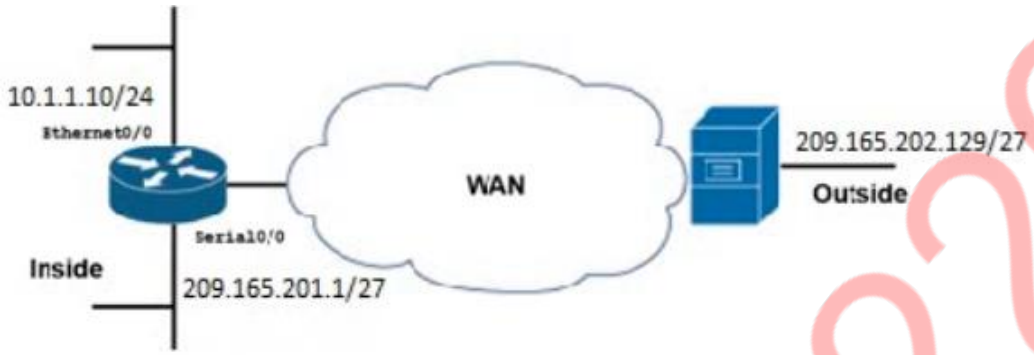
After a redundant route processor failure occurs on a Layer 3 device, which mechanism allows for packets to be forwarded from a neighboring router based on the most recent tables?

◉ NSF

○ RPVST+

○ BFD

○ RP failover




```
R1
interface Ethernet0/0
ip address 10.1.1.10 255.255.255.0
ip nat inside
!
interface Serial0/0
ip address 209.165.201.1 255.255.255.224
ip nat outside
!
ip nat pool Busi 209.165.201.1 209.165.201.2 netmask 255.255.255.252
ip nat inside source list 1 pool Busi
!
access-list 1 permit 10.1.1.0 0.0.0.255
!

R1# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 0 extended)
Outside interfaces:
Serial0/0
Inside interfaces:
Ethernet0/0
Hits: 119 Misses: 1
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool Busi refcount 1
pool fred: netmask 255.255.255.252
start 209.165.201.1 end 209.165.201.2
type generic, total addresses 2, allocated 1 (50%), misses 0
!
```

Refer to the exhibit. A network engineer configures NAT on R1 and enters the **show** command to verify the configuration. What does the output confirm?

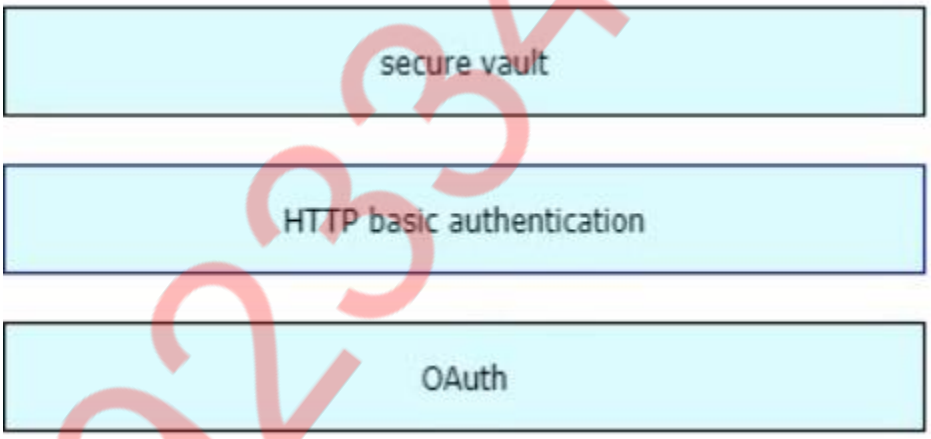
- A Telnet session from 160.1.1.1 to 10.1.1.10 has been initiated.
- R1 is configured with PAT overload parameters.
- R1 is configured with NAT overload parameters.
- The first packet triggered NAT to add an entry to the NAT table.

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

- (●) Option 43
- ( ) Option 60
- ( ) Option 67
- ( ) Option 150

Drag and drop the REST API authentication methods from the left onto their descriptions on the right.

HTTP basic authentication	public API resource
OAuth	username and password in an encoded string
secure vault	authorization through identity provider



```
event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.3 get-type next entry-op gt entry-val 80 poll-interval 5
!
action 1.0 cli command "enable"
action 2.0 syslog msg "high cpu"
action 3.0 cli command "term length 0"
```

Refer to the exhibit. An engineer must create a script that appends the output of the **show process cpu sorted** command to a file. Which action completes the configuration?

- **action 4.0 syslog command "show process cpu sorted | append flash:high-cpu-file"**
- **action 4.0 cli command "show process cpu sorted | append flash:high-cpu-file"**
- **action 4.0 cns-event "show process cpu sorted | append flash:high-cpu-file"**
- **action 4.0 publish-event "show process cpu sorted | append flash:high-cpu-file"**

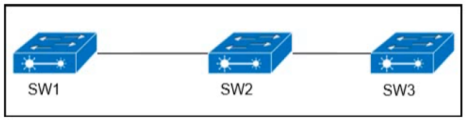
```
flow monitor FLOW-MONITOR-1
 record netflow ipv6 original-input
 exit
!
sampler SAMPLER-1
 mode deterministic 1 out-of 2
 exit
!
ip cef
ipv6 cef
!
interface GigabitEthernet 0/0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
!
```

Refer to the exhibit. What is the effect of introducing the sampler feature into the Flexible NetFlow configuration on the router?

- CPU and memory utilization are reduced when compared with what is required for full NetFlow.
- Every second IPv4 packet is forwarded to the collector for inspection.
- NetFlow updates to the collector are sent 50% less frequently.
- The resolution of sampling data increases, but it requires more performance from the router.

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

- RADIUS server
- PKI server
- NTP server
- TACACS server



Refer to the 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?

