

## Exam Questions 350-401

Implementing and Operating Cisco Enterprise Network Core Technologies

<https://www.2passeasy.com/dumps/350-401/>



#### NEW QUESTION 1

- (Topic 4)

Which two security features are available when implementing NTP? (Choose two.)

- A. symmetric server passwords
- B. dock offset authentication
- C. broadcast association mode
- D. encrypted authentication mechanism
- E. access list-based restriction scheme

**Answer:** DE

#### NEW QUESTION 2

- (Topic 4)

An engineer must implement a configuration to allow a network administrator to connect to the console port of a router and authenticate over the network. Which command set should the engineer use?

- A. aaa new-modelaaa authentication login default enable
- B. aaa new-modelaaa authentication login console local
- C. aaa new-model aaa authentication login console group radius
- D. aaa new-modelaaa authentication enable default

**Answer:** B

#### NEW QUESTION 3

- (Topic 4)

A network administrator wants to install new VoIP switches in a small network closet but is concerned about the current heat level of the room. Which of the following should the administrator take into consideration before installing the new equipment?

- A. The power load of the switches
- B. The humidity in the room
- C. The fire suppression system
- D. The direction of airflow within the switches

**Answer:** D

#### Explanation:

This is because the direction of airflow within the switches can affect the heat level of the room, as the switches can either exhaust or intake hot air from the environment. The network administrator should take into consideration the direction of airflow within the switches before installing the new equipment, and ensure that the switches are aligned in the same direction and have enough space for ventilation. The network administrator should also avoid mixing switches with different airflow directions, as this can create a hot spot and reduce the cooling efficiency. The source of this answer is the Cisco ENCOR v1.1 course, module 2, lesson 2.1: Implementing Device Hardening.

#### NEW QUESTION 4

- (Topic 4)

An engineer must configure a router to allow users to run specific configuration commands by validating the user against the router database. Which configuration must be applied?

- A. aaa authentication network default local
- B. aaa authentication exec default local
- C. aaa authorization exec default local
- D. aaa authorization network default local

**Answer:** C

#### NEW QUESTION 5

- (Topic 4)

Refer to the exhibit.

General	Security	QoS	Policy-Mapping	Advanced
Allow AAA Override	<input checked="" type="checkbox"/>	Enabled		
Coverage Hole Detection	<input checked="" type="checkbox"/>	Enabled		
Enable Session Timeout	<input checked="" type="checkbox"/>	1800		Session Timeout (secs)
Aironet IE	<input checked="" type="checkbox"/>	Enabled		
Diagnostic Channel	<input type="checkbox"/>	Enabled		
Override Interface ACL		IPv4 Guest_Permit		IPv6 None
Layer2 Ad		None		
URL ACL		None		
P2P Blocking Action		Disabled		
Client Exclusion	<input type="checkbox"/>	Enabled	180	Timeout Value (secs)
Maximum Allowed Clients		0		
Static IP Tunneling	<input type="checkbox"/>	Enabled		
Wi-Fi Direct Clients Policy		Disabled		

An engineer configures a new WLAN that will be used for secure communications; however, wireless clients report that they are able to communicate with each other. Which action resolves this issue?

- A. Enable Client Exclusions.
- B. Disable Aironet IE
- C. Enable Wi-Fi Direct Client Policy
- D. Enable P2P Blocking.

Answer: D

#### NEW QUESTION 6

- (Topic 4)

By default, which virtual MAC address does HSRP group 30 use?

- A. 00:05:0c:07:ac:30
- B. 00:00:0c:07:ac:1e
- C. 05:0c:5e:ac:07:30
- D. 00:42:18:14:05:1e

Answer: B

#### NEW QUESTION 7

- (Topic 4)

A customer has 20 stores located throughout a city. Each store has a single Cisco access point managed by a central WLC. The customer wants to gather analysis for users in each store. Which technique supports these requirements?

- A. angle of arrival
- B. hyperlocation
- C. trilateration
- D. presence

Answer: B

#### NEW QUESTION 8

- (Topic 4)

A network engineer must configure a switch to allow remote access for all feasible protocols. Only a password must be requested for device authentication and all idle sessions must be terminated in 30 minutes. Which configuration must be applied?

- line vty 0 15  
password cisco  
transport input all  
exec-timeout 0 30
- line console 0  
password cisco  
exec-timeout 30 0
- line vty 0 15  
password cisco  
transport input telnet ssh  
exec-timeout 30 0
- username cisco privilege 15 cisco  
line vty 0 15  
transport input telnet ssh  
login local  
exec-timeout 0 30

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

Answer: C

**NEW QUESTION 9**

- (Topic 4)

An engineer must configure router R1 to validate user logins via RADIUS and fall back to the local user database if the RADIUS server is not available. Which configuration must be applied?

- A. aaa authorization exec default radius local
- B. aaa authorization exec default radius
- C. aaa authentication exec default radius local
- D. aaa authentication exec default radius

Answer: C

**NEW QUESTION 10**

- (Topic 4)

Refer to the exhibit.

```

Port 13 (FastEthernet1/0/11)
  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 001b.0d8e.e080
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
-----
Fa1/0/7 Desg FWD 2 128.9 P2p Bound(PVST)
Fa1/0/10 Desg FWD 2 128.12 P2p Bound(PVST)
Fa1/0/11 Root FWD 2 128.13 P2p
Fa1/0/12 Altn BLK 2 128.14 P2p

DSW1#sh spanning-tree mst
#### MST1 vlass mapped: 10.20
Bridge address 001b.0d8e.e080 priority 32769 (32768 sysid 1)
Root address 0018.7363.4300 priority 32769 (32768 sysid 1)
port Fa1/0/11 cost 2 ran hops 19

!
... output omitted
!
    
```

Which two commands ensure that DSW1 becomes the root bridge for VLAN 10 and 20? (Choose two.)

- A. spanning-tree mst 1 priority 1
- B. spanning-tree mstp vlan 10.20 root primary
- C. spanning-tree mst 1 root primary
- D. spanning-tree mst 1 priority 4096
- E. spanning-tree mst vlan 10.20 priority root

Answer: DE

#### NEW QUESTION 10

- (Topic 4)

```
no aaa new-model
username admin privilege 15 secret cisco123
ip http secure-port 445
```

Refer to the exhibit Which command must be applied to complete the configuration and enable RESTCONF?

- A. ip http secure-server
- B. ip http server
- C. ip http secure-port 443
- D. ip http client username restconf

Answer: A

#### NEW QUESTION 14

- (Topic 4)

A customer requires their wireless network to be fully functional, even if the wireless controller fails. Which wireless design supports these requirements?

- A. FlexConnect
- B. mesh
- C. centralized
- D. embedded

Answer: A

#### Explanation:

This is because FlexConnect is a feature that allows wireless access points to operate in standalone mode when they lose connectivity to the wireless LAN controller. FlexConnect enables the access points to switch the data traffic locally, without sending it to the controller, and to perform local authentication, without relying on the central server. FlexConnect also allows the access points to maintain the wireless network functionality, such as SSIDs, security policies, and QoS, even if the wireless controller fails. FlexConnect is suitable for branch locations or remote offices that have limited WAN bandwidth or reliability. The source of this answer is the Cisco ENCOR v1.1 course, module 7, lesson 7.3: Implementing FlexConnect.

#### NEW QUESTION 15

- (Topic 4)

An engineer must protect the password for the VTY lines against over-the-shoulder attacks. Which configuration should be applied?

- A. service password-encryption
- B. username netadmin secret 9 \$9\$vFpMf8elb4RVV8\$seZ/bDA
- C. username netadmin secret 7\$1\$42J36k33008Pyh4QzwXyZ4
- D. line vty 0 15 p3ssword XD822j

Answer: A

#### Explanation:

```
cisco(config)#username test privilege 15 password test777 cisco(config)#do s running-config | include user
username test privilege 15 password 0 test777
cisco(config)#service password-encryption cisco(config)#do s running-config | include user
username test privilege 15 password 7 044F0E151B761B19 cisco(config)#
cisco(config)#do wr
Building configuration... [OK]
cisco(config)#
```

#### NEW QUESTION 17

- (Topic 4)

```
interface GigabitEthernet1
 ip address 10.10.10.1 255.255.255.0
 !
 access-list 10 permit 10.10.10.1
 !
 monitor session 10 type erspan-source
 source interface Gi1
 destination
  erspan-id 10
 ip address 192.168.1.1
 !
```

Refer to the exhibit. Which command filters the ERSPAN session packets only to interface GigabitEthernet1?

- A. source ip 10.10.10.1
- B. source interface gigabitethernet1 ip 10.10.10.1
- C. filter access-group 10
- D. destination ip 10.10.10.1

Answer: C

**NEW QUESTION 19**

DRAG DROP - (Topic 4)

Drag and drop the automation characteristics from the left onto the corresponding tools on the right. Not all options are used.

based on Python	Puppet
proprietary syntax in configuration files based on Ruby	
high availability offered through a multi-primary architecture	Chef
Ruby syntax in configuration files	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

based on Python	Puppet
proprietary syntax in configuration files based on Ruby	
high availability offered through a multi-primary architecture	Chef
Ruby syntax in configuration files	

**NEW QUESTION 23**

- (Topic 4)

What is the result of applying this access control list?

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

- A. TCP traffic with the URG bit set is allowed
- B. TCP traffic with the SYN bit set is allowed
- C. TCP traffic with the ACK bit set is allowed

D. TCP traffic with the DF bit set is allowed

Answer: C

**NEW QUESTION 24**

DRAG DROP - (Topic 4)

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

declarative	Chef
uses Ruby	
uses Python	SaltStack
procedural	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

declarative	Chef
uses Ruby	
uses Python	SaltStack
procedural	

**NEW QUESTION 29**

- (Topic 4)

An engineer is connected to a Cisco router through a Telnet session. Which command must be issued to view the logging messages from the current session as soon as they are generated by the router?

- A. logging buffer
- B. service timestamps log uptime
- C. logging host
- D. terminal monitor

Answer: D

**NEW QUESTION 31**

- (Topic 4)

```
router(config)# line con 0
line con 0
 password cisco
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 !
end

router#sh run | i username|aaa
no aaa new-model
username user password 0 user
router#
```

Refer to the exhibit Which configuration enables password checking on the console line, using only a password?

A)

```
router(config)# line con 0
router(config-line)# exec-timeout 0 0
```

B)

```
router(config)# line con 0
router(config-line)# login
```

C)

```
router(config)# line con 0
router(config-line)# login local
```

D)

```
router(config)# line vty 0 4
router(config-line)# login
```

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

**Answer: B**

### NEW QUESTION 33

- (Topic 4)

How does Protocol Independent Multicast function?

- A. In sparse mode, it establishes neighbor adjacencies and sends hello messages at 5- second intervals.
- B. It uses the multicast routing table to perform the multicast forwarding function.
- C. It uses unicast routing information to perform the multicast forwarding function.
- D. It uses broadcast routing information to perform the multicast forwarding function.

**Answer: C**

### NEW QUESTION 34

- (Topic 4)

```

Switch1#show ip int br
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet1  192.168.1.1     YES manual up          up
GigabitEthernet2  172.16.40.10   YES manual administratively down down
Loopback0         172.16.10.10   YES manual up          up

Switch2#show ip int br
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet1  192.168.1.2     YES manual up          up
GigabitEthernet2  172.16.20.10   YES manual up          up
Loopback0         10.10.10.10    YES manual up          up

Switch1(config)#monitor session 1 type erspan-source
Switch1(config-mon-erspan-src)#source interface gigabitethernet1
Switch1(config-mon-erspan-src)#destination
Switch1(config-mon-erspan-src-dst)#erspan-id 110
Switch1(config-mon-erspan-src-dst)#ip address 10.10.10.10
Switch1(config-mon-erspan-src-dst)#origin ip address 172.16.10.10

Switch2(config)#monitor session 1 type erspan-destination
Switch2(config-mon-erspan-dst)#destination interface GigabitEthernet2
Switch2(config-mon-erspan-dst)#source
Switch2(config-mon-erspan-dst-src)#
Switch2(config-mon-erspan-dst-src)#ip address 10.10.10.10
    
```

Refer to the exhibit. An engineer must configure an ERSPAN tunnel that mirrors traffic from linux1 on Switch1 to Linux2 on Switch2. Which command must be added to the destination configuration to enable the ERSPAN tunnel?

- A. (config-mon-erspan-dst-src)# origin ip address 172.16.10.10
- B. (config-mon-erspan-dst-src)# erspan-id 172.16.10.10
- C. (config-mon-erspan-dst-src)# no shut
- D. (config-mon-erspan-dst-src)# erspan-id 110

Answer: D

**NEW QUESTION 38**

DRAG DROP - (Topic 4)

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

uses virtual links to link an area that does not have a connection to the backbone	EIGRP
hello packets are sent by default every 5 seconds on high-bandwidth links	
default cost is based on interface bandwidth only	OSPF
metric is calculated using bandwidth and delay by default	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

uses virtual links to link an area that does not have a connection to the backbone	EIGRP
hello packets are sent by default every 5 seconds on high-bandwidth links	
default cost is based on interface bandwidth only	OSPF
metric is calculated using bandwidth and delay by default	

**NEW QUESTION 40**

- (Topic 4)

Based on the router's API output in JSON format below, which Python code will display the value of the "hostname" key?

```
{
  "response": [{
    "family": "Switches",
    "macAddress": "00:42:50:62:99:00",
    "hostname": "SwitchIDF14",
    "upTime": "352 days, 6:17:26:10",
    "lastUpdated": "2020-07-12 21:15:29"
  }]
}
```

- json\_data = json.loads(response.text)  
print(json\_data[response][0][hostname])
- json\_data = json.loads(response.text)  
print(json\_data[response][family][hostname])
- json\_data = response.json()  
print(json\_data[response][0][hostname])
- json\_data = response.json()  
print(json\_data[response][family][hostname])

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

Answer: B

#### NEW QUESTION 45

- (Topic 4)

An engineer must configure a new WLAN that allows a user to enter a passphrase and provides forward secrecy as a security measure. Which Layer 2 WLAN configuration is required on the Cisco WLC?

- A. WPA2 Personal
- B. WPA3 Enterprise
- C. WPA3 Personal
- D. WPA2 Enterprise

Answer: C

#### NEW QUESTION 46

- (Topic 4)

When using BFD in a network design, which consideration must be made?

- A. BFD is used with first hop routing protocols to provide subsecond convergence.
- B. BFD is more CPU-intensive than using reduced hold timers with routing protocols.
- C. BFD is used with dynamic routing protocols to provide subsecond convergence.
- D. BFD is used with NSF and graceful to provide subsecond convergence.

Answer: C

#### NEW QUESTION 50

- (Topic 4)

```
username cisco privilege 15 noescape secret 5 F7u$9cyE438490035m8TQ$nv&6502x
username cisco autocommand show startup-config
aaa authentication login default local-case enable
aaa authorization exec default local
```

An engineer applies this configuration to router R1. How does R1 respond when the user 'cisco' logs in?

- A. It displays the startup config and then permits the user to execute commands
- B. It places the user into EXEC mode and permits the user to execute any command
- C. It displays the startup config and then terminates the session.
- D. It places the user into EXEC mode but permits the user to execute only the show startup-config command

Answer: A

**NEW QUESTION 55**

- (Topic 1)

What is used to perform OoS packet classification?

- A. the Options field in the Layer 3 header
- B. the Type field in the Layer 2 frame
- C. the Flags field in the Layer 3 header
- D. the TOS field in the Layer 3 header

Answer: D

**Explanation:**

Type of service, when we talk about PACKET, means layer 3

**NEW QUESTION 57**

- (Topic 1)

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

- A. Adjust the resource reservation limits
- B. Live migrate the VM to another host
- C. Reset the VM
- D. Reset the host

Answer: A

**NEW QUESTION 60**

- (Topic 1)

What is the function of a VTEP in VXLAN?

- A. provide the routing underlay and overlay for VXLAN headers
- B. dynamically discover the location of end hosts in a VXLAN fabric
- C. encapsulate and de-encapsulate traffic into and out of the VXLAN fabric
- D. statically point to end host locations of the VXLAN fabric

Answer: C

**NEW QUESTION 63**

- (Topic 2)

Refer to the exhibit.

```
DSW2#sh spanning-tree vlan 10

VLAN0010
Spanning tree enabled protocol rstp
Root ID    Priority    4106
Address    0018.7363.4300
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    4106 (priority 4096 sys-id-ext 20)
Address    0018.7363.4300
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa1/0/7        Desg FWD 2         128.9    P2p Peer (STP)
Fa1/0/10       Desg FWD 4         128.12   P2p Peer (STP)
Fa1/0/11       Desg FWD 2         128.13   P2p Peer (STP)
Fa1/0/12       Desg FWD 2         128.14   P2p Peer (STP)
```

What is the result when a switch that is running PVST+ is added to this network?

- A. DSW2 operates in Rapid PVST+ and the new switch operates in PVST+
- B. Both switches operate in the PVST+ mode
- C. Spanning tree is disabled automatically on the network
- D. Both switches operate in the Rapid PVST+ mode.

Answer: A

**Explanation:**

From the output we see DSW2 is running in RSTP mode (in fact Rapid PVST+ mode as Cisco does not support RSTP alone). When a new switch running PVST+ mode is added to the topology, they keep running the old STP instances as RSTP (in fact Rapid PVST+) is compatible with PVST+.

**NEW QUESTION 64**

- (Topic 2)

In a Cisco StackWise Virtual environment, which planes are virtually combined in the common logical switch?

- A. management and data
- B. control and management
- C. control, and forwarding
- D. control and data

**Answer: B**

**NEW QUESTION 68**

DRAG DROP - (Topic 2)

Drag and drop the tools from the left onto the agent types on the right.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**NEW QUESTION 73**

- (Topic 2)

Which technology does VXLAN use to provide segmentation for Layer 2 and Layer 3 traffic?

- A. bridge domain
- B. VLAN
- C. VRF
- D. VNI

**Answer: D**

**Explanation:**

VXLAN has a 24-bit VXLAN network identifier (VNI), which allows for up to 16 million (= 2<sup>24</sup>) VXLAN segments to coexist within the same infrastructure. This surely solve the small number of traditional VLANs.

**NEW QUESTION 78**

- (Topic 2)

When are multicast RPs required?

- A. RPs are required only when using protocol independent multicast dense mode.
- B. By default, the RP is needed periodically to maintain sessions with sources and receivers.
- C. RPs are required for protocol Independent multicast sparse mode and dense mode.
- D. By default, the RP is needed only start new sessions with sources and receivers.

**Answer: D**

**NEW QUESTION 79**

- (Topic 2)

What is the difference between a RIB and a FIB?

- A. The RIB is used to make IP source prefix-based switching decisions
- B. The FIB is where all IP routing information is stored

- C. The RIB maintains a mirror image of the FIB
- D. The FIB is populated based on RIB content

Answer: D

**Explanation:**

CEF uses a Forwarding Information Base (FIB) to make IP destination prefix- based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and those changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table. Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for route cache maintenance that is associated with earlier switching paths such as fast switching and optimum switching.

Note: In order to view the Routing information base (RIB) table, use the “show ip route” command. To view the Forwarding Information Base (FIB), use the “show ip cef” command. RIB is in Control plane while FIB is in Data plane.

**NEW QUESTION 84**

- (Topic 2)

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

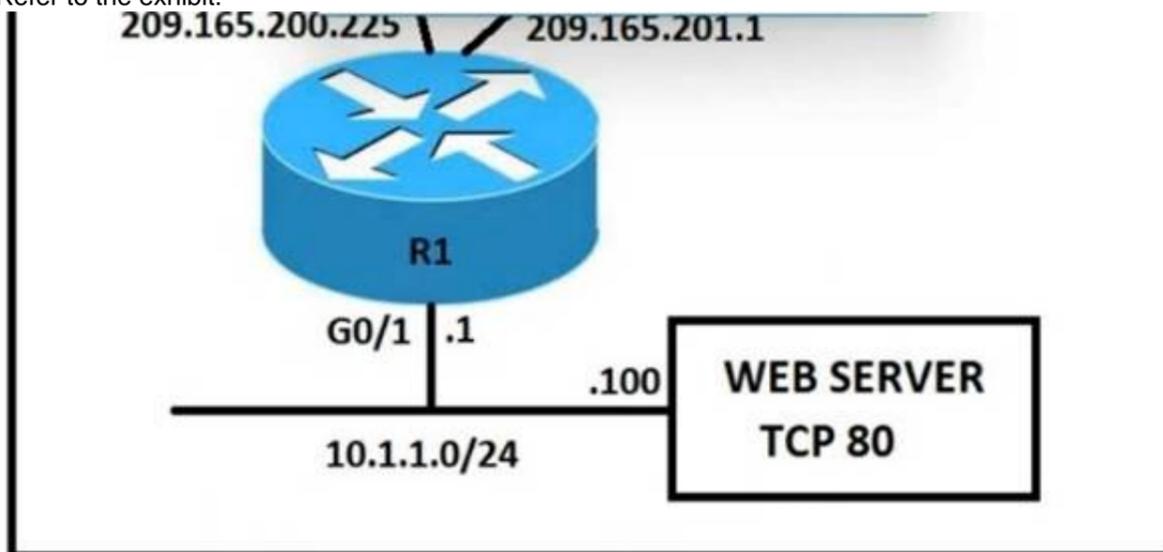
- A. with IP SLA
- B. ARP probing
- C. using BFD
- D. with OMP

Answer: C

**NEW QUESTION 85**

- (Topic 2)

Refer to the exhibit.



An engineer must configure static NAT on R1 to allow users HTTP access to the web server on TCP port 80. The web server must be reachable through ISP 1 and ISP 2. Which command set should be applied to R1 to fulfill these requirements?

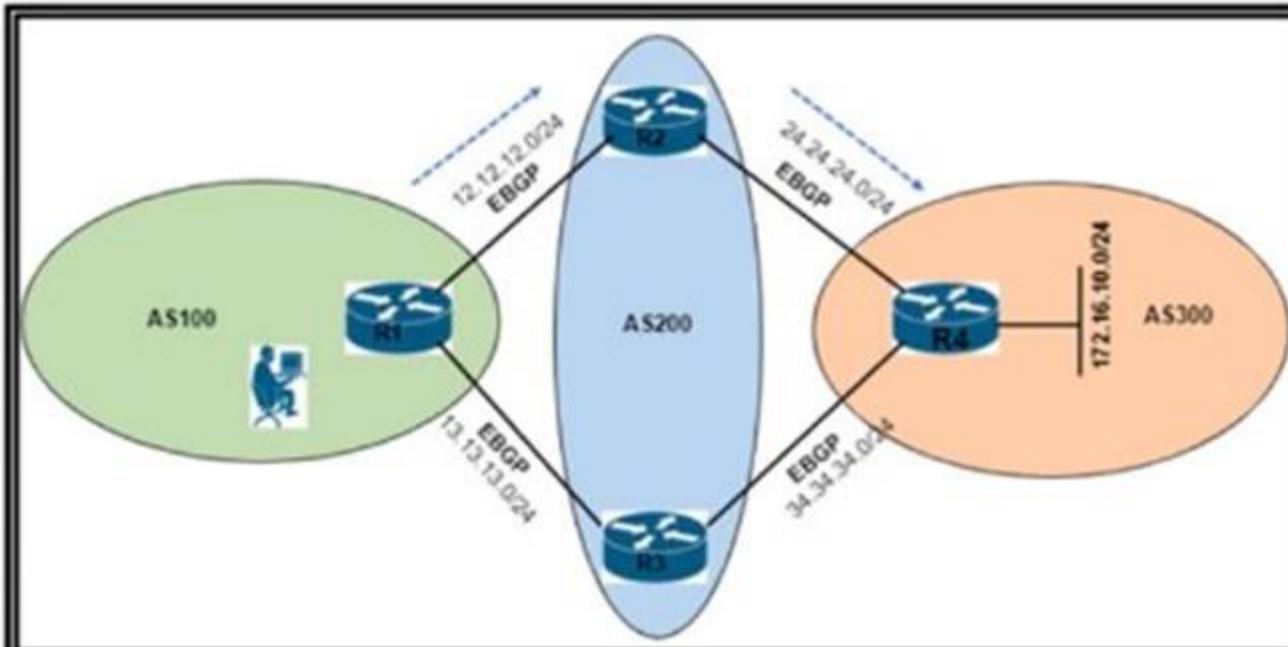
- A. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 extendable ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80 extendable
- B. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80
- C. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80
- D. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 no-alias ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80 no-alias

Answer: B

**NEW QUESTION 90**

- (Topic 2)

Refer to the exhibit.



```
R1#sh ip bgp
BGP table version is 2, local router ID is 13.13.13.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
                r RIB-failure, S Stale, m multipath, b backup-path, f RT-
Filter,
                x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
   Network          Next
Hop      Metric    LocPrf  Weight    Path
* 172.16.1.0/24      13.13.13.3          0
  200 300 i
*>
      200 300 i          12.12.12.2          0
```

An engineers reaching network 172 16 10 0/24 via the R1-R2-R4 path. Which configuration forces the traffic to take a path of R1-R3-R4?  
A)

```
R1(config)#route-map RM_AS_PATH_PREPEND
R1(config-route-map)#set as-path prepend 200 200
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#neighbor 12.12.12.2 route-map RM_AS_PATH_PREPEND in
R1(config-router)#end
R1#clear ip bgp 12.12.12.2 soft in
```

```
B)
R1(config)#router bgp 100
R1(config-router)#neighbor 13.13.13.3 weight 1
R1(config-router)#end
```

```
C)
R2(config)#route-map RM_MED permit 10
R2(config-route-map)#set metric 1
R2(config-route-map)#exit
R2(config)#router bgp 200
R2(config-router)#neighbor 12.12.12.1 route-map RM_MED out
R2(config-router)#end
R2#clear ip bgp 12.12.12.1 soft out
```

```
D)
R1(config)#route-map RM_LOCAL_PREF permit 10
R1(config-route-map)#set local-preference 101
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#neighbor 13.13.13.3 route-map RM_LOCAL_PREF in
R1(config-router)#end
R1#clear ip bgp 13.13.13.3 soft in
```

A. Option A

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

**Answer:** D

#### NEW QUESTION 93

- (Topic 2)

Which threat defence mechanism, when deployed at the network perimeter, protects against zero-day attacks?

- A. intrusion prevention
- B. stateful inspection
- C. sandbox
- D. SSL decryption

**Answer:** C

#### Explanation:

Reference: <https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html> "File analysis and sandboxing: Secure Malware Analytics' highly secure environment helps you execute, analyze, and test malware behavior to discover previously unknown ZERO-DAY threats. The integration of Secure Malware Analytics' sandboxing technology into Malware Defense results in more dynamic analysis checked against a larger set of behavioral indicators."

#### NEW QUESTION 96

- (Topic 2)

Which outcome is achieved with this Python code?

```
client.connect ( ip, port= 22, username= usr, password= pswd )
stdin, stdout, stderr = client.exec_command ( 'show ip bgp 192.168.101.0 bestpath\n ' )
print (stdout)
```

- A. connects to a Cisco device using SSH and exports the routing table information
- B. displays the output of the show command in a formatted way
- C. connects to a Cisco device using SSH and exports the BGP table for the prefix
- D. connects to a Cisco device using Telnet and exports the routing table information

**Answer:** C

#### NEW QUESTION 101

- (Topic 2)

Refer to the exhibit.

```
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: access-group name SNMP
police:
  cir 8000 bps, bc 1500 bytes
  conformed 0 packets, 0 bytes; actions:
  transmit
  exceeded 0 packets, 0 bytes; actions:
  drop
  conformed 0000 bps, exceeded 0000 bps
```

```
Class-map: class-default (match-any)
13858 packets, 1378745 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
```

How does the router handle traffic after the CoPP policy is configured on the router?

- A. Traffic coming to R1 that does not match access list SNMP is dropped.
- B. Traffic coming to R1 that matches access list SNMP is policed.
- C. Traffic passing through R1 that matches access list SNMP is policed.
- D. Traffic generated by R1 that matches access list SNMP is policed.

**Answer:** C

#### NEW QUESTION 104

- (Topic 2)

What is required for a virtual machine to run?

- A. a Type 1 hypervisor and a host operating system
- B. a hypervisor and physical server hardware
- C. only a Type 1 hypervisor

D. only a Type 2 hypervisor

**Answer:** B

**NEW QUESTION 108**

- (Topic 2)

A customer wants to provide wireless access to contractors using a guest portal on Cisco ISE. The portal is also used by employees. A solution is implemented, but contractors receive a certificate error when they attempt to access the portal. Employees can access the portal without any errors. Which change must be implemented to allow the contractors and employees to access the portal?

- A. Install a trusted third-party certificate on the Cisco ISE.
- B. Install an Internal CA signed certificate on the contractor devices
- C. Install an internal CA signed certificate on the Cisco ISE
- D. install a trusted third-party certificate on the contractor devices.

**Answer:** C

**NEW QUESTION 113**

- (Topic 2)

Which method is used by an AP to join HA controllers and is configured in NVRAM?

- A. stored WLC information
- B. DNS
- C. IP Helper Addresses
- D. Primary/Secondary/Tertiary/Backup

**Answer:** A

**Explanation:**

An AP can be “primed” with up to three controllers—a primary, a secondary, and a tertiary. These are stored in nonvolatile memory so that the AP can remember them after a reboot or power failure.

**NEW QUESTION 117**

DRAG DROP - (Topic 2)

Drag and drop characteristics of PIM dense mode from the left to the right.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

PIM-DM supports only source trees – that is, (S,G) entries—and cannot be used to build a shared distribution tree.

**NEW QUESTION 120**

- (Topic 2)

An engineer configures GigabitEthernet 0/1 for VRRP group 115. The router must assume the primary role when it has the highest priority in the group. Which command set is required to complete this task?

```
interface GigabitEthernet0/1
ip address 10.10.10.2 255.255.255.0
vrrp 115 ip 10.10.10.1
vrrp 115 authentication 406530697
```

- Router(config-if)# vrrp 115 priority 100
- Router(config-if)# standby 115 priority 100  
Router(config-if)# standby 115 preempt
- Router(config-if)# vrrp 115 track 1 decrement 10  
Router(config-if)# vrrp 115 preempt
- Router(config-if)# vrrp 115 track 1 decrement 100  
Router(config-if)# vrrp 115 preempt

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

Answer: C

**NEW QUESTION 123**

- (Topic 2)

Why would a log file contain a \* next to the date?

- A. The network device was receiving NTP time when the log messages were recorded.
- B. The network device was unable to reach The NTP server when the log messages were recorded
- C. The network device is not configured to use NTP.
- D. The network device is nor configured to use NTP time stamps for logging

Answer: B

**NEW QUESTION 127**

DRAG DROP - (Topic 2)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

**NEW QUESTION 131**

- (Topic 2)

Refer to the exhibit.



An engineer is troubleshooting an application running on Apple phones. The application is receiving incorrect QoS markings. The systems administrator confirmed that all configuration profiles are correct on the Apple devices. Which change on the WLC optimizes QoS for these devices?

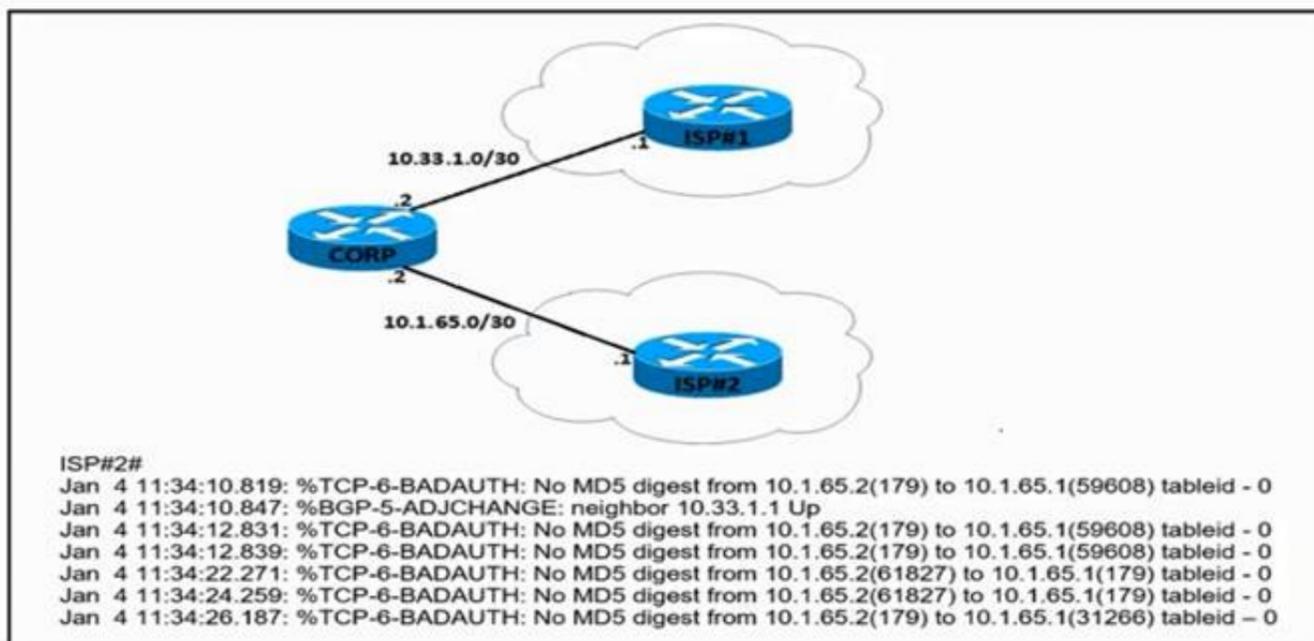
- A. Enable Fastlane
- B. Set WMM to required
- C. Change the QoS level to Platinum
- D. Configure AVC Profiles

Answer: C

**NEW QUESTION 136**

- (Topic 2)

Refer to the exhibit.