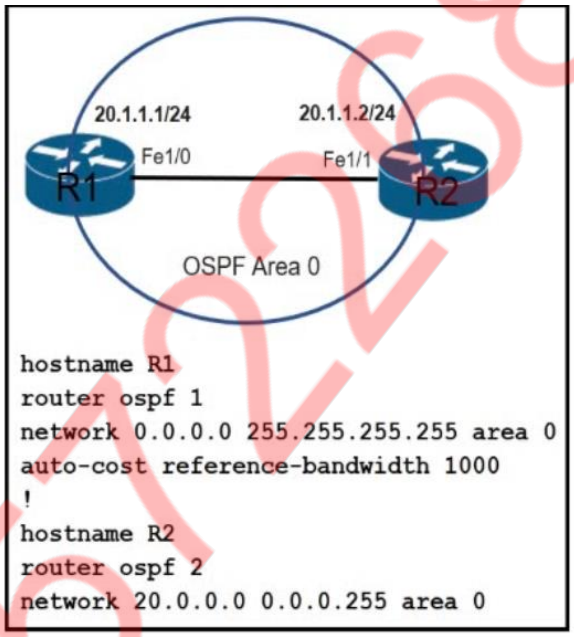
- SW1(config)#**vtp mode transparent**
- SW3(config)#**vtp mode transparent**
- SW2(config)#**vtp pruning**
- [x] SW1(config)#**vtp pruning**

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

- [ ] PUSH
- [ ] ADD
- [x] HEAD
- [ ] REMOVE
- [ ] PULL
- [x] PATCH

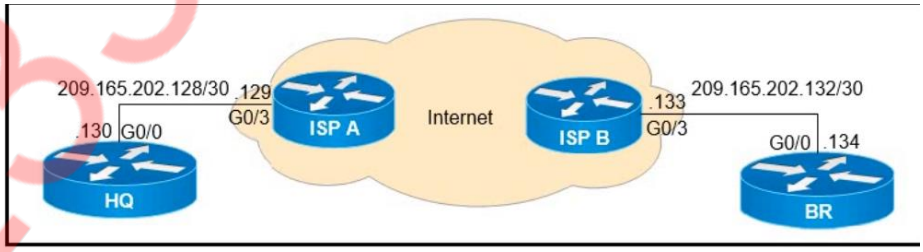
Which command set configures RSPAN to capture outgoing traffic from VLAN 3 on interface GigabitEthernet 0/3 while ignoring other VLAN traffic on the same interface?

- **monitor session 2 source interface gigabitethernet0/3 rx**
  monitor session 2 filter vlan 1 - 2 , 4 - 4094
- **monitor session 2 source interface gigabitethernet0/3 rx**
  monitor session 2 filter vlan 3
- **monitor session 2 source interface gigabitethernet0/3 tx**
  monitor session 2 filter vlan 1 - 2 , 4 - 4094
- [x] **monitor session 2 source interface gigabitethernet0/3 tx**
  monitor session 2 filter vlan 3



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

- **network 20.1.1.2 0.0.0.0 area 0**
- **network 20.0.0.2 0.0.0.3 area 0**
- **network 20.0.0.2 0.0.0.0 area 0**
- **network 20.1.1.0 0.0.0.0 area 0**



Refer to the exhibit. What is the effect of these commands on the BR and HQ tunnel interfaces?

BR(config)#interface tunnel1
BR(config-if)#keepalive 5 3

HQ(config)#interface tunnel1
HQ(config-if)#keepalive 5 3

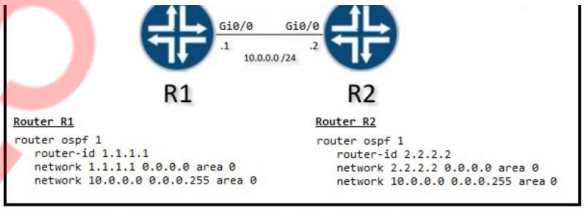
- The tunnel line protocol goes down when the keepalive counter reaches 5.
- The tunnel line protocol goes down when the keepalive counter reaches 6.
- The keepalives are sent every 3 seconds and 5 retries.
- The keepalives are sent every 5 seconds and 3 retries.

How do cloud deployments differ from on-premises deployments?

- Cloud deployments require less frequent upgrades than on-premises deployments
- Cloud deployments are more customizable than on-premises deployments.
- Cloud deployments require longer implementation times than on-premises deployments.
- Cloud deployments have lower upfront costs than on-premises deployments.

What function does VXLAN perform in a Cisco SD-Access deployment?

- policy plane forwarding
- control plane forwarding
- data plane forwarding
- systems management and orchestration



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?

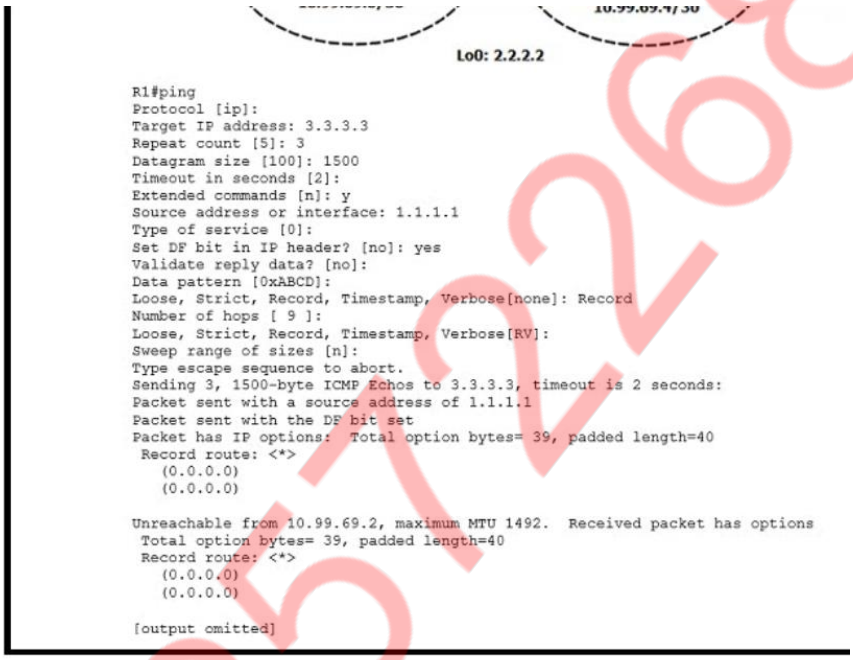
- R1(config-if)**interface Gi0/0**
  R1(config-if)**ip ospf database-filter all out**

  R2(config-if)**interface Gi0/0**
  R2(config-if)**ip ospf database-filter all out**
- 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**
- 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**
- 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**

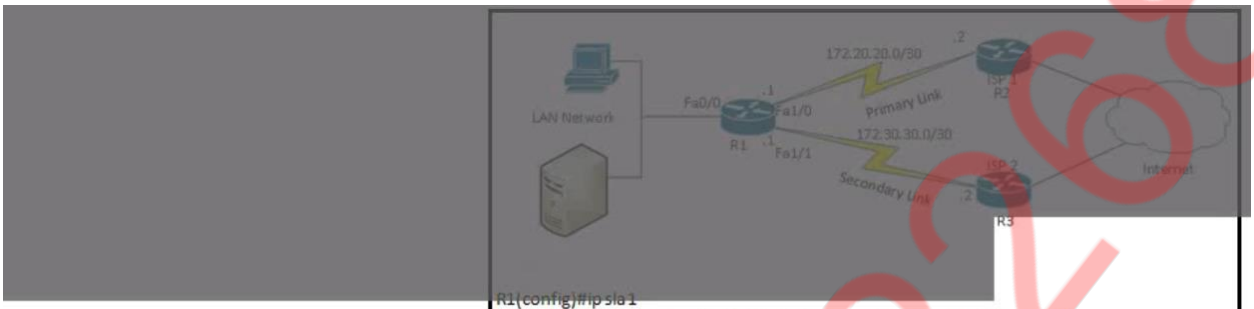


Refer to the exhibit. R1 is able to ping the R3 fa0/1 interface. Why do the extended pings fail?

- R2 and R3 do not have an OSPF adjacency.
- The DF bit has been set.
- The maximum packet size accepted by the command is 1476 bytes.
- R3 is missing a return route to 10.99.69.0/30.

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

- HTTPS
- HTTP
- SSH
- TCP




```
R1(config)#ip sla 1
R1(config-ip-sla)#icmp-echo 172.20.20.2 source-interface FastEthernet0/0
R1(config-ip-sla-echo)#timeout 5000
R1(config-ip-sla-echo)#frequency 10
R1(config-ip-sla-echo)#threshold 500
R1(config)#ip sla schedule 1 start-time now life forever
R1(config)#track 10 ip sla 1 reachability
R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2 track 10
R1(config)#no ip route 0.0.0.0 0.0.0.0 172.20.20.2
R1(config)#ip route 0.0.0.0 0.0.0.0 172.30.30.2 5
```

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

- [x] A route back to the R1 LAN network is missing in R2.
- [x] The source-interface is configured incorrectly.
- [ ] The default route has the wrong next hop IP address.
- [ ] The threshold value is wrong.
- [ ] The destination must be 172.30.30.2 for icmp-echo.

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?

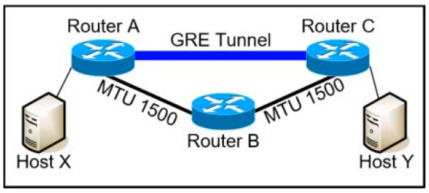
- (•) Mobility Express
- ( ) SD-Access wireless
- ( ) local mode
- ( ) autonomous

```
access-list 100 permit gre host 209.165.201.1 host 209.165.201.6

crypto isakmp policy 5
authentication pre-share
hash sha256
encryption aes
group 14

crypto isakmp key D@t@c3nt3r address 209.165.201.6

crypto ipsec transform-set My_Set esp-aes esp-sha-hmac
mode transport

crypto map MAP 10 ipsec-isakmp
 set peer 209.165.201.6
 set transform-set My_Set
 match addre 100

interface GigabitEthernet0/0
description outside_interface
 no switchport
 ip address 209.165.201.1 255.255.255.252
 crypto map MAP

interface Tunnel100
ip address 192.168.100.1 255.255.255.0
ip mtu 1400
tunnel source GigabitEthernet0/0
tunnel destination 209.165.201.6

ip route 10.20.0.0 255.255.255.0  192.168.100.2 Tunnel100
```

```
access-list 100 permit gre host 209.165.201.6 host 209.165.201.1

crypto isakmp policy 5
authentication pre-share
hash sha256
encryption aes
group 14

crypto isakmp key D@t@c3nt3 address 209.165.201.1

crypto ipsec transform-set My_Set esp-aes esp-sha-hmac
mode transport

crypto map MAP 10 ipsec-isakmp
 set peer 209.165.201.1
 set transform-set My_Set
 match address 100

Interface GigabitEthernet0/1
description outside_interface
 no switchport
 ip address 209.165.201.6 255.255.255.252
 crypto map MAP

interface Tunnel100
ip address 192.168.100.2 255.255.255.0
ip mtu 1400
tunnel source GigabitEthernet0/1
tunnel destination 209.165.201.1

ip route 10.10.0.0 255.255.255.0 192.168.100.1 Tunnel100
```

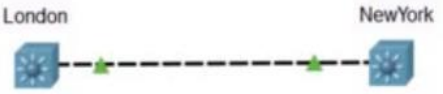
Refer to the exhibit. A network engineer must simplify the IPsec configuration by enabling IPsec over GRE using IPsec profiles. Which two configuration changes accomplish this? (Choose two).

- [ ] Remove the crypto map and modify the ACL to allow traffic between 10.10.0.0/24 to 10.20.0.0/24.
- [x] Remove all configuration related to crypto map from R1 and R2 and eliminate the ACL.
- [x] Create an IPsec profile, associate the transform-set, and apply the profile to the tunnel interface.
- [ ] Create an IPsec profile, associate the transform-set ACL, and apply the profile to the tunnel interface.
- [ ] Apply the crypto map to the tunnel interface and change the tunnel mode to tunnel mode ipsec ipv4.