An engineer attempts to establish BGP peering between router CORP and two ISP routers. What is the root cause for the failure between CORP and ISP#2?

- A. Router ISP#2 is configured to use SHA-1 authentication.
- B. There is a password mismatch between router CORP and router ISP#2.
- C. Router CORP is configured with an extended access control list.
- D. MD5 authorization is configured incorrectly on router ISP#2.

Answer: B

**NEW QUESTION 139**

- (Topic 2)

When firewall capabilities are considered, which feature is found only in Cisco next-generation firewalls?

- A. malware protection
- B. stateful inspection
- C. traffic filtering
- D. active/standby high availability

Answer: A

**NEW QUESTION 142**

DRAG DROP - (Topic 2)

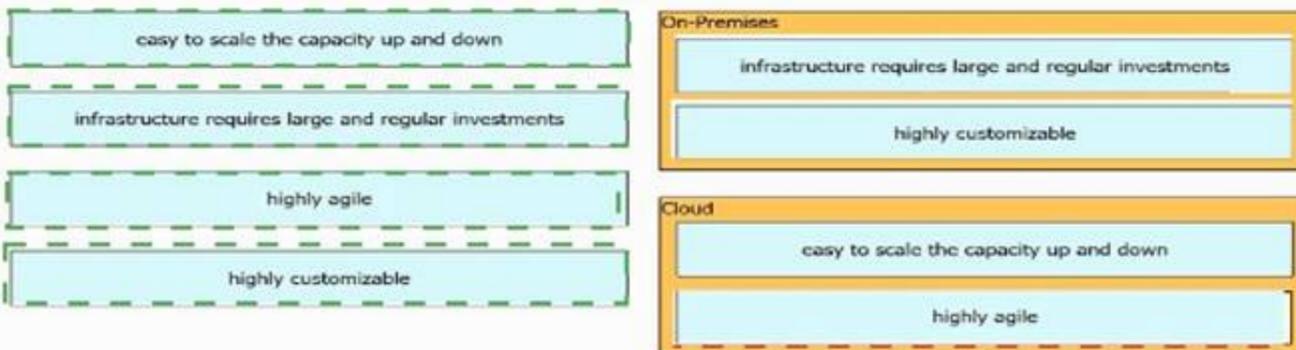
Drag and drop the characteristics from the left onto the infrastructure deployment models they describe on the right.



- A. Mastered
- B. Not Mastered

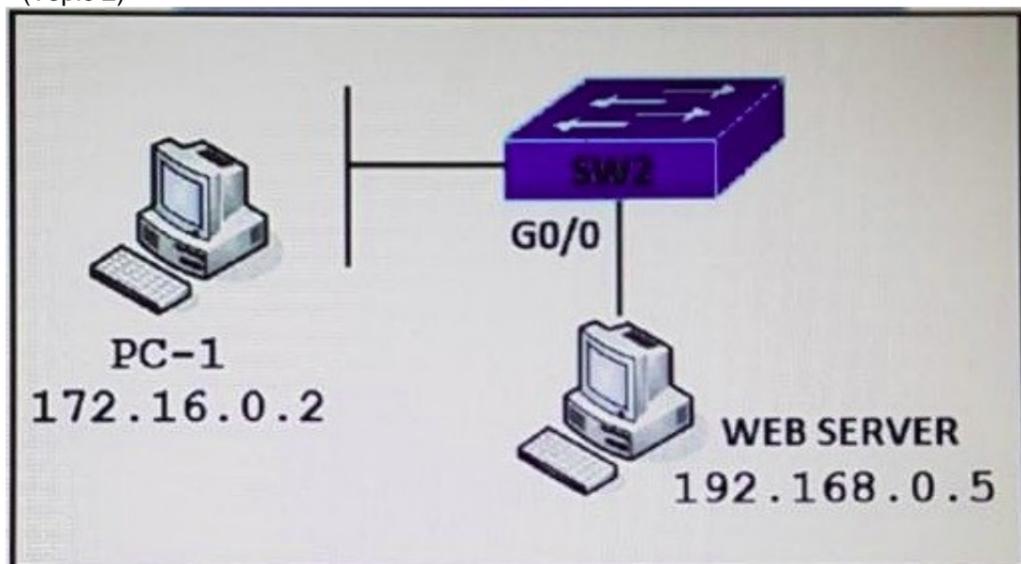
Answer: A

Explanation:



**NEW QUESTION 144**

- (Topic 2)



Refer to the exhibit. PC-1 must access the web server on port 8080. To allow this traffic, which statement must be added to an access control list that is applied on SW2 port G0/0 in the inbound direction?

- A. permit host 172.16.0.2 host 192.168.0.5 eq 8080
- B. permit host 192.168.0.5 host 172.16.0.2 eq 8080
- C. permit host 192.168.0.5 eq 8080 host 172.16.0.2
- D. permit host 192.168.0.5 it 8080 host 172.16.0.2

Answer: C

Explanation:

The inbound direction of G0/0 of SW2 only filter traffic from Web Server to PC-1 so the source IP address and port is of the Web Server.

**NEW QUESTION 148**

- (Topic 2)

Which two actions, when applied in the LAN network segment, will facilitate Layer 3 CAPWAP discovery for lightweight AP? (Choose two.)

- A. Utilize DHCP option 17.
- B. Configure WLC IP address on LAN switch.
- C. Utilize DHCP option 43.
- D. Configure an ip helper-address on the router interface
- E. Enable port security on the switch port

Answer: CE

Explanation:

Reference: [https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless- controllers/119286-lap-notjoin-wlc-tshoot.html](https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/119286-lap-notjoin-wlc-tshoot.html)

**NEW QUESTION 152**

- (Topic 2)

What is one primary REST security design principle?

- A. fail-safe defaults
- B. password hash
- C. adding a timestamp in requests
- D. OAuth

**Answer: A****Explanation:**

Reference: <https://yurisubach.com/2017/04/04/restful-api-security-principles/> "Fail-safe defaults Access to any resource (like API endpoint) should be denied by default. Access granted only in case of specific permission.

**NEW QUESTION 153**

- (Topic 2)

Refer to the exhibit.

```
Switch1# show interfaces trunk
I Output omitted for brevity
Port Mode Encapsulation Status Native
Gi1/0/20 auto 802.1q trunking 10

Port Vlans allowed on trunk
Gi1/0/20 1-4094

Switch2# show interfaces trunk
I Output omitted for brevity
Port Mode Encapsulation Status Native
Gi1/0/20 auto 802.1q trunking 10

Port Vlans allowed on trunk
Gi1/0/20 1-4094
```

The trunk does not work over the back-to-back link between Switch1 interface Gig1/0/20 and Switch2 interface Gig1/0/20. Which configuration fixes the problem?

- A)  
Switch1(config)#interface gig1/0/20  
Switch1(config-if)#switchport mode dynamic auto
- B)  
Switch2(config)#interface gig1/0/20  
Switch2(config-if)#switchport mode dynamic desirable
- C)  
Switch1(config)#interface gig1/0/20  
Switch1(config-if)#switchport trunk native vlan 1  
Switch2(config)#interface gig1/0/20  
Switch2(config-if)#switchport trunk native vlan 1
- D)  
Switch2(config)#interface gig1/0/20  
Switch2(config-if)#switchport mode dynamic auto

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

**Answer: B**

**NEW QUESTION 154**

- (Topic 2)

An engineer must create an EEM applet that sends a syslog message in the event a change happens in the network due to trouble with an OSPF process. Which action should the engineer use?

```
event manager applet LogMessage
  event routing network 172.30.197.0/24 type all
```

- A. action 1 syslog msg "OSPF ROUTING ERROR"
- B. action 1 syslog send "OSPF ROUTING ERROR"
- C. action 1 syslog pattern "OSPF ROUTING ERROR"
- D. action 1 syslog write "OSPF ROUTING ERROR"

**Answer: C**

**NEW QUESTION 157**

- (Topic 2)

Refer to the exhibit.

```
>>> 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'
```

Which Python code snippet prints the descriptions of disabled interfaces only?

A)

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

B)

```
for interface in netconf_data["GigabitEthernet"]:
    print(interface["enabled"])
    print(interface["description"])
```

C)

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

D)

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

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

**Answer: D**

**NEW QUESTION 159**

- (Topic 2)

Which two GRE features are configured to prevent fragmentation? (Choose two.)



**NEW QUESTION 167**

DRAG DROP - (Topic 2)

An engineer creates the configuration below. Drag and drop the authentication methods from the left into the order of priority on the right. Not all options are used.

```
R1#sh run | i aaa
aaa new-model
aaa authentication login default group ACE group AAA_RADIUS local-case
aaa session-id common
R1#
```

AAA servers of AAA\_RADIUS group

local configured username in non-case-sensitive format

local configured username in case-sensitive format

AAA servers of ACE group

tacacs servers of group ACE

If no method works, then deny login.

- A. Mastered
- B. Not Mastered

**Answer:** A

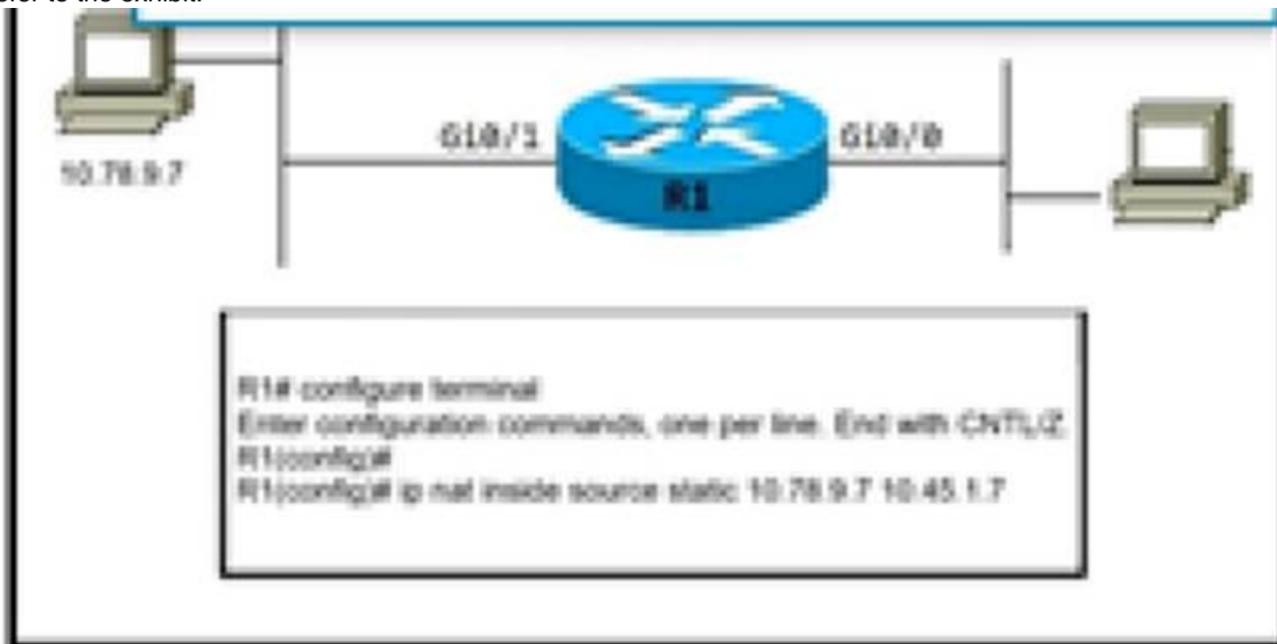
**Explanation:**

priority 1: AAA servers of ACE group  
 priority 2: AAA servers of AAA\_RADIUS group  
 priority 3: local configured username in case-sensitive format  
 priority 4: If no method works, then deny login

**NEW QUESTION 170**

- (Topic 2)

Refer to the exhibit.



A network architect has partially configured static NAT. which commands should be asked to complete the configuration?

- A. R1(config)#interface GigabitEthernet0/0 R1(config)#ip nat outside R1(config)#interface GigabitEthernet0/1 R1(config)#ip nat inside
- B. R1(config)#interface GigabitEthernet0/0 R1(config)#ip nat outside R1(config)#interface GigabitEthernet0/1 R1(config)#ip nat inside
- C. R1(config)#interface GigabitEthernet0/0 R1(config)#ip nat inside R1(config)#interface GigabitEthernet0/1 R1(config)#ip nat outside
- D. R1(config)#interface GigabitEthernet0/0 R1(config)#ip nat inside R1(config)#interface GigabitEthernet0/1 R1(config)#ip nat outside

**Answer:** B

**NEW QUESTION 171**

- (Topic 2)

Which two parameters are examples of a QoS traffic descriptor? (Choose two)

- A. MPLS EXP bits
- B. bandwidth
- C. DSCP
- D. ToS

E. packet size

**Answer:** AC

#### NEW QUESTION 172

- (Topic 2)

A network monitoring system uses SNMP polling to record the statistics of router interfaces. The SNMP queries work as expected until an engineer installs a new interface and reloads the router. After this action, all SNMP queries for the router fail. What is the cause of this issue?

- A. The SNMP community is configured incorrectly.
- B. The SNMP interface index changed after reboot.
- C. The SNMP server traps are disabled for the interface index.
- D. The SNMP server traps are disabled for the link state.

**Answer:** B

#### NEW QUESTION 173

- (Topic 2)

An engineer must create an EEM script to enable OSPF debugging in the event the OSPF neighborhood goes down. Which script must the engineer apply?

- event manager applet ENABLE\_OSPF\_DEBUG  
event syslog pattern "%OSPF-5-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from LOADING to FULL"  
action 1.0 cli command "enable"  
action 2.0 cli command "debug ip ospf event"  
action 3.0 cli command "debug ip ospf adj"  
action 4.0 syslog priority informational msg "ENABLE\_OSPF\_DEBUG"
- event manager applet ENABLE\_OSPF\_DEBUG  
event syslog pattern "%OSPF-5-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from LOADING to FULL"  
action 1.0 cli command "debug ip ospf event"  
action 2.0 cli command "debug ip ospf adj"  
action 3.0 syslog priority informational msg "ENABLE\_OSPF\_DEBUG"
- event manager applet ENABLE\_OSPF\_DEBUG  
event syslog pattern "%OSPF-5-ADJCHG: Process 6, Nbr 1.1.1.1 on Serial0/0 from FULL to DOWN"  
action 1.0 cli command "enable"  
action 2.0 cli command "debug ip ospf event"  
action 3.0 cli command "debug ip ospf adj"  
action 4.0 syslog priority informational msg "ENABLE\_OSPF\_DEBUG"
- event manager applet ENABLE\_OSPF\_DEBUG  
event syslog pattern "%OSPF-1-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from FULL to DOWN"  
action 1.0 cli command "debug ip ospf event"  
action 2.0 cli command "debug ip ospf adj"  
action 3.0 syslog priority informational msg "ENABLE\_OSPF\_DEBUG"

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

**Answer:** C

#### NEW QUESTION 176

- (Topic 2)

Refer to the exhibit.

Person#1:  
 First Name is Johnny  
 Last Name is Table  
 Hobbies are:  
 • Running  
 • Video games

Person#2:  
 First Name is Billy  
 Last Name is Smith  
 Hobbies are:  
 • Napping  
 • Reading

Which JSON syntax is derived from this data?

- A) 

```
{{"First Name": "Johnny", "Last Name": "Table", "Hobbies": ["Running", "Video games"]}, {"First Name": "Billy", "Last Name": "Smith", "Hobbies": ["Napping", "Reading"]}}
```
- B) 

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

```
{{"First Name": "Johnny", "Last Name": "Table", "Hobbies": "Running", "Hobbies": "Video games"}, {"First Name": "Billy", "Last Name": "Smith", "Hobbies": "Napping", "Hobbies": "Reading"}}
```
- D) 

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

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

**Answer: D**

**NEW QUESTION 178**

- (Topic 2)

Which two items are found in YANG data models? (Choose two.)