Refer to the exhibit. MTU has been configured on the underlying physical topology, and no MTU command has been configured on the tunnel interfaces. What happens when a 1500-byte IPv4 packet traverses the GRE tunnel from host X to host Y, assuming the DF bit is cleared?

- [x] The packet arrives on router C fragmented.
- [ ] The packet is discarded on router A.
- [ ] The packet is discarded on router B.
- [ ] The packet arrives on router C without fragmentation.




```
London(config)#interface range fa0/1-2
London(config-if-range)#switchp trunk encapsulation dot1q
London(config-if-range)#switchp mode trunk
London(config-if-range)#channel-group 1 mode active
London(config-if-range)#end
London#
```

```
NewYork#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SD)           PAgP   Fa0/1(I) Fa0/2(D)
NewYork#
NewYork#show etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po1
------------
Age of the Port-channel   = 00d:00h:14m:20s
Logical slot/port   = 2/1       Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =   PAGP
Port Security       = Disabled
```

Refer to the exhibit. Communication between London and New York is down. Which command set must be applied to the NewYork switch to resolve the issue?

- NewYork(config)#no interface po1
  NewYork(config)#interface range fa0/1-2
  NewYork(config-if)#channel-group 1 mode on
  NewYork(config-if)#end
  NewYork#
- **NewYork(config)#no interface po1**
  NewYork(config)#interface range fa0/1-2
  NewYork(config-if)#channel-group 1 mode passive
  NewYork(config-if)#end
  NewYork#
- NewYork(config)#no interface po1
  NewYork(config)#interface range fa0/1-2
  NewYork(config-if)#channel-group 1 mode auto
  NewYork(config-if)#end
  NewYork#
- NewYork(config)#no interface po1
  NewYork(config)#interface range fa0/1-2
  NewYork(config-if)#channel-group 1 mode negotiate
  NewYork(config-if)#end
  NewYork#

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

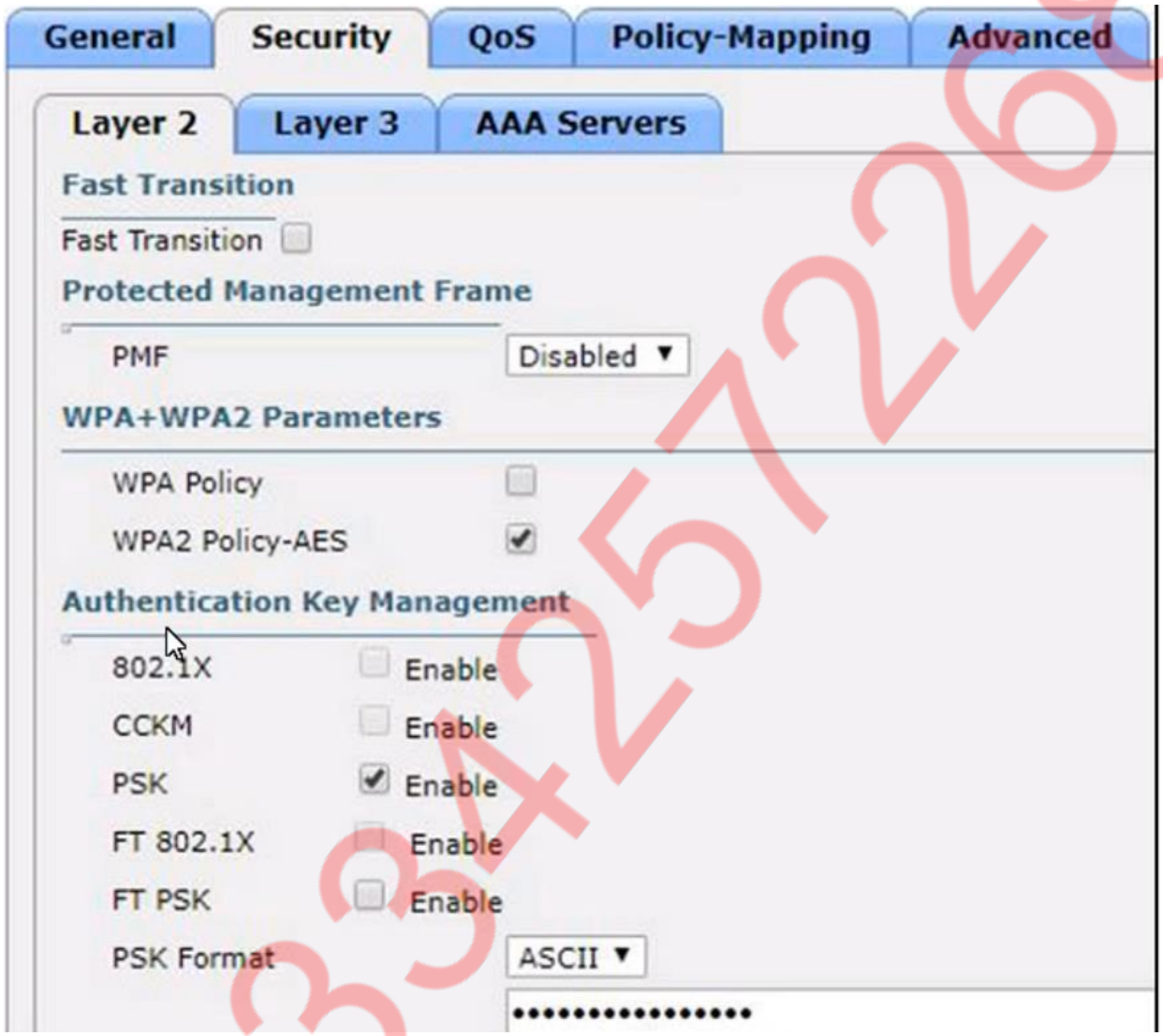
- (•) It creates two entries for each network node, one for its identity and another for its location on the network.
- ( ) It allows LISP to be applied as a network virtualization overlay through encapsulation.
- ( ) It allows multiple instances of a routing table to co-exist within the same router.
- ( ) It creates head-end replication used to deliver broadcast and multicast frames to the entire network.