- A. HTTP return codes
- B. rpc statements
- C. JSON schema
- D. container statements
- E. XML schema

**Answer: CE**

**NEW QUESTION 182**

DRAG DROP - (Topic 2)

Drag and drop the snippets onto the blanks within the code to construct a script that configures BGP according to the topology. Not all options are used, and some options may be used twice.

```
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
    <router>
      <ios-bgp:bgp>
        <ios-bgp:id> /ios-bgp:id
        <ios-bgp:neighbor>
          <ios-bgp:id> /ios-bgp:id
          <ios-bgp:remote-as> /ios-bgp:remote-as
        </ios-bgp:neighbor>
        <ios-bgp:address-family>
          <ios-bgp:no-vrf>
          <ios-bgp:ipv4>
            <ios-bgp:af-name>unicast</ios-bgp:af-name>
            <ios-bgp:ipv4-unicast>
              <ios-bgp:neighbor>
                <ios-bgp:id> /ios-bgp:id
                <ios-bgp:soft-reconfiguration>inbound</ios-bgp:soft-reconfiguration>
              </ios-bgp:neighbor>
            </ios-bgp:ipv4-unicast>
          </ios-bgp:ipv4>
        </ios-bgp:address-family>
      </ios-bgp:bgp>
    </router>
  </native>
</config>
```



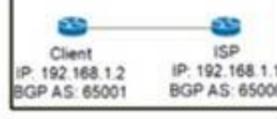
- 192.168.1.1
- 192.168.1.2
- 65000
- 65001
- Client
- ISP

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

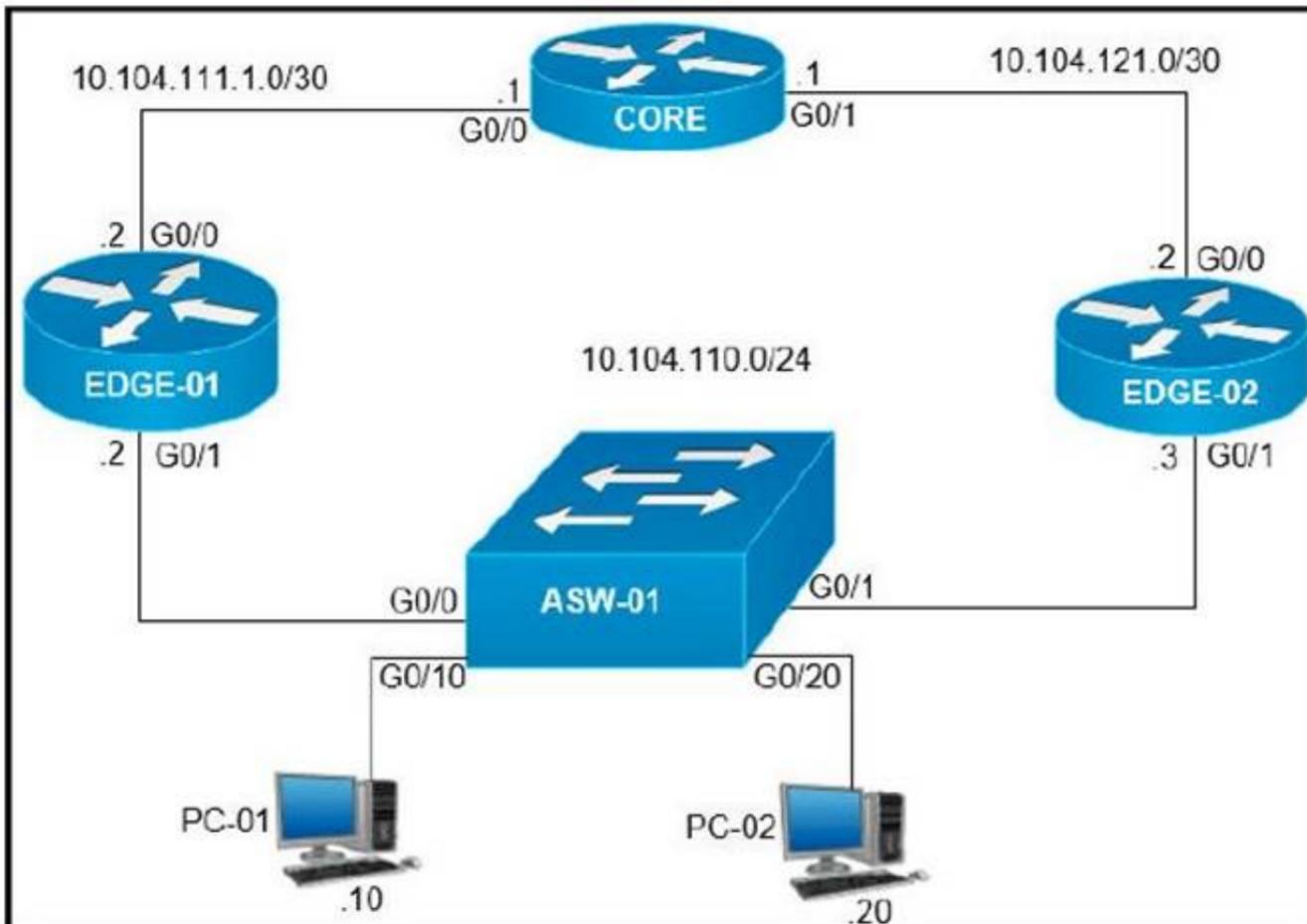
```
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
    <router>
      <ios-bgp:bgp>
        <ios-bgp:id> ISP
        <ios-bgp:neighbor>
          <ios-bgp:id> 192.168.1.1
          <ios-bgp:remote-as> 65001
        </ios-bgp:neighbor>
        <ios-bgp:address-family>
          <ios-bgp:no-vrf>
          <ios-bgp:ipv4>
            <ios-bgp:af-name>unicast</ios-bgp:af-name>
            <ios-bgp:ipv4-unicast>
              <ios-bgp:neighbor>
                <ios-bgp:id> 65001
                <ios-bgp:soft-reconfiguration>inbound</ios-bgp:soft-reconfiguration>
              </ios-bgp:neighbor>
            </ios-bgp:ipv4-unicast>
          </ios-bgp:ipv4>
        </ios-bgp:address-family>
      </ios-bgp:bgp>
    </router>
  </native>
</config>
```



- 192.168.1.1
- 192.168.1.2
- 65000
- 65001
- Client
- ISP

NEW QUESTION 183

- (Topic 2)  
 Refer to the exhibit.



On which interfaces should VRRP commands be applied to provide first hop redundancy to PC-01 and PC-02?

- A. G0/0 and G0/1 on Core
- B. G0/0 on Edge-01 and G0/0 on Edge-02
- C. G0/1 on Edge-01 and G0/1 on Edge-02
- D. G0/0 and G0/1 on ASW-01

**Answer:** C

#### NEW QUESTION 188

- (Topic 2)

What is the process for moving a virtual machine from one host machine to another with no downtime?

- A. high availability
- B. disaster recovery
- C. live migration
- D. multisite replication

**Answer:** C

#### NEW QUESTION 189

- (Topic 2)

What is the responsibility of a secondary WLC?

- A. It shares the traffic load of the LAPs with the primary controller.
- B. It avoids congestion on the primary controller by sharing the registration load on the LAPs.
- C. It registers the LAPs if the primary controller fails.
- D. It enables Layer 2 and Layer 3 roaming between itself and the primary controller.

**Answer:** C

#### NEW QUESTION 194

- (Topic 2)

Which DHCP option provides the CAPWAP APs with the address of the wireless controller(s)?

- A. 43
- B. 66
- C. 69
- D. 150

**Answer:** A

**Explanation:**

#### DHCP Option 43

DHCP option 43 is an option used for providing Wireless LAN Controller IP addresses to the AP. The DHCP option 43 is used to notify the AP to convert into CAPWAP AP.

#### NEW QUESTION 199

- (Topic 2)

How does a fabric AP fit in the network?

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

**Answer:** D

#### NEW QUESTION 200

- (Topic 2)

Refer to the exhibit.

```
mode random 1 out-of 2
exit
!
ip cef
!
interface GigabitEthernet 0/0/0
ip address 172.16.6.2 255.255.255.0
```

Which command set must be added to the configuration to analyze 50 packets out of every 100?

- A)  
**interface GigabitEthernet 0/0/0**  
**ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input**
- B)  
**sampler SAMPLER-1**  
**no mode random 1-out-of 2**  
**mode percent 50**
- interface GigabitEthernet 0/0/0**  
**ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input**
- C)  
**flow monitor FLOW-MONITOR-1**  
**record v4\_r1**  
**sampler SAMPLER-1**
- interface GigabitEthernet 0/0/0**  
**ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input**
- D)  
**sampler SAMPLER-1**  
**mode random 1-out-of 2**  
**flow FLOW-MONITOR-1**
- interface GigabitEthernet 0/0/0**  
**ip flow monitor SAMPLER-1 input**

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

**Answer: A**

#### **NEW QUESTION 204**

- (Topic 2)

Which technology uses network traffic telemetry, contextual information, and file reputation to provide insight into cyber threats?

- A. threat defense
- B. security services
- C. security intelligence
- D. segmentation

**Answer: C**

#### **NEW QUESTION 206**

- (Topic 2)

Which technology is used as the basis for the cisco sd-access data plane?

- A. IPsec
- B. LISP
- C. VXLAN
- D. 802.1Q

**Answer: C**

#### **Explanation:**

A virtual network identifier (VNI) is a value that identifies a specific virtual network in the data plane.

#### **NEW QUESTION 211**

- (Topic 1)

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

**NEW QUESTION 215**

- (Topic 1)

```

London
NewYork

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(O)
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?

A)

```

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#
    
```

B)

```

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#
    
```

C)

```

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#
    
```

D)

```
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#
```

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

Answer: D

**NEW QUESTION 219**

- (Topic 1)

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

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

Answer: B

**Explanation:**

The most common implementations of OAuth (OAuth 2.0) use one or both of these tokens:

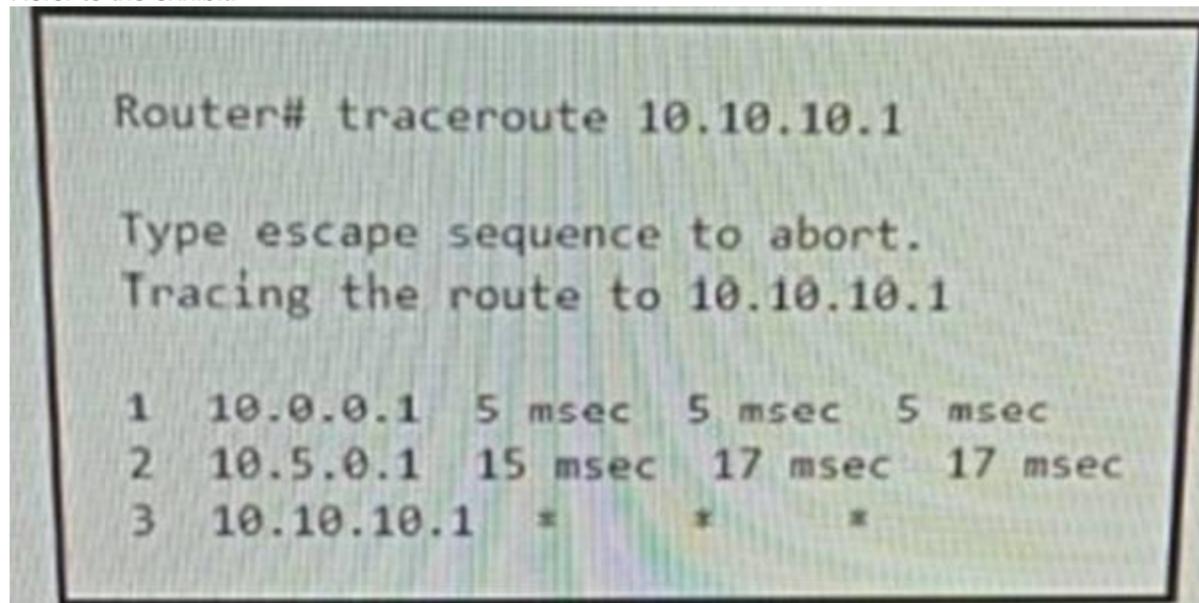
+ access token: sent like an API key, it allows the application to access a user's data; optionally, access tokens can expire.

+ refresh token: optionally part of an OAuth flow, refresh tokens retrieve a new access token if they have expired. OAuth2 combines Authentication and Authorization to allow more sophisticated scope and validity control.

**NEW QUESTION 220**

- (Topic 1)

Refer to the exhibit.



An engineer is troubleshooting a connectivity issue and executes a traceoute. What does the result confirm?

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

Answer: D

**Explanation:**

In Cisco routers, the codes for a traceroute command reply are:

! — success\* — time outN — network unreachableH — host unreachableP — protocol unreachableA — admin deniedQ — source quench received (congestion)? — unknown (any other ICMP message)

In Cisco routers, the codes for a traceroute command reply are:  
 ! — success\* — time outN — network unreachableH — host unreachableP — protocol unreachableA — admin deniedQ — source quench received (congestion)? — unknown (any other ICMP message)

**NEW QUESTION 225**

- (Topic 1)

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

- A. End user subnets and endpoints are part of the underlay network.

- B. The underlay switches provide endpoint physical connectivity for users.
- C. Static routing is a requirement,
- D. It must support IPv4 and IPv6 underlay networks

**Answer:** B

**Explanation:**

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

**NEW QUESTION 226**

- (Topic 1)

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

- A. Layer 3
- B. inter-xTR
- C. auto anchor
- D. fast roam

**Answer:** B

**Explanation:**

A fabric edge node provides onboarding and mobility services for wired users and devices (including fabric-enabled WLCs and APs) connected to the fabric. It is a LISP tunnel router (xTR) that also provides the anycast gateway, endpoint authentication, and assignment to overlay host pools (static or DHCP), as well as group-based policy enforcement (for traffic to fabric endpoints).

From Cisco's guide, under SDA roaming - When a client on a fabric enabled WLAN, roams from an access point to another access point on a different access-switch, it is called Inter- xTR, like a highway. Intra is within intra is between. Like interstate highways. That's how I remember. [https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b\\_wl\\_16\\_10\\_cg/mobility.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/mobility.html)

**NEW QUESTION 230**

- (Topic 1)

Which design principle states that a user has no access by default to any resource, and unless a resource is explicitly granted, it should be denied?

- A. least privilege
- B. fail-safe defaults
- C. economy of mechanism
- D. complete mediation

**Answer:** B

**NEW QUESTION 235**

- (Topic 1)

Which entity is responsible for maintaining Layer 2 isolation between segments In a VXLAN environment?

- A. switch fabric
- B. VTEP
- C. VNID
- D. host switch

**Answer:** C

**Explanation:**

The 24-bit VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments. VXLAN uses an 8-byte VXLAN header that consists of a 24-bit VNID and a few reserved bits. The VXLAN header together with the original Ethernet frame goes in the UDP payload. The 24-bit VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments.

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/vxlan/configuration/guide/b\\_Cisco\\_Nexus\\_9000\\_Series\\_NX-OS\\_VXLAN\\_Configuration\\_Guide\\_7x/b\\_Cisco\\_Nexus\\_9000\\_Series\\_NX-OS\\_VXLAN\\_Configuration\\_Guide\\_7x\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/vxlan/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_7x_chapter_010.html)

**NEW QUESTION 240**

- (Topic 1)

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state      conn-id status
209.165.201.6 209.165.201.1 QM_IDLE    1001 ACTIVE
```

Refer to the exhibit. After configuring an IPsec VPN, an engineer enters the show command to verify the ISAKMP SA status. What does the status show?

- A. ISAKMP SA is authenticated and can be used for Quick Mode.
- B. Peers have exchanged keys, but ISAKMP SA remains unauthenticated.
- C. VPN peers agreed on parameters for the ISAKMP SA
- D. ISAKMP SA has been created, but it has not continued to form.

**Answer:** B

**Explanation:**

The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM\_IDLE, and a Quick Mode exchange begins.  
<https://www.ciscopress.com/articles/article.asp?p=606584>

**NEW QUESTION 242**

- (Topic 1)  
 which entity is a Type 1 hypervisor?

- A. Oracle VM VirtualBox
- B. VMware server
- C. Citrix XenServer
- D. Microsoft Virtual PC

**Answer: C**

**NEW QUESTION 246**

- (Topic 1)  
 Which congestion queuing method on Cisco IOS based routers uses four static queues?

- A. Priority
- B. custom
- C. weighted fair
- D. low latency

**Answer: A**

**NEW QUESTION 247**

- (Topic 1)

```

R1
router bgp 1000
address-family ipv4 unicast
neighbor 209.165.201.2 remote-as 2000
network 10.0.0.0 mask 255.255.255.0
description Peer Router B

R2
router bgp 2000
address-family ipv4 unicast
neighbor 209.165.201.1 remote-as 1000
network 10.0.0.0 mask 255.255.255.0
description Peer Router A
    
```

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

- A. R1#network 192.168.0.0 mask 255.255.0.0
- B. R2#no network 10.0.0.0 255.255.255.0
- C. R2#network 192.168.0.0 mask 255.255.0.0
- D. R2#network 209.165.201.0 mask 255.255.192.0
- E. R1#no network 10.0.0.0 255.255.255.0

**Answer: BC**

**NEW QUESTION 248**

DRAG DROP - (Topic 1)  
 Drag and drop the threat defense solutions from the left onto their descriptions on the right.

Umbrella	provides malware protection on endpoints
AMP4E	provides IPS/IDS capabilities
FTD	performs security analytics by collecting network flows
StealthWatch	protects against email threat vector
ESA	provides DNS protection

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Umbrella	AMP4E
AMP4E	FTD
FTD	StealthWatch
StealthWatch	ESA
ESA	Umbrella

**NEW QUESTION 249**

- (Topic 1)

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. R1 becomes the active router.
- B. R1 becomes the standby router.
- C. If R2 goes down, R1 becomes active but reverts to standby when R2 comes back online.
- D. If R1 goes down
- E. R2 becomes active and remains the active device when R1 comes back online.
- F. If R1 goes down, R2 becomes active but reverts to standby when R1 comes backonline.

Answer: AD

**NEW QUESTION 254**

- (Topic 1)

Which outbound access list, applied to the WAN interface of a router, permits all traffic except for http traffic sourced from the workstation with IP address 10.10.10.1?

A)

```
ip access-list extended 100
deny tcp host 10.10.10.1 any eq 80
permit ip any any
```

B)

```
ip access-list extended 200
deny tcp host 10.10.10.1 eq 80 any
permit ip any any
```

C)

```
ip access-list extended NO_HTTP
deny tcp host 10.10.10.1 any eq 80
```

D)

```
ip access-list extended 10
deny tcp host 10.10.10.1 any eq 80
permit ip any any
```

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

**Answer: A****NEW QUESTION 256**

- (Topic 1)

A network engineer is configuring Flexible Netflow and enters these commands Sampler Netflow1 Mode random one-out-of 100 Interface fastethernet 1/0 Flow-sampler netflow1 Which are two results of implementing this feature instead of traditional Netflow? (Choose two.)

- A. CPU and memory utilization are reduced.
- B. Only the flows of top 100 talkers are exported
- C. The data export flow is more secure.
- D. The number of packets to be analyzed are reduced
- E. The accuracy of the data to be analyzed is improved

**Answer: AD****NEW QUESTION 261**

- (Topic 1)

```
aaa new-model
aaa authentication login authorizationlist tacacs+
tacacs-server host 192.168.0.202
tacacs-server key ciscotestkey
line vty 0 4
login authentication authorizationlist
```

Refer to the exhibit. What is the effect of this configuration?

- A. When users attempt to connect to vty lines 0 through 4, the device will authenticate them against TACACS+ if local authentication fails
- B. The device will authenticate all users connecting to vty lines 0 through 4 against TACACS+
- C. The device will allow users at 192.168.0.202 to connect to vty lines 0 through 4 using the password ciscotestkey
- D. The device will allow only users at 192.166.0.202 to connect to vty lines 0 through 4

**Answer: B****NEW QUESTION 266**

- (Topic 1)

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

**Answer:** D

**Explanation:**

SW1 has been configured with the following commands: SW1(config)#monitor session 1 source remote vlan 50 SW1(config)#monitor session 2 source interface fa0/14 SW1(config)#monitor session 2 destination interface fa0/15

The session 1 on SW1 was configured for Remote SPAN (RSPAN) while session 2 was configured for local SPAN. For RSPAN we need to configure the destination port to complete the configuration.

Note: In fact we cannot create such a session like session 1 because if we only configure Source RSPAN VLAN 50 (with the command monitor session 1 source remote vlan 50) then we will receive a Type: Remote Source Session (not Remote Destination Session).

**NEW QUESTION 269**

- (Topic 1)

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

- A. sniffer
- B. monitor
- C. bridge
- D. local

**Answer:** B

**NEW QUESTION 272**

- (Topic 1)

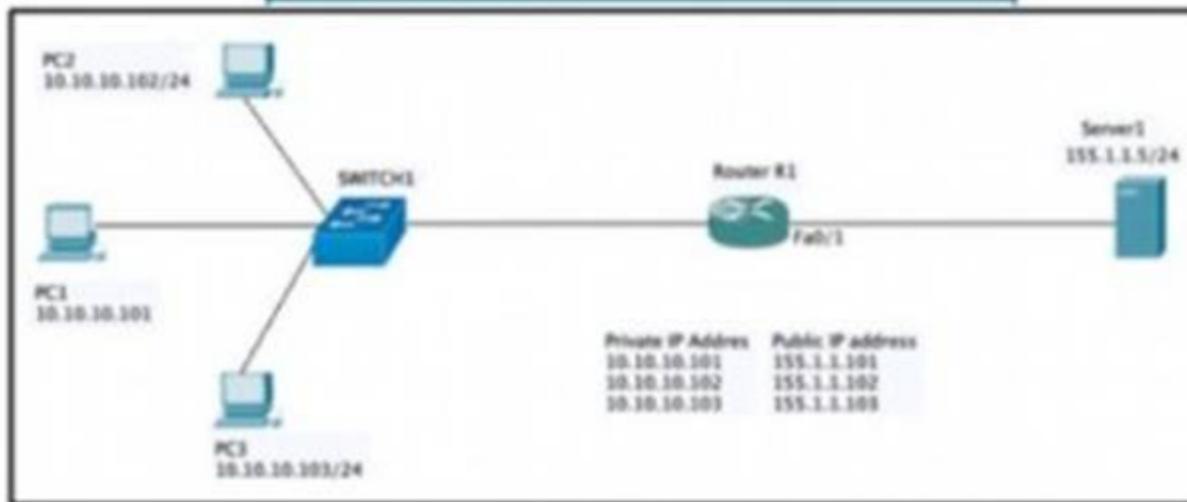
Which device makes the decision for a wireless client to roam?

- A. wireless client
- B. wireless LAN controller
- C. access point
- D. WCS location server

**Answer:** A

**NEW QUESTION 276**

- (Topic 1)



Refer to the exhibit. Which set of commands on router r R1 Allow deterministic translation of private hosts PC1, PC2, and PC3 to addresses in the public space?  
 A)

```
RouterR1(config)#int f0/0
RouterR1(config-if)#ip nat inside
RouterR1(config-if)#exit
RouterR1(config)#int f0/1
RouterR1(config-if)#ip nat outside
RouterR1(config-if)#exit
RouterR1(config)#ip nat inside source static 10.10.10.101 155.1.1.101
RouterR1(config)#ip nat inside source static 10.10.10.102 155.1.1.102
RouterR1(config)#ip nat inside source static 10.10.10.103 155.1.1.103
```

B)

```
RouterR1(config)#int f0/0
RouterR1(config-if)#ip nat inside
RouterR1(config-if)#exit
RouterR1(config)#int f0/1
RouterR1(config-if)#ip nat outside
RouterR1(config-if)#exit
RouterR1(config)#ip nat inside source static 10.10.10.101 155.1.1.101
RouterR1(config)#ip nat inside source static 10.10.10.102 155.1.1.102
RouterR1(config)#ip nat inside source static 10.10.10.103 155.1.1.103
```

C)

```
RouterR1(config)#int f0/0
RouterR1(config-if)#ip nat inside
RouterR1(config-if)#exit
RouterR1(config)#int f0/1
RouterR1(config-if)#ip nat outside
RouterR1(config-if)#exit
RouterR1(config)#access-list 1 10.10.10.0 0.0.0.255
RouterR1(config)#ip nat pool POOL 155.1.1.101 155.1.1.103 netmask 255.255.255.0
RouterR1(config)#ip nat inside source list 1 pool POOL
```

D)

```
RouterR1(config)#int f0/0
RouterR1(config-if)#ip nat inside
RouterR1(config-if)#exit
RouterR1(config)#int f0/1
RouterR1(config-if)#ip nat outside
RouterR1(config-if)#exit
RouterR1(config)#access-list 1 10.10.10.0 0.0.0.255
RouterR1(config)#ip nat inside source list 1 interface f0/1 overload
```

- A. Option A
- B. Option B

- C. Option C
- D. Option D

Answer: A

**NEW QUESTION 279**

- (Topic 1)



Refer to the exhibit. An engineer attempts to configure a trunk between switch sw1 and switch SW2 using DTP, but the trunk does not form. Which command should the engineer apply to switch SW2 to resolve this issue?

- A. switchport mode dynamic desirable
- B. switchport nonegotiate
- C. no switchport
- D. switchport mode access

Answer: A

**NEW QUESTION 283**

- (Topic 1)

Which characteristic distinguishes Ansible from Chef?

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

Answer: C

**NEW QUESTION 284**

- (Topic 1)

**Router2# show policy-map control-plane****Control Plane****Service-policy input: CISCO****Class-map: CISCO (match-all)**

20 packets, 11280 bytes

5 minute offered rate 0 bps, drop rate 0 bps

Match: access-group 120

police:

8000 bps, 1500 limit, 1500 extended limit

conformed 15 packets, 6210 bytes; action: transmit

exceeded 5 packets, 5070 bytes; action: drop

violated 0 packets, 0 bytes; action: drop

conformed 0 bps, exceed 0 bps, violate 0 bps

**Class-map: class-default (match-any)**

105325 packets, 11415151 bytes

5 minute offered rate 0 bps, drop rate 0 bps

Match: any

Refer to the exhibit. An engineer configures CoPP and enters the show command to verify the implementation. What is the result of the configuration?

- A. All traffic will be policed based on access-list 120.
- B. If traffic exceeds the specified rate, it will be transmitted and remarked.
- C. Class-default traffic will be dropped.
- D. ICMP will be denied based on this configuration.

**Answer: A**

**NEW QUESTION 287**

- (Topic 1)

Which controller is capable of acting as a STUN server during the onboarding process of Edge devices?

- A. vBond
- B. vSmart
- C. vManage
- D. PNP server

**Answer: A**

**NEW QUESTION 292**

- (Topic 1)

What are two benefits of virtual switching when compared to hardware switching? (Choose two.)

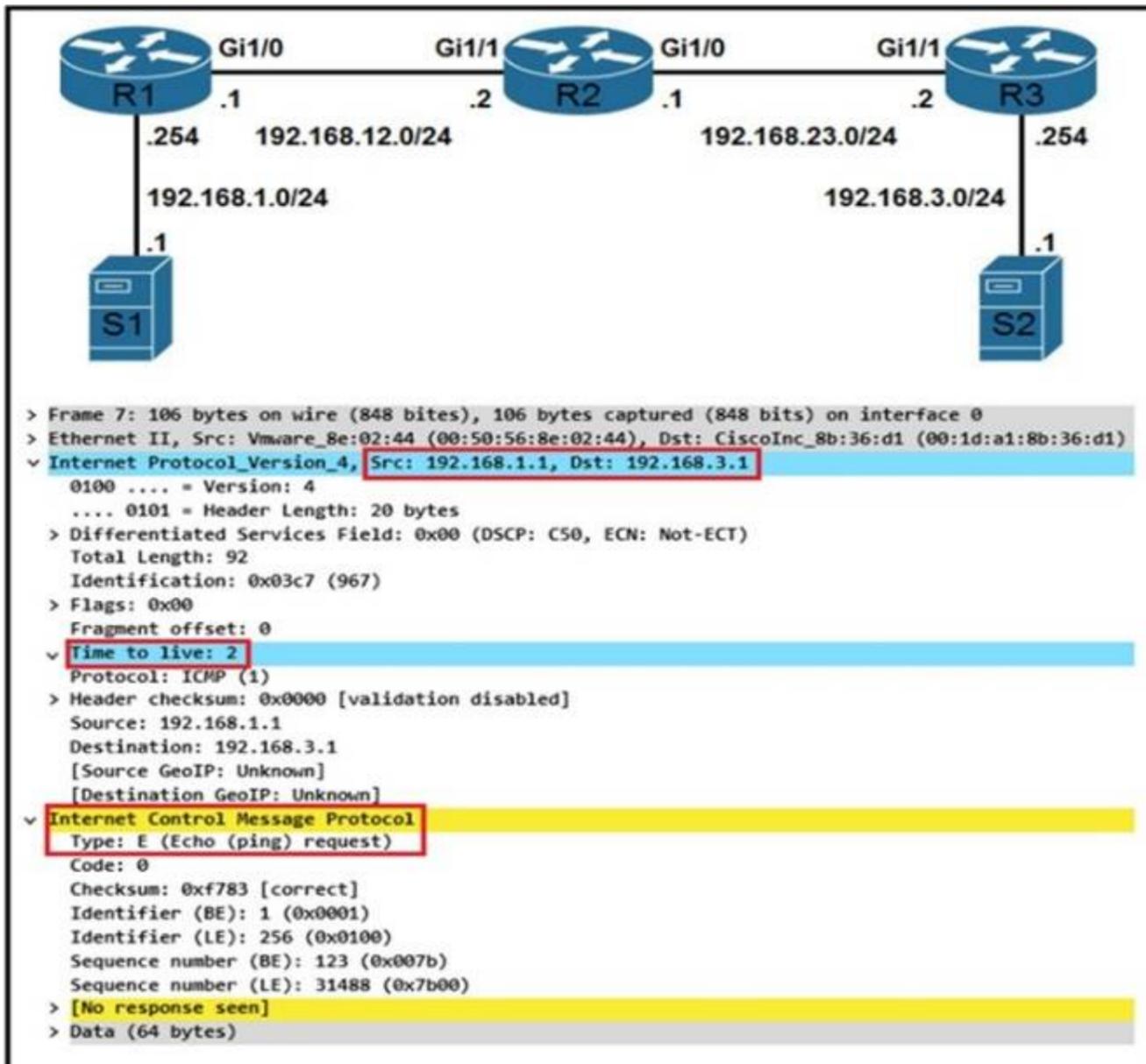
- A. increased MTU size
- B. hardware independence
- C. VM-level isolation
- D. increased flexibility
- E. extended 802.1Q VLAN range

**Answer: CD**

**NEW QUESTION 293**

- (Topic 1)

Refer to the exhibit.



Which troubleshooting a routing issue, an engineer issues a ping from S1 to S2. When two actions from the initial value of the TTL? (Choose two.)

- A. The packet reaches R3, and the TTL expires
- B. R2 replies with a TTL exceeded message
- C. R3 replies with a TTL exceeded message.
- D. The packet reaches R2 and the TTL expires
- E. R1 replies with a TTL exceeded message
- F. The packet reaches R1 and the TTL expires.

Answer: AD

**Explanation:**

Source MAC in the capture is VMWare, MAC is Cisco. Routers first check the TTL before any further process, subtract 1 at R1. Send to R2, subtract and you have ZERO. Discard packet and reply with ICMP Time Exceeded message from that point, don't even bother checking the Route table for further processing.

**NEW QUESTION 298**

- (Topic 1)

If the noise floor is -90 dBm and wireless client is receiving a signal of -75 dBm, what is the SNR?

- A. 15
- B. 1.2
- C. -165
- D. .83

Answer: A

**NEW QUESTION 303**

- (Topic 1)

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?

A)

```
monitor session 2 source interface gigabitethernet0/3 tx
monitor session 2 filter vlan 3
```

B)

```
monitor session 2 source interface gigabitethernet0/3 tx
monitor session 2 filter vlan 1 - 2 , 4 - 4094
```

C)

```
monitor session 2 source interface gigabitethernet0/3 rx  
monitor session 2 filter vlan 3
```

D)

```
monitor session 2 source interface gigabitethernet0/3 rx  
monitor session 2 filter vlan 1 - 2 , 4 - 4094
```

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

Answer: A

**NEW QUESTION 305**

- (Topic 1)

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

A)

```
standby 300 priority 110  
standby 300 timers 1 110
```

B)

```
standby version 2  
standby 300 priority 110  
standby 300 preempt
```

C)

```
standby 300 priority 90  
standby 300 preempt
```

D)

```
standby version 2  
standby 300 priority 90  
standby 300 preempt
```

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

Answer: B

**NEW QUESTION 310**

- (Topic 1)

```
ip vrf BLUE
 rd 1:1
!
interface Vlan100
 description GLOBAL_INTERFACE
 ip address 10.10.1.254 255.255.255.0
!
access-list 101 permit ip 10.10.5.0 0.0.0.255 10.10.1.0
255.255.255.0
!
route-map VRF_TO_GLOBAL permit 10
 match ip address 101
 set global
!
interface Vlan500
 description VRF_BLUE
 ip vrf forwarding BLUE
 ip address 10.10.5.254 255.255.255.0
 ip policy route-map VRF_TO_GLOBAL
```

Refer to the exhibit. An engineer attempts to create a configuration to allow the Blue VRF to leak into the global routing table, but the configuration does not function as expected. Which action resolves this issue?

- A. Change the access-list destination mask to a wildcard.
- B. Change the source network that is specified in access-list 101.
- C. Change the route-map configuration to VRF\_BLUE.
- D. Change the access-list number in the route map

**Answer: A**

#### NEW QUESTION 314

- (Topic 1)

Where is radio resource management performed in a Cisco SD-access wireless solution?

- A. DNA Center
- B. control plane node
- C. wireless controller
- D. Cisco CMX

**Answer: C**

#### Explanation:

Fabric wireless controllers manage and control the fabric-mode APs using the same general model as the traditional local-mode controllers which offers the same operational advantages such as mobility control and radio resource management. A significant difference is that client traffic from wireless endpoints is not tunneled from the APs to the wireless controller. Instead, communication from wireless clients is encapsulated in VXLAN by the fabric APs which build a tunnel to their first-hop fabric edge node. Wireless traffic is tunneled to the edge nodes as the edge nodes provide fabric services such as the Layer 3 Anycast Gateway, policy, and traffic enforcement. <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html>

#### NEW QUESTION 319

- (Topic 1)

How does an on-premises infrastructure compare to a cloud infrastructure?

- A. On-premises can increase compute power faster than cloud
- B. On-premises requires less power and cooling resources than cloud
- C. On-premises offers faster deployment than cloud
- D. On-premises offers lower latency for physically adjacent systems than cloud.

**Answer: D**

#### NEW QUESTION 321

- (Topic 1)

Which TCP setting is tuned to minimize the risk of fragmentation on a GRE/IP tunnel?