Which two methods are used to reduce the AP coverage area? (Choose two.)

- [ ] Enable Fastlane.
- [ ] Disable 2.4 GHz and use only 5 GHz.
- [x] Reduce AP transmit power.
- [ ] Reduce channel width from 40 MHz to 20 MHz.
- [x] Increase minimum mandatory data rate.

An engineer must configure HSRP group 300 on a Cisco IOS router. When the router is functional, it must be the active HSRP router. The peer router has been configured using the default priority value. Which command set is required?

- (•) **standby 300 priority 110**
  standby 300 timers 1 110
- ( ) **standby version 2**
  standby 300 priority 110
  standby 300 preempt
- ( ) **standby 300 priority 90**
  standby 300 preempt
- ( ) **standby version 2**
  standby 300 priority 90
  standby 300 preempt



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

- text string
- username and password
- certificate
- RADIUS token

What is a consideration when designing a Cisco SD-Access underlay network?

- End user subnets and endpoints are part of the underlay network.
- Static routing is a requirement.
- The underlay switches provide endpoint physical connectivity for users.
- It must support IPv4 and IPv6 underlay networks.

Wireless users report frequent disconnections from the wireless network. While troubleshooting, a network engineer finds that after the user is disconnected, 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?

- increase the dynamic channel assignment interval
- increase the AP heartbeat timeout
- enable BandSelect
- enable coverage hole detection

Name is Bob Johnson
Age is 75
Is alive

Favorite foods are:
• Cereal
• Mustard
• Onions

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

- {'Name': 'Bob Johnson', 'Age': 75, 'Alive': True, 'Favorite Foods': 'Cereal', 'Mustard', 'Onions'}
- {Name: Bob Johnson, Age: 75, Alive: true, Favorite Foods: [Cereal, Mustard, Onions]}
- {"Name": "Bob Johnson", "Age": Seventyfive, "Alive": true, "Favorite Foods": ["Cereal", "Mustard", "Onions"]}
- {"Name": "Bob Johnson", "Age": 75, "Alive": true, "Favorite Foods": ["Cereal", "Mustard", "Onions"]}

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

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. What explains this behavior?

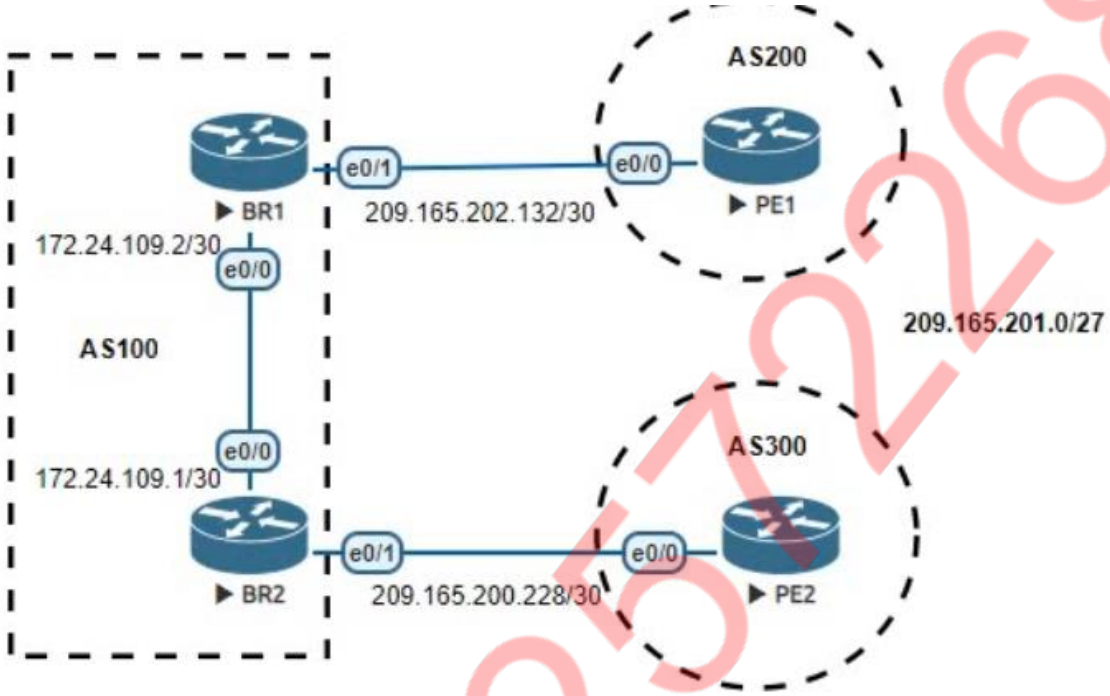
- After an access control list is applied to an interface, that interface must be shut and no shut for the access control list to take effect.
- The access control list must contain an explicit deny to block traffic from the router.
- Access control lists that are applied outbound to a router interface do not affect traffic that is sourced from the router.
- Only standard access control lists can block traffic from a source IP address.

What is YANG used for?

- scraping data via CLI
- processing SNMP read-only polls
- describing data models
- providing a transport for network configuration data between client and server

Which method should an engineer use to deal with a long-standing contention issue between any two VMs on the same host?