- A. MTU
- B. Window size
- C. MRU
- D. MSS

**Answer: D**

#### Explanation:

The TCP Maximum Segment Size (TCP MSS) defines the maximum amount of data that a host is willing to accept in a single TCP/IP datagram. This TCP/IP datagram might be fragmented at the IP layer. The MSS value is sent as a TCP header option only in TCP SYN segments. Each side of a TCP connection reports its MSS value to the other side. Contrary to popular belief, the MSS value is not negotiated between hosts. The sending host is required to limit the size of data in a single

TCP segment to a value less than or equal to the MSS reported by the receiving host. TCP MSS takes care of fragmentation at the two endpoints of a TCP connection, but it does not handle the case where there is a smaller MTU link in the middle between these two endpoints. PMTUD was developed in order to avoid fragmentation in the path between the endpoints. It is

**NEW QUESTION 326**

- (Topic 1)

What is the output of this code?

```
def get_credentials():
    creds={'username': 'cisco', 'password': 'c3577dc8ae4e36c0bfb6fe5398614245'}
    return (creds.get('username'))

print(get_credentials())
```

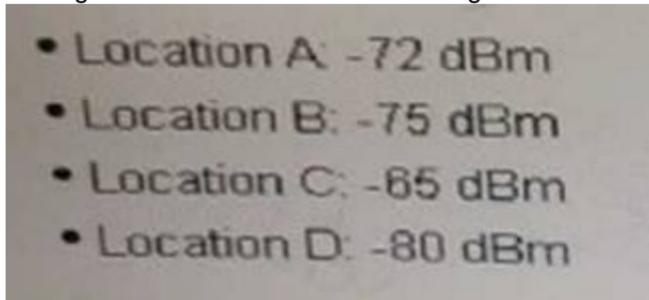
- A. username Cisco
- B. get\_credentials
- C. username
- D. CISCO

**Answer: D**

**NEW QUESTION 328**

- (Topic 1)

An engineer measures the Wi-Fi coverage at a customer site. The RSSI values are recorded as follows:



Which two statements does the engineer use to explain these values to the customer? (Choose two)

- A. The signal strength at location C is too weak to support web surfing
- B. Location D has the strongest RF signal strength
- C. The RF signal strength at location B is 50% weaker than location A
- D. The signal strength at location B is 10 dB better than location C
- E. The RF signal strength at location C is 10 times stronger than location B

**Answer: CE**

**NEW QUESTION 333**

- (Topic 1)

"HTTP/1.1 204 content" is returned when `curl -I -x delete` command is issued. Which situation has occurred?

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

**Answer: B**

**Explanation:**

HTTP Status 204 (No Content) indicates that the server has successfully fulfilled the request and that there is no content to send in the response payload body.

**NEW QUESTION 334**

- (Topic 1)

What is one benefit of implementing a VSS architecture?

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

**Answer: C**

**Explanation:**

Support Virtual Switching System (VSS) to provide resiliency, and increased operational efficiency with a single point of management; VSS increases operational efficiency by simplifying the network, reducing switch management overhead by at least 50 percent. – Single configuration file and node to manage. Removes the need to configure redundant switches twice with identical policies.

**NEW QUESTION 335**

- (Topic 4)

A network administrator is designing a new network for a company that has frequent power spikes. The company wants to ensure that employees can the best solution for the administrator to recommend?

- A. Generator
- B. Cold site
- C. Redundant power supplies
- D. Uninterruptible power supply

**Answer: D**

**Explanation:**

This is because an uninterruptible power supply (UPS) is a device that provides backup power to a network device or a computer in case of a power outage or a power spike. A UPS can prevent data loss, corruption, or damage to the device by providing a smooth and continuous power supply. A UPS can also protect the device from power surges, brownouts, or voltage fluctuations. The source of this answer is the Cisco ENCOR v1.1 course, module 2, lesson 2.1: Implementing Device Hardening.

**NEW QUESTION 338**

- (Topic 4)

Which of the following security methods uses physical characteristics of a person to authorize access to a location?

- A. Access control vestibule
- B. Palm scanner
- C. PIN pad
- D. Digital card reader
- E. Photo ID

**Answer: B**

**Explanation:**

This is because a palm scanner is a type of biometric security method that uses the physical characteristics of a person's palm, such as the shape, size, and vein patterns, to authorize access to a location. A palm scanner is more reliable and secure than other methods, such as a PIN pad or a digital card reader, which can be easily stolen, lost, or shared. A palm scanner is also more hygienic and convenient than other biometric methods, such as a fingerprint scanner or a facial recognition system, which can be affected by dirt, oil, or lighting conditions. The source of this answer is the Cisco ENCOR v1.1 course, module 2, lesson 2.2: Implementing Device Access Control.

**NEW QUESTION 339**

- (Topic 4)

Which two features are available only in next-generation firewalls? (Choose two.)

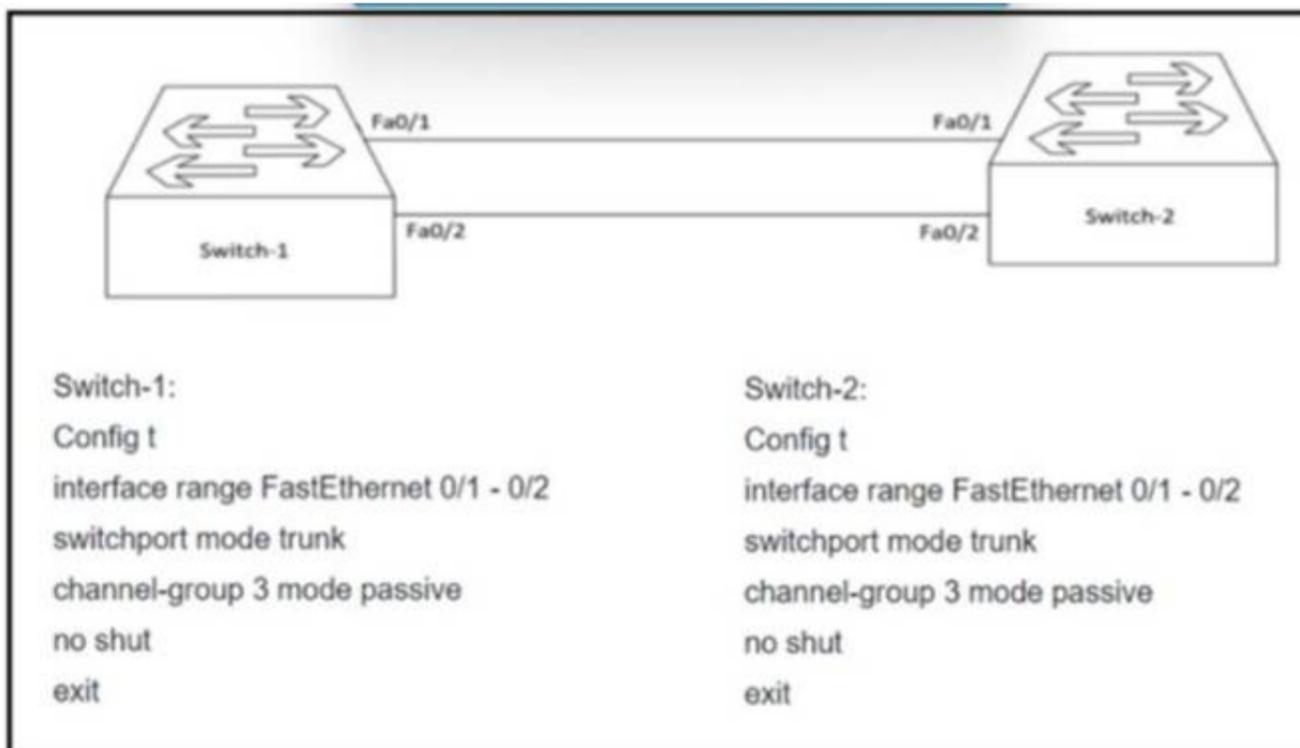
- A. virtual private network
- B. deep packet inspection
- C. stateful inspection
- D. application awareness
- E. packet filtering

**Answer: CD**

**NEW QUESTION 342**

- (Topic 4)

Refer to the exhibit.



An LACP port channel is configured between Switch-1 and Switch-2, but It falls to come up. Which action will resolve the issue?

- A. Configure Switch-1 with channel-group mode active
- B. Configure Switch-2 with channel-group mode desirable.
- C. Configure Switch-1 with channel-group mode on.
- D. Configure SwKch-2 with channel-group mode auto

Answer: A

**NEW QUESTION 343**

DRAG DROP - (Topic 4)

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

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

**NEW QUESTION 348**

- (Topic 4)

Which device, in a LISP routing architecture, receives and de-encapsulates LISP traffic for endpoints within a LISP-capable site?

- A. MR
- B. ETR
- C. OMS
- D. ITR

Answer: B

**NEW QUESTION 352**

- (Topic 4)

An engineer applies this EEM applet to a router:

```
event manager applet Test
event timer watchdog time 600
action 1.0 cli command "enable"
action 2.0 cli command "term exec prompt timestamp"
action 3.0 cli command "term length 0"
action 4.0 cli command "show ip arp | in 0005.4210.0049"
action 5.0 regexp ".*(ARPA).*" $_cli_result
action 6.0 if $_regexp_result eq 1
action 7.0 syslog msg $_cli_result
action 8.0 end
```

What does the applet accomplish?

- A. It generates a syslog message every 600 seconds on the status of the specified MAC address.
- B. It checks the MAC address table every 600 seconds to see if the specified address has been learned.
- C. It compares syslog output to the MAC address table every 600 seconds and generates an event when there is a match.
- D. It compares syslog output to the MAC address table every 600 seconds and generates an event when no match is found.

**Answer: B**

#### NEW QUESTION 356

- (Topic 4)

How do the RIB and the FIB differ?

- A. FIB contains routes learned through a dynamic routing protocol, and the RIB contains routes that are static or directly connected.
- B. RIB contains the interface for a destination, and the FIB contains the next hop information.
- C. FIB is derived from the control plane, and the RIB is derived from the data plane.
- D. RIB is derived from the control plane, and the FIB is derived from the RIB.

**Answer: D**

#### NEW QUESTION 360

- (Topic 4)

What does the statement `print(format(0.8, '.0%'))` display?

- A. 80%
- B. 8%
- C. .08%
- D. 8.8%

**Answer: B**

#### NEW QUESTION 364

- (Topic 4)

What is stateful switchover?

- A. mechanism used to prevent routing protocol loops during an RP switchover
- B. mechanism to take control from a failed RP while maintaining connectivity
- C. First Hop Redundancy Protocol for host gateway connectivity
- D. cluster protocol used to facilitate switch failover

**Answer: D**

#### NEW QUESTION 366

- (Topic 4)

What is one benefit of implementing a data model language?

- A. accuracy of the operations performed
- B. uses XML style of data formatting
- C. machine-oriented logic and language-facilitated processing.
- D. conceptual representation to simplify interpretation.

**Answer: A**

#### NEW QUESTION 368

- (Topic 4)

Which of the following protocols has a default administrative distance value of 90?

- A. RIP
- B. EIGRP
- C. OSPF
- D. BGP

**Answer:** B

**Explanation:**

This is because EIGRP is an advanced distance vector routing protocol that uses a composite metric to calculate the best path to a destination. EIGRP has a default administrative distance value of 90, which means that it is more trustworthy than RIP (120) or OSPF (110), but less trustworthy than BGP (20). The source of this answer is the Cisco ENCOR v1.1 course, module 4, lesson 4.1: Implementing EIGRP.

**NEW QUESTION 369**

- (Topic 4)

What do Chef and Ansible have in common?

- A. They rely on a declarative approach.
- B. They rely on a procedural approach.
- C. They use YAML as their primary configuration syntax.
- D. They are clientless architectures.

**Answer:** B

**NEW QUESTION 373**

- (Topic 4)

When a DNS host record is configured for a new Cisco AireOS WLC, which hostname must be added to allow APs to successfully discover the WLC?

- A. CONTROLLER-CAPWAP-CISCO
- B. CISCO-CONTROLLER-CAPWAP
- C. CAPWAP-CISCO-CONTROLLER
- D. CISCO-CAPWAP-CONTROLLER

**Answer:** D

**NEW QUESTION 377**

- (Topic 4)

A technician is assisting a user who cannot connect to a website. The technician attempts to ping the default gateway and DNS server of the workstation. According to troubleshooting methodology, this is an example of:

- A. a divide-and-conquer approach.
- B. a bottom-up approach.
- C. a top-to-bottom approach.
- D. implementing a solution.

**Answer:** C

**Explanation:**

This is because a top-to-bottom approach is a troubleshooting methodology that starts from the highest layer of the OSI model and works its way down to the lowest layer. The technician is using this approach by first testing the network layer connectivity with the ping command, which uses the ICMP protocol. If the ping is successful, the technician can move on to the next layer, such as the transport layer or the application layer. If the ping fails, the technician can troubleshoot the lower layers, such as the data link layer or the physical layer. The source of this answer is the Cisco ENCOR v1.1 course, module 10, lesson 10.3: Applying Troubleshooting Methodologies.

**NEW QUESTION 380**

- (Topic 4)

```
monitor session 11 type erspan-source
source interface GigabitEthernet3
destination
erspan-id 12
ip address 10.10.10.10
origin ip address 10.100.10.10
```

Refer to the exhibit. Which command set completes the ERSPAN session configuration?

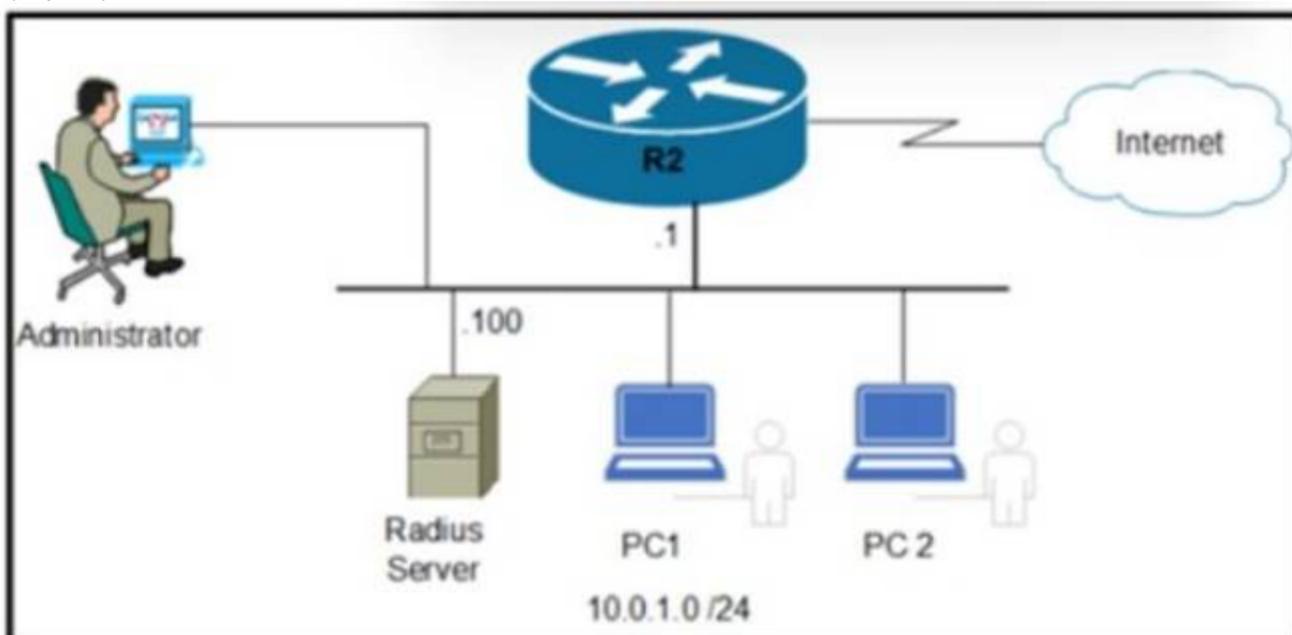
- monitor session 12 type erspan-destination  
destination interface GigabitEthernet4  
source  
erspan-id 12  
ip address 10.10.10.10
- monitor session 11 type erspan-destination  
destination interface GigabitEthernet4  
source  
erspan-id 12  
ip address 10.100.10.10
- monitor session 11 type erspan-destination  
destination interface GigabitEthernet4  
source  
erspan-id 11  
ip address 10.10.10.10
- monitor session 12 type erspan-destination  
destination interface GigabitEthernet4  
source  
erspan-id 11  
ip address 10.10.10.10

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

Answer: A

#### NEW QUESTION 384

- (Topic 4)



Refer to the exhibit. Which command set enables router R2 to be configured via NETCONF?

- A)
 

```
R1(config)# username Netconf privilege 15 password example_password
R1(config)# netconf-yang
R1(config)# netconf-yang feature candidate-datastore
```
- B)
 

```
R1(config)# snmp-server manager
R1(config)# snmp-server community ENCOR ro
```

C)

```
R1(config)# snmp-server manager
R1(config)# snmp-server community ENCOR rw
```

D)

```
R1(config)# netconf
R1(config)# ip http secure-server
```

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

**Answer:** A

#### NEW QUESTION 388

- (Topic 4)

What is a characteristics of Cisco SD-WAN?