- adjust the resource reservation limits
- live migrate the VM to another host
- reset the VM
- reset the host



BR1
router bgp 100
neighbor 172.24.109.1 remote-as 100
neighbor 172.24.109.1 next-hop-self
neighbor 209.165.202.134 remote-as 200

PE1
router bgp 200
bgp log-neighbor-changes
neighbor 209.165.202.133 remote-as 100

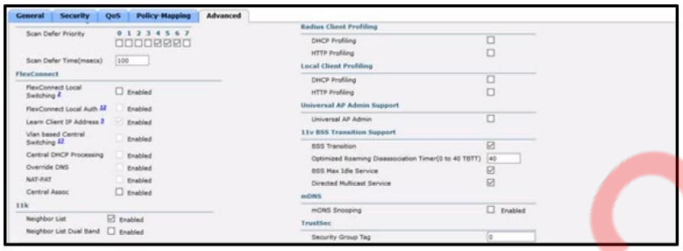
BR2
router bgp 100
neighbor 172.24.109.2 remote-as 100
neighbor 172.24.109.2 next-hop-self
neighbor 209.165.200.230 remote-as 300

PE2
router bgp 300
bgp log-neighbor-changes
neighbor 209.165.200.229 remote-as 100

```
BR2#sh ip route | i 209.165.201.0
209.165.201.0/27 is subnetted, 1 subnets
B 209.165.201.0 [20/0] via 209.165.200.230, 00:00:17
```

Refer to the exhibit. Which configuration change will force BR2 to reach 209.165.201.0/27 via BR1?

- Set the origin to igp on BR2 toward PE2 inbound.
- Set the local preference to 150 on PE1 toward BR1 outbound.
- Set the MED to 1 on PE2 toward BR2 outbound.
- Set the weight attribute to 65,535 on BR1 toward PE1.



Refer to the exhibit. An engineer configured the Bonjour Gateway on a Cisco WLC to support Apple Airplay. Users cannot see Apple TV while on the WLAN. Which action resolves this issue?

- Disable Directed Multicast.
- Enable FlexConnect Local Switching.
- Disable Neighbor List Dual Band.
- Enable mDNS Snooping.

This is new question you can check the answer for this question

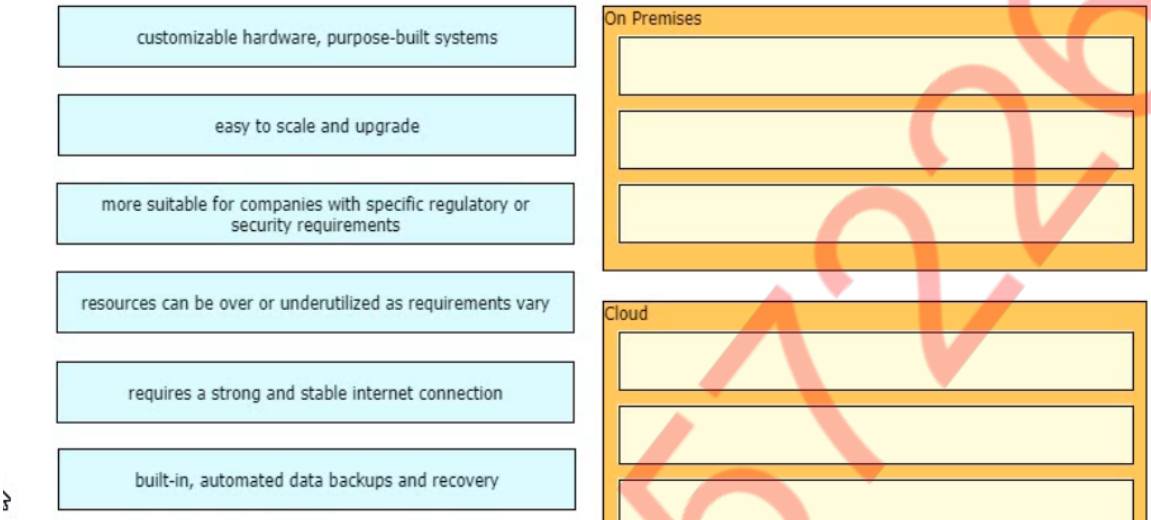
When a wired client connects to an edge switch in a Cisco SD-Access fabric, which component decides whether the client has access to the network?

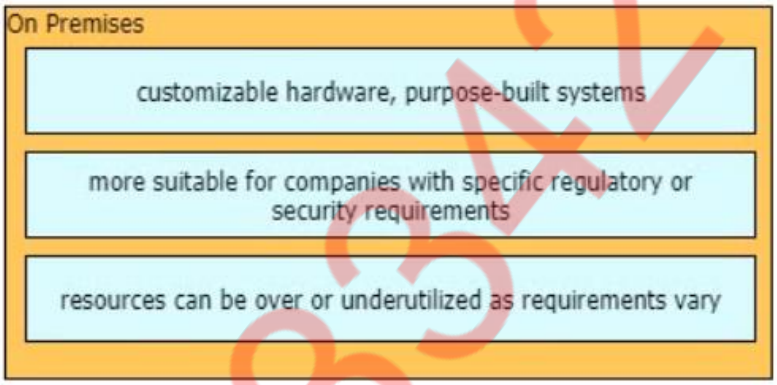
- RADIUS server
- edge node
- Identity Services Engine
- control-plane node

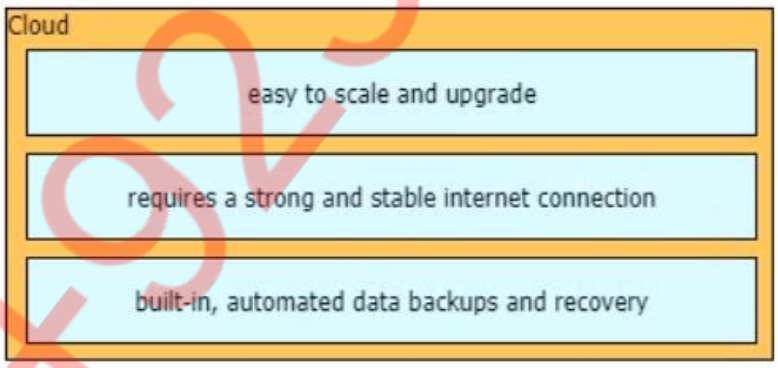
A company has an existing Cisco 5520 HA cluster using SSO. An engineer deploys a new single Cisco Catalyst 9800 WLC to test new features. The engineer successfully configures a mobility tunnel between the 5520 cluster and 9800 WLC. Clients connected to the corporate WLAN roam seamlessly between access points on the 5520 and 9800 WLC. After a failure on the primary 5520 WLC, all WLAN services remain functional; however, clients cannot roam between the 5520 and 9800 controllers without dropping their connection. Which feature must be configured to remedy the issue?