- A. operates over DTLS/TLS authenticated and secured tunnels
- B. requires manual secure tunnel configuration
- C. uses unique per-device feature templates
- D. uses control connections between routers

**Answer:** A

#### NEW QUESTION 390

- (Topic 4)

Which function does a virtual switch provide?

- A. CPU context switching (or multitasking between virtual machines)
- B. RAID storage for virtual machines
- C. emulation of power for virtual machines.
- D. connectivity between virtual machines

**Answer:** D

#### Explanation:

This is because a virtual switch is a software-based switch that operates at the data link layer of the OSI model and provides connectivity between virtual machines that are running on the same physical host or different hosts. A virtual switch can also connect virtual machines to external networks, such as the Internet or a local area network, by using physical network adapters on the host. A virtual switch can perform the same functions as a physical switch, such as learning MAC addresses, forwarding frames, and applying VLANs. The source of this answer is the Cisco ENCOR v1.1 course, module 9, lesson 9.1: Implementing Network Virtualization.

#### NEW QUESTION 393

- (Topic 4)

A company hires a network architect to design a new OTT wireless solution within a Cisco

SD-Access Fabric wired network. The architect wants to register access points to the WLC to centrally switch the traffic. Which AP mode must the design include?

- A. Bridge
- B. Fabric
- C. FlexConnect
- D. local

**Answer:** D

#### NEW QUESTION 394

- (Topic 4)

What is one method for achieving REST API security?

- A. using built-in protocols known as Web Services Security
- B. using a combination of XML encryption and XML signatures
- C. using a MD5 hash to verify the integrity
- D. using HTTPS and TLS encryption

**Answer:** D

#### NEW QUESTION 397

- (Topic 4)

A customer wants to connect a device to an autonomous Cisco AP configured as a WGB. The WGB is configured properly; however, it fails to associate to a CAPWAP-enabled AP. Which change must be applied in the advanced WLAN settings to resolve this issue?

- A. Enable Aironet IE.
- B. Enable passive client.
- C. Disable AAA override.
- D. Disable FlexConnect local switching.

Answer: A

**NEW QUESTION 400**

- (Topic 4)

```
list = [1, 2, 3, 4]
list[3] = 10
print(list)
```

Refer to the exhibit. What is the value of the variable list after the code is run?

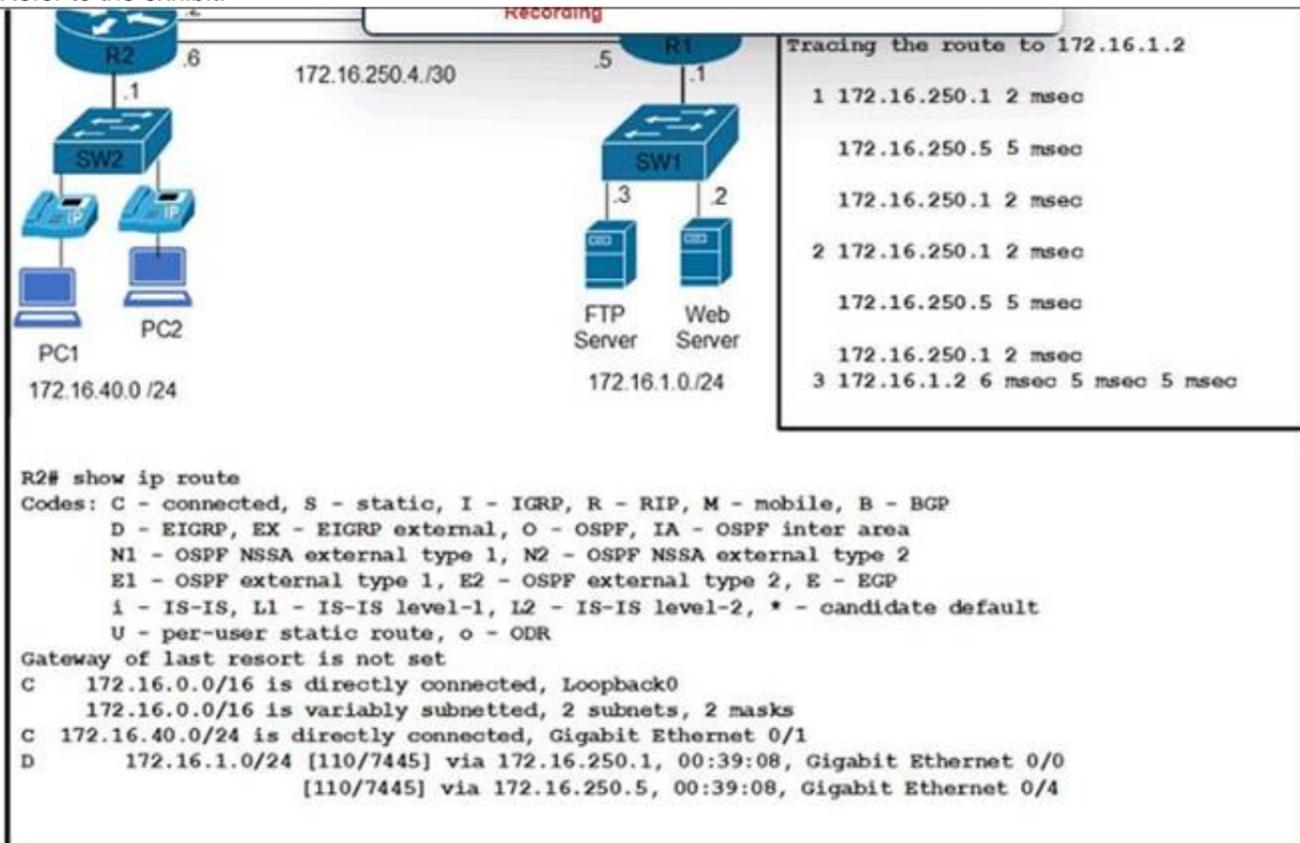
- A. [1, 2, 10]
- B. [1, 2, 3, 10]
- C. [1, 2, 10, 4]
- D. [1, 10, 10, 10]

Answer: B

**NEW QUESTION 401**

- (Topic 4)

Refer to the exhibit.



Clients are reporting an issue with the voice traffic from the branch site to the central site. What is the cause of this issue?

- A. The voice traffic is using the link with less available bandwidth.
- B. There is a routing loop on the network.
- C. Traffic is load-balancing over both links, causing packets to arrive out of order.
- D. There is a high delay on the WAN links.

Answer: C

**Explanation:**

Traffic is load-balancing over both links, causing packets to arrive out of order. This can cause voice quality issues, such as jitter and delay. To avoid this problem, voice traffic should be sent over a single path, using a routing protocol that supports unequal-cost load balancing, such as EIGRP. The source of this answer is the Cisco ENCOR v1.1 course, module 4, lesson 4.3: Implementing EIGRP.

**NEW QUESTION 403**

- (Topic 4)

```
ip access-list extended 101
 10 deny ip any any
!
event manager applet Block_Users
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "interface GigabitEthernet1"
 action 4.0 cli command "ip access-group 101 in"
 action 5.0 cli command "ip access-group 101 out"
```

Refer to the exhibit. An engineer builds an EEM script to apply an access list. Which statement must be added to complete the script?

- A. event none
- B. action 2.1 cli command "ip action 3.1 ell command 101"
- C. action 6.0 ell command "ip access-list extended 101"
- D. action 6.0 cli command "ip access-list extended 101"

Answer: A

**NEW QUESTION 407**

- (Topic 4)

Which configuration filters out DOT1X messages in the format shown below from being sent toward Syslog server 10.15.20.33?

- A) logging discriminator DOT1X facility drops DOT1X  
logging host 10.15.20.33 discriminator DOT1X
- B) logging discriminator DOT1X msg-body drops DOTX  
logging host 10.15.20.33 discriminator DOTX
- C) logging discriminator DOT1X mnemonics includes DOTX  
logging host 10.15.20.33 discriminator DOT1X
- D) logging discriminator DOT1X mnemonics includes DOT1X  
logging host 10.15.20.33 discriminator DOTX

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

Answer: A

**NEW QUESTION 408**

DRAG DROP - (Topic 4)

Drag and drop the code snippets from the bottom onto the blanks in the code to construct a request that configures a deny rule on an access list?

```
{
  "ip": {
    "access-list": {
      "ios-acl:extended": {
        "ios-acl:name": "ato",
        "ios-acl: [ ] ": {
          "ios-acl:sequence": "111111",
          "ios-acl:ace-rule": {
            "ios-acl:action": "[ ]",
            "ios-acl:protocol": "[ ]",
            "ios-acl:any": "",
            "ios-acl: [ ] ": ""
          }
        }
      }
    }
  }
}
```

- deny
- access-list-seq-rule
- dst-any
- ip

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```

{
  "ip": {
    "access-list": {
      "ios-acl:extended": {
        "ios-acl:name": "ato",
        "ios-acl:dst-any": "dst-any",
        "ios-acl:sequence": "111111",
        "ios-acl:ace-rule": {
          "ios-acl:action": "deny",
          "ios-acl:protocol": "ip",
          "ios-acl:any": "",
          "ios-acl:access-list-seq-rule": "access-list-seq-rule"
        }
      }
    }
  }
}

```

deny    access-list-seq-rule    dst-any    ip

**NEW QUESTION 413**

- (Topic 4)

Which JSON script is properly formatted?

A)

```

[
  "Session":{
    "title":"Writing 201",
    "grade":"11",
    "location":"Maine",
  }
]

```

B)

```

{
  "river": [
    {
      "name":"Mississippi",
      "state":"Louisiana",
      "ranking":"13"
    }
  ]
}

```

C)

```

"paint":[
  {
    "type":"indoor",
    "color":"white",
    "sheen":"satin"
  }
]

```

D)

```
{
  "file":
  [
    "name":"File_4616,
    "location":"User_files",
    "bytes":"13070",
  ]
}
```

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

**Answer:** A

**Explanation:**

Option A is the properly formatted JSON script. JSON (JavaScript Object Notation) is a standard text-based format for representing structured data based on JavaScript object syntax. It is commonly used for transmitting data in web applications (e.g., sending some data from the server to the client, so it can be displayed on a web page, or vice versa). The JSON syntax rules are as follows<sup>12</sup>:

? Data is in name/value pairs, separated by commas. A name/value pair consists of a field name (in double quotes), followed by a colon, followed by a value: "name": "value".

? Curly braces hold objects. An object can contain multiple name/value pairs: {"name": "value", "name": "value", ...}.

? Square brackets hold arrays. An array can contain multiple values, separated by commas: ["value", "value", ...].

? Values can be strings (in double quotes), numbers, booleans (true or false), null, objects, or arrays.

Option A follows these rules and is a valid JSON script. It defines an object with four name/value pairs: "name", "age", "hobbies", and "address". The value of "name" is a string, the value of "age" is a number, the value of "hobbies" is an array of strings, and the value of "address" is another object with two name/value pairs: "city" and "country". The object is enclosed in curly braces and the name/value pairs are separated by commas.

Option B is not a valid JSON script because it uses single quotes instead of double quotes for the field names and string values. JSON requires double quotes for strings<sup>12</sup>.

Option C is not a valid JSON script because it does not use commas to separate the name/value pairs. JSON requires commas to separate the data elements within an object or an array<sup>12</sup>.

Option D is not a valid JSON script because it uses a semicolon instead of a colon to separate the field name and the value. JSON requires a colon to separate the name and the value in a name/value pair<sup>12</sup>. References: 1: JSON Introduction, 2: JSON Syntax

**NEW QUESTION 415**

- (Topic 4)

A company recently rearranged some users' workspaces and moved several users to different desks. The network administrator receives a report that all of the users who were moved are having connectivity issues. Which of the following is the most likely reason?

- A. Ports are error disabled.
- B. Ports are administratively down.
- C. Ports are having an MDIX issue.
- D. Ports are trunk ports.

**Answer:** A

**Explanation:**

This is because ports can become error disabled when they detect certain errors or violations on the network, such as a loop, a security breach, or a duplex mismatch. When a port is error disabled, it shuts down and stops forwarding traffic until it is manually re-enabled by the administrator. The users who were moved to different desks may have plugged their devices into ports that were configured with different settings or security policies than their original ports, and this may have triggered the error disable state. The source of this answer is the Cisco ENCOR v1.1 course, module 3, lesson 3.3: Implementing EtherChannel.

**NEW QUESTION 418**

- (Topic 4)

In which two ways does the routing protocol OSPF differ from EIGRP? (Choose two.)

- A. OSPF supports an unlimited number of hop
- B. EIGRP supports a maximum of 255 hops.
- C. OSPF provides shorter convergence time than EIGRP.
- D. OSPF is distance vector protocol
- E. EIGRP is a link-state protocol.
- F. OSPF supports only equal-cost load balancing
- G. EIGRP supports unequal-cost load balancing.
- H. OSPF supports unequal-cost load balancing
- I. EIGRP supports only equal-cost load balancing.

**Answer:** AD

**NEW QUESTION 422**

- (Topic 4)

A customer has a wireless network deployed within a multi-tenant building. The network provides client access, location-based services, and is monitored using Cisco DNA Center. The security department wants to locate and track malicious devices based on threat signatures. Which feature is required for this solution?

- A. Cisco aWIPS policies on the WLC
- B. Cisco aWIPS policies on Cisco DNA Center

- C. malicious rogue rules on the WLC
- D. malicious rogue rules on Cisco DNA Center

Answer: B

**NEW QUESTION 425**

- (Topic 4)

Refer to the exhibit.

```
R2(config)#event manager applet script_1
R2(config-applet)#action 1 cli command "enable"
R2(config-applet)#action 2 cli command "config t"
R2(config-applet)#action 3 cli command "interface ge0/0"
R2(config-applet)#action 4 cli command "ip add 172.16.1.1 255.255.255.0"
R2(config-applet)#action 5 cli command "no sh"
R2(config-applet)#action 6 cli command "end"
R2(config-applet)#exit
```

An engineer must create a manually triggered EEM applet to enable the R2 router interface and assign an IP address to it. What is required to complete this configuration?

- A. R2(config-applet)# event oir
- B. R2(config-applet)#action 4 cli command "ip add 172.16.1.1 0.0.0.255"
- C. R2(config)# event manager session cli username
- D. R2(config-applet)# event none sync yes

Answer: D

**NEW QUESTION 430**

- (Topic 4)

Which element is unique to a Type 2 hypervisor?

- A. memory
- B. VM OS
- C. host OS
- D. host hardware

Answer: C

**NEW QUESTION 434**

- (Topic 4)

A firewall address of 192.166.1.101 can be pinged from a router but, when running a traceroute to it, this output is received

```
1 * * *
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
```

What is the cause of this issue?

- A. The firewall blocks ICMP traceroute traffic.
- B. The firewall rule that allows ICMP traffic does not function correctly
- C. The firewall blocks ICMP traffic.
- D. The firewall blocks UDP traffic

Answer: D

#### NEW QUESTION 438

- (Topic 4)

By default, which virtual MAC address does HSRP group 22 use?

- A. c0:42:01:67:05:16
- B. c0:07:0c:ac:00:22
- C. 00:00:0c:07:ac:16
- D. 00:00:0c:07:ac:22

Answer: D

#### NEW QUESTION 440

- (Topic 4)

An engineer must configure Interface and sensor monitoring on a router. The NMS server is located in a trusted zone with IP address 10.15.2.19. Communication between the router and the NMS server must be encrypted and password-protected using the most secure algorithms. Access must be allowed only for the NMS server and with the minimum permission levels needed. Which configuration must the engineer apply?

A)

```
ip access-list standard nms
 permit 10.15.2.19 255.255.255.255

snmp-server view ro cisco included

snmp-server view ro ifEntry included

snmp-server group nms v3 priv read ro access nms
snmp-server user user1 nms v3 auth 3des Password1 pri aes 192 Password123
```

B)

```
ip access-list standard nms
 permit 10.15.2.19 0.0.0.0

snmp-server view rw iso included

snmp-server view rw ifEntry included

snmp-server group nms v3 auth write rw access nms
snmp-server user user1 nms v3 auth des Password1 pri des Password123
```

C)

```
ip access-list extended nms
 permit 1 host 10.15.2.19 any

snmp-server view ro internet included

snmp-server view ro ifEntry included

snmp-server group nms v3 priv notify ro access nms
snmp-server user user1 nms v3 encrypted auth md5 Password1 pri 3des Password123
```

D)