- mobility MAC on the 5520 cluster
- mobility MAC on the 9800 WLC
- new mobility on the 5520 cluster
- new mobility on the 9800 WLC

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







```
Router#show run | b vty
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
```

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

- **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 4
  access-class 23 in
  transport input ssh
- **access-list 23 permit 10.10.10.0 255.255.255.0**
  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

PYTHON CODE:

```
import requests
import json

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

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

print(response['ins_api']['outputs']['output']['body']['kickstart_ver_str'])
```

HTTP JSON Response:

```
{
  "ins_api": {
    "type": "cli_show",
    "version": "1.0",
    "sid": "eoc",
    "outputs": {
      "output": {
        "input": "show version",
        "msg": "Success",
        "code": "200",
        "body": {
          "bios_ver_str": "07.61",
          "kickstart_ver_str": "7.0(3)I7(4)",
          "bios_cmpl_time": "04/06/2017",
          "kick_file_name": "bootflash:///nxos.7.0.3.I7.4.bin",
          "kick_cmpl_time": " 6/14/1970 2:00:00",
          "kick_tmstmp": "06/14/1970 09:49:04",
          "chassis_id": "Nexus9000 93180YC-EX chassis",
          "cpu_name": "Intel(R) Xeon(R) CPU  @ 1.80GHz",
          "memory": 24633488,
          "mem_type": "kB",
          "rr_usecs": 134703,
          "rr_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": {}
            }
          }
        }
      }
    }
  }
}
```

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

- 7.61
- KeyError: 'kickstart_ver_str'
- 7.0(3)I7(4)
- NameError: name 'json' is not defined

```
Router# traceroute 10.10.10.1

Type escape sequence to abort.
Tracing the route to 10.10.10.1

1  10.0.0.1  5 msec  5 msec  5 msec
2  10.5.0.1  15 msec  17 msec  17 msec
3  10.10.10.1  *  *  *
```

Refer to the exhibit. An engineer is troubleshooting a connectivity issue and executes a traceroute. What does the result confirm?

- The protocol is unreachable.
- The destination server reported it is too busy.
- The destination port is unreachable.
- The probe timed out.

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

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

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

- 1

```
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
```

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

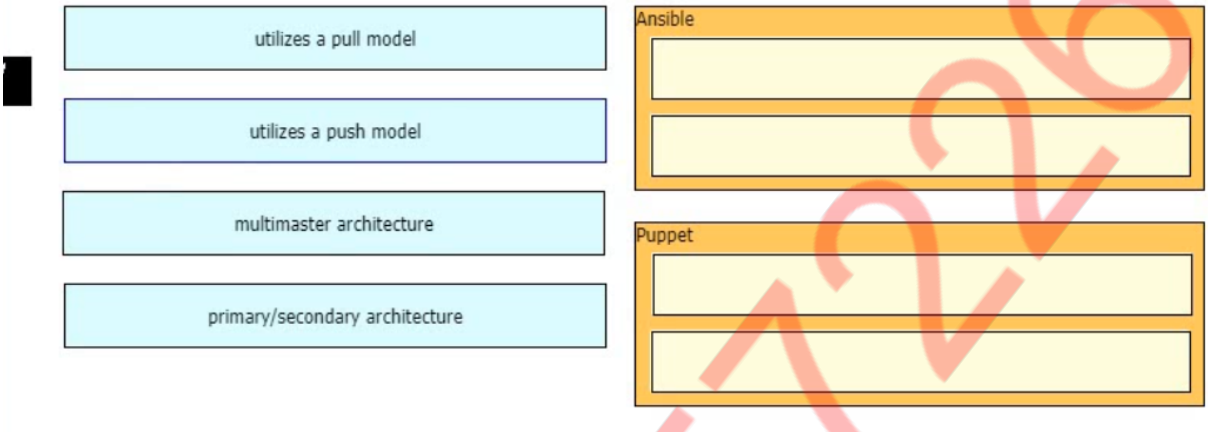
- [ ] R1 becomes the standby router.
- [x] If R1 goes down, R2 becomes active and remains the active device when R1 comes back online.
- [ ] If R2 goes down, R1 becomes active but reverts to standby when R2 comes back online.
- [x] R1 becomes the active router.
- [ ] If R1 goes down, R2 becomes active but reverts to standby when R1 comes back online.

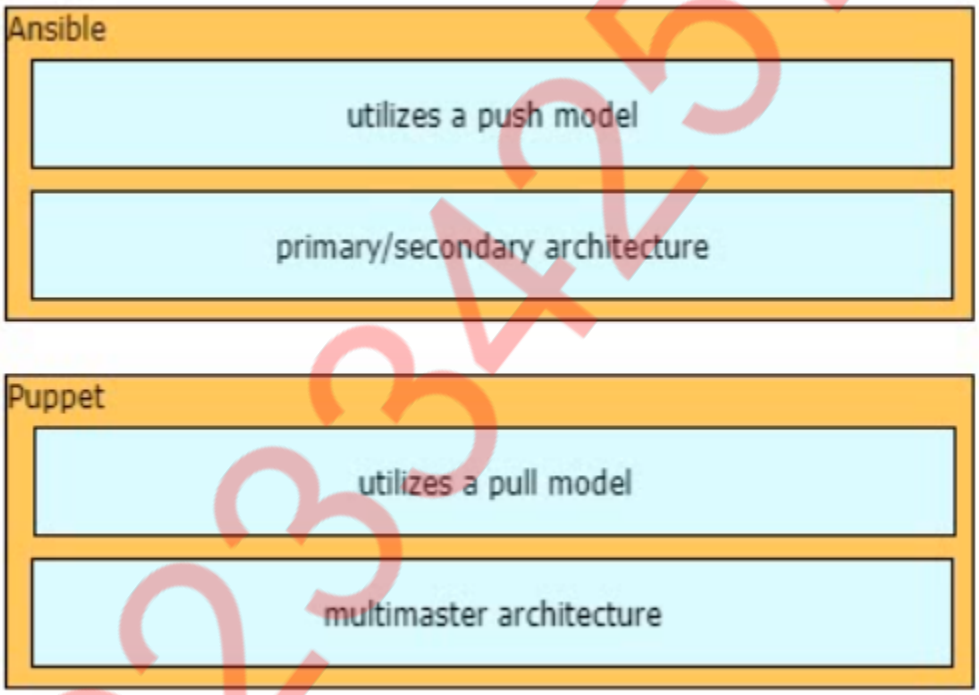
```
>>> netconf_data["GigabitEthernet"][0]["enabled"]
u'false'
>>> netconf_data["GigabitEthernet"][1]["enabled"]
u'true'
>>> netconf_data["GigabitEthernet"][2]["enabled"]
u'false'
>>> netconf_data["GigabitEthernet"][0]["description"]
u'my description'
```

Refer to the exhibit. Which Python code snippet prints the descriptions of disabled interfaces only?

- ( )
```
for interface in netconf_data["GigabitEthernet"]:
    if interface["disabled"] != 'true':
    print(interface["description"])
```
- (•)
```
for interface in netconf_data["GigabitEthernet"]:
    if interface["enabled"] != 'true':
        print(interface["description"])
```
- ( )
```
for interface in netconf_data["GigabitEthernet"]:
    if interface["enabled"] != 'false':
        print(interface["description"])
```
- ( )
```
for interface in netconf_data["GigabitEthernet"]:
    print(interface["enabled"])
    print(interface["description"])
```

Drag and drop the characteristics from the left onto the orchestration tools they describe on the right.





The login method is configured on the VTY lines of a router with these parameters:

- The first method for authentication is TACACS
- If TACACS is unavailable, login is allowed without any provided credentials

Which configuration accomplishes this task?

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

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

R1#**sh run | include username**
R1#

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#

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

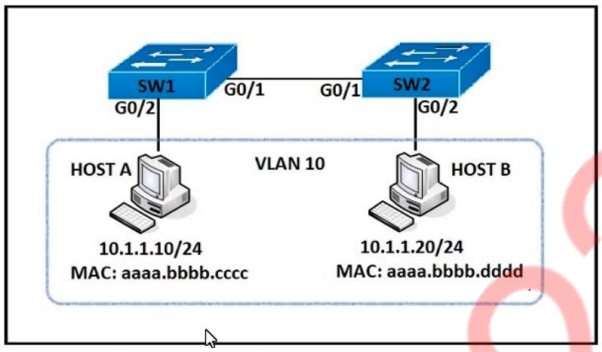
R1#**sh run | section vty**
line vty 0 4
transport input none
R1#

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

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

R1#**sh run | include username**
R1#

Answer here is A



Refer to the exhibit. An engineer must deny HTTP traffic from host A to host B while allowing all other communication between the hosts. Drag and drop the commands into the configuration to achieve these results. Some commands may be used more than once. Not all commands are used.

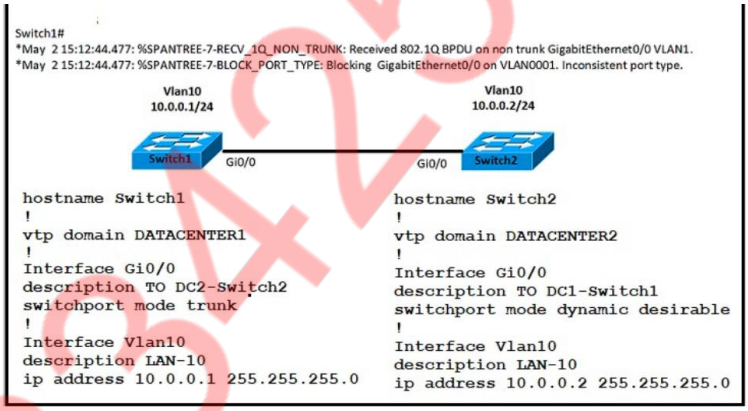
```
SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)# [          ] tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# ip access-list extended MATCH_ALL
SW1(config-ext-nacl)# [          ] ip any any

SW1(config)# vlan access-map HOST-A-B 10
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# [          ]

SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address MATCH_ALL
SW1(config-access-map)# [          ]

SW1(config)# vlan filter HOST-A-B vlan 10
```

action drop | action forward | filter | permit | deny | match

```
SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)# [ permit ] tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# ip access-list extended MATCH_ALL
SW1(config-ext-nacl)# [ permit ] ip any any

SW1(config)# vlan access-map HOST-A-B 10
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# [ action drop ]

SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address MATCH_ALL
SW1(config-access-map)# [ action forward ]
```

What is the structure of a JSON web token?

- [x] three parts separated by dots: header, payload, and signature
- [ ] header and payload
- [ ] payload and signature
- [ ] three parts separated by dots: version, header, and signature



Refer to the exhibit. An engineer implemented several configuration changes and receives the logging message on Switch1. Which action should the engineer take to resolve this issue?

- [ ] Change Switch1 to switch port mode dynamic auto.
- [x] Change the VTP domain to match on both switches.
- [ ] Change Switch1 to switch port mode dynamic desirable.
- [ ] Change Switch2 to switch port mode dynamic auto.

```
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
```

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

- (•) RSPAN session 1 is incompletely configured for monitoring.
- ( ) RSPAN session 1 monitors activity on VLAN 50 of a remote switch.
- ( ) SPAN session 2 only monitors egress traffic exiting port FastEthernet 0/14.
- ( ) SPAN session 2 monitors all traffic entering and exiting port FastEthernet 0/15.

Which congestion queuing method on Cisco IOS based routers uses four static queues?

- (•) priority
- ( ) custom
- ( ) weighted fair
- ( ) low latency