```
ip access-list standard nms
 permit 10.15.2.19 0.0.0.0

snmp-server view ro iso included
```

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

Answer: A

#### Explanation:

Option A is the correct configuration to apply interface and sensor monitoring on a router with the given requirements. This option uses SNMPv3, which is the most secure version of SNMP that supports encryption and authentication. The configuration steps are as follows:

? Create an access list named nms that permits only the NMS server with IP address 10.15.2.19 to access the router: ip access-list standard nms and permit 10.15.2.19 0.0.0.0.

? Create a view named rw that includes all the SNMP objects: snmp-server view rw included.

? Create a group named nms that uses SNMPv3 with privacy (encryption) and authentication, and assigns the view rw and the access list nms to the group: snmp-

server group nms v3 priv read rw access nms.

? Create a user named nms that belongs to the group nms and uses DES for authentication and AES for encryption, with the passwords despass and aespass respectively: snmp-server user nms nms v3 auth des despass priv aes 192 aespass.

Option B is incorrect because it does not use encryption for SNMP communication, which is required by the question. The noauth keyword in the snmp-server group command means that no authentication or encryption is used, which makes the SNMP packets vulnerable to eavesdropping and tampering1.

Option C is incorrect because it does not use the most secure algorithms for SNMP communication, which is required by the question. The md5 and des keywords in the snmp-server user command mean that MD5 and DES are used for authentication and encryption respectively, which are considered weak and outdated algorithms. AES and SHA are recommended instead1.

Option D is incorrect because it does not restrict the access to the NMS server only, which is required by the question. The snmp-server community command creates a community string that acts as a password for SNMP access, but it does not specify an access list to limit the source IP addresses that can use the community string. Therefore, any device that knows the community string can access the router via SNMP1. References: 1: Configuring SNMPv3, 2: SNMP Configuration Guide, Cisco IOS XE Gibraltar 16.12.x

**NEW QUESTION 441**

- (Topic 4)

```
>traceroute www.crmABC.com
Tracing route to www.crmABC.com [192.168.100.1]
 0 0ms 0ms 0ms 10.10.10.1
 1 3ms 5ms 3ms 10.10.10.1
 2 4ms 6ms 4ms 10.100.100.1
 3 4ms 6ms 4ms 10.100.200.1
 4 4ms 6ms 4ms 10.100.100.1
 5 4ms 6ms 4ms 10.100.200.1
 6 4ms 6ms 4ms 10.100.100.1
 7 4ms 6ms 4ms 10.100.200.1
<output truncated>
```

Refer to the exhibit Users cannot reach the web server at 192.168 100 1. What is the root cause for the failure?

- A. The server is attempting to load balance between links 10.100 100.1 and 10 100.200.1.
- B. The server is out of service.
- C. There is a loop in the path to the server.
- D. The gateway cannot translate the server domain name.

**Answer: C**

**NEW QUESTION 445**

- (Topic 4)

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

Refer to the exhibit. An engineer must update the existing configuration to achieve these results:

- Only administrators from the 192.168 1.0.'24 subnet can access the vty lines.
- \* Access to the vty lines using clear-text protocols is prohibited. Which command set should be applied?

A)

```
access-list 1 permit 192.168.1.0 255.255.255.0
line vty 0 15
access-class 1 in
transport input telnet rlogin
```

B)

```
access-list 1 permit 192.168.1.0 0.0.0.255
line vty 0 15
access-class 1 in
line vty 0 15
access-class 1 in
transport input none
```

C)

```
access-list 1 permit 192.168.1.0 0.0.0.255
line vty 0 15
access-class 1 in
transport input ssh
```

D)

```
access-list 1 permit 192.168.1.0 0.0.0.255
line vty 0 15
access-class 1 in
```

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

**Answer: B****Explanation:**

Option B is the correct command set to update the existing configuration to achieve the desired results. The configuration steps are as follows<sup>12</sup>:

? Define a standard access list that permits only the administrators from the 192.168.1.0/24 subnet to access the vty lines. In this case, the access list is named ADMIN and it allows any host with an IP address in the range of 192.168.1.1 to 192.168.1.254 to access the vty lines: ip access-list standard ADMIN and permit 192.168.1.0 0.0.0.255.

? Apply the access list to the vty lines using the access-class command. This command restricts incoming and outgoing connections between a particular vty and the addresses in the access list. In this case, the access list ADMIN is applied to the vty lines 0 to 15 in the inbound direction, which means that only the hosts that match the access list can initiate a connection to the vty lines: line vty 0 15 and access-class ADMIN in.

? Disable the clear-text protocols such as Telnet for the vty lines using the transport input command. This command specifies which protocols are allowed for incoming connections. In this case, only SSH is allowed for the vty lines, which is a secure protocol that encrypts the data between the client and the server: transport input ssh.

Option A is incorrect because it does not apply the access list to the vty lines, which is required to restrict the access to the administrators from the 192.168.1.0/24 subnet. Without the access-class command, any host can attempt to connect to the vty lines<sup>12</sup>.

Option C is incorrect because it does not disable the clear-text protocols for the vty lines, which is required to prohibit the access to the vty lines using unsecure protocols. Without the transport input ssh command, both Telnet and SSH are allowed for the vty lines by default<sup>12</sup>.

Option D is incorrect because it uses an extended access list instead of a standard access list, which is not recommended for controlling access to the vty lines. An extended access list requires more configuration and processing than a standard access list, and it cannot be applied directly to the vty lines. It has to be applied to each interface that can be used to access the vty lines, which increases the complexity and the possibility of errors<sup>12</sup>. References: 1: Controlling Access to a Virtual Terminal Line, 2: Configuring Secure Shell

**NEW QUESTION 450**

- (Topic 4)

Which router is elected the IGMP Querier when more than one router is in the same LAN segment?

- A. The router with the shortest uptime
- B. The router with the lowest IP address
- C. The router with the highest IP address
- D. The router with the longest uptime

**Answer: B****NEW QUESTION 452**

- (Topic 4)

Refer to the exhibit.

```
R2#
*May 27 15:33:59.642: OSPF-1 ADJ Gi1: Send DBD to 192.168.201.137 seq 0xDE7 opt 0x52 flag 0x7 len 32
*May 27 15:33:59.642: OSPF-1 ADJ Gi1: Retransmitting DBD to 192.168.201.137 [15]
*May 27 15:33:59.645: OSPF-1 ADJ Gi1: Rcv DBD from 192.168.201.137 seq 0xDE7 opt 0x52 flag 0x2 len 112 mtu 9100 state EXSTART
```



D. Option D

Answer: C

#### NEW QUESTION 460

- (Topic 4)

Which JSON script is properly formatted?

A)

```
[ "Lodging":  
  {  
    "type":B&B,  
    "location":Oceanfront,  
    "contact":946-230-7462  
  }  
]
```

B)

```
{  
  "frames": [  
    {  
      "type":"premium",  
      "material":"wood",  
      "shape":"square"  
    }  
  ]  
}
```

C)

```
[  
  {  
    "subject": {  
      [  
        "title":"Sewing"  
        "listing":"elective"  
        "session":"Summer"  
      ]  
    }  
  ]  
]
```

D)

```
[ "class": {  
  "title": "Science"  
  "Grade": "11",  
  "location": "Room C",  
  }  
]
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

#### Explanation:

Option A is the properly formatted JSON script. JSON (JavaScript Object Notation) is a standard text-based format for representing structured data based on JavaScript object syntax. It is commonly used for transmitting data in web applications (e.g., sending some data from the server to the client, so it can be displayed on a web page, or vice versa). The JSON syntax rules are as follows:

? Data is in name/value pairs, separated by commas. A name/value pair consists of a field name (in double quotes), followed by a colon, followed by a value: "name": "value".

? Curly braces hold objects. An object can contain multiple name/value pairs: {"name": "value", "name": "value", ...}.

? Square brackets hold arrays. An array can contain multiple values, separated by commas: ["value", "value", ...].

? Values can be strings (in double quotes), numbers, booleans (true or false), null, objects, or arrays.

Option A follows these rules and is a valid JSON script. It defines an object with four name/value pairs: "name", "age", "hobbies", and "address". The value of "name" is a string, the value of "age" is a number, the value of "hobbies" is an array of strings, and the value of "address" is another object with two name/value pairs: "city" and "country". The object is enclosed in curly braces and the name/value pairs are separated by commas.

Option B is not a valid JSON script because it uses single quotes instead of double quotes for the field names and string values. JSON requires double quotes for strings.

Option C is not a valid JSON script because it does not use commas to separate the name/value pairs. JSON requires commas to separate the data elements

within an object or an array<sup>12</sup>.

Option D is not a valid JSON script because it uses a semicolon instead of a colon to separate the field name and the value. JSON requires a colon to separate the name and the value in a name/value pair<sup>12</sup>. References: 1: JSON Introduction, 2: JSON Syntax

#### NEW QUESTION 463

- (Topic 4)

What is a characteristic of the Cisco DNA Center Template Editor feature?

- A. It facilitates software upgrades to network devices from a central point.
- B. It facilitates a vulnerability assessment of the network devices.
- C. It provides a high-level overview of the health of every network device.
- D. It uses a predefined configuration through parameterized elements or variables.

**Answer:** D

#### Explanation:

This is because the Cisco DNA Center Template Editor feature is a tool that allows the network administrator to create and deploy configuration templates to multiple network devices. The configuration templates use parameterized elements or variables, which are placeholders for values that can be customized for each device. For example, a variable can represent the hostname, IP address, or interface number of a device. The parameterized elements or variables can be defined manually or automatically using the Cisco DNA Center inventory. The source of this answer is the Cisco ENCOR v1.1 course, module 8, lesson 8.5: Implementing Network Configuration Management.

#### NEW QUESTION 465

DRAG DROP - (Topic 4)

Drag and drop the code snippets from the bottom onto the blanks in the Python script to convert a Python object into a JSON string. Not all options are used.

```
import   
  
data = {  
    "measurement": "freeMemory",  
    "maxDataPoints": 30,  
    "alert": True,  
    "policy": "1.2.1",  
    "devices": [{"model": "Cisco 2921 ISR", "ipv4": '10.10.10.1'}]  
}  
model = data["devices"][0]["model"]  
  
json_string =  (data)  
  
print(  )
```

model

json.loads

json

json\_string

json.dumps

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

<https://stackoverflow.com/questions/45834577/turn-python-object-into-json-output>

#### NEW QUESTION 469

- (Topic 4)

Which technology reduces the implementation of STP and leverages both unicast and multicast?

- A. VSS
- B. VXLAN
- C. VPC
- D. VLAN

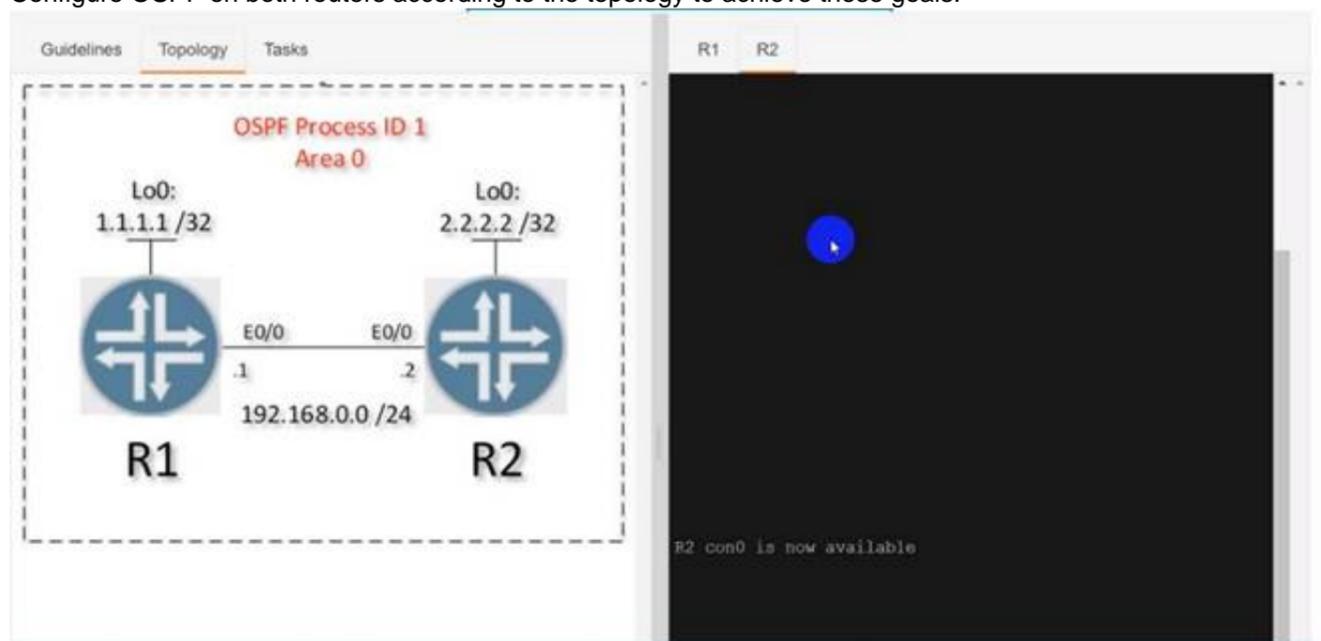
**Answer:** B

#### NEW QUESTION 470

SIMULATION - (Topic 4)

Simulation 04

Configure OSPF on both routers according to the topology to achieve these goals:



Guidelines Topology Tasks

Configure OSPF on both routers according to the topology to achieve these goals:

1. Ensure that all networks are advertised between the routers without using the "network" statement under the "router ospf" configuration section.
2. Configure a single command on both routers to ensure:
  - The DR/BDR election does not occur on the link between the OSPF neighbors.
  - No extra OSPF host routes are generated.

Submit feedback about this item.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Solution:

```
R1
Router ospf 1 Int loop0
Ip ospf 1 area 0 Int et0/0
Ip ospf 1 area 0
Ip ospf network point-to-point Copy run start
```

```
R2
Router ospf 1 Int loop0
Ip ospf 1 area 0 Int et0/0
Ip ospf 1 area 0
Ip ospf network point-to-point Copy run start
```

Verification:-

```
R2#sh ip os
R2#sh ip ospf nei
R2#sh ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address
  Interface
1.1.1.1          0    FULL/ -         00:00:34   192.168.0
.1      Ethernet0/0
R2#
```

```
R1#sh ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address
  Interface
2.2.2.2          0    FULL/ -         00:00:32   192.168
.2      Ethernet0/0
R1#sh ip ospf route

      OSPF Router with ID (1.1.1.1) (Process ID 1)

      Base Topology (MTID 0)

      Area BACKBONE (0)

      Intra-area Route List

* 192.168.0.0/24, Intra, cost 10, area 0, Connected
  via 192.168.0.1, Ethernet0/0
* 1.1.1.1/32, Intra, cost 1, area 0, Connected
  via 1.1.1.1, Loopback0
*> 2.2.2.2/32, Intra, cost 11, area 0
  via 192.168.0.2, Ethernet0/0

      First Hop Forwarding Gateway Tree

192.168.0.1 on Ethernet0/0, count 1
192.168.0.2 on Ethernet0/0, count 1
1.1.1.1 on Loopback0, count 1
R1#
```

**NEW QUESTION 472**

- (Topic 4)

Refer to the exhibit.

```

R1#traceroute
Protocol [ip]:
Target IP address: 3.3.3.3
Source address: 1.1.1.1
Numeric display [n]:
Timeout in seconds: [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]: Record
Number of hops [9]:
Loose, Strict, Record, Timestamp, Verbose [RV]:
Type escape sequence to abort.

Continued --->

Tracing the route to 3.3.3.3

 1 10.99.69.2  36 msec
Received packet has options
Total option bytes = 40, padded length=40
Record route:
(10.99.69.1) <*>
(0.0.0.0)
(0.0.0.0)
End of list
----output omitted----

 2 10.99.69.6  !A
Received packet has options
Total option bytes = 40, padded length=40
Record route:
(10.99.69.1)
(10.99.69.5) <*>
(0.0.0.0)
(0.0.0.0)
End of list
!A
----output omitted----
    
```

The traceroute fails from R1 to R3. What is the cause of the failure?

- A. The loopback on R3 is in a shutdown state.
- B. An ACL applied Inbound on loopback0 of R2 is dropping the traffic.
- C. An ACL applied Inbound on fa0/1 of R3 is dropping the traffic.
- D. Redistribution of connected routes into OSPF is not configured.

Answer: C

**NEW QUESTION 477**

- (Topic 4)

Which of the following attacks becomes more effective because of global leakages of users' passwords?

- A. Dictionary
- B. Brute-force
- C. Phishing
- D. Deauthentication

Answer: A

**Explanation:**

This is because a dictionary attack is a type of password cracking attack that uses a list of common or previously leaked passwords to guess the credentials of a user. A dictionary attack becomes more effective because of global leakages of users' passwords, as the attacker can use the leaked passwords as a source for the dictionary. The source of this answer is the Cisco ENCOR v1.1 course, module 2, lesson 2.3: Implementing Wireless Security.

**NEW QUESTION 479**

DRAG DROP - (Topic 4)

Drag and drop the tools from the left onto the agent types on the right.

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

**NEW QUESTION 481**

- (Topic 4)

An engineer must configure a multicast UDP jitter operation. Which configuration should be applied?

- A)  
 Router(config)#ip sla 1  
 Router(config)#udp-jitter 192.0.2.115 65051 num-packets 20
- B)  
 Router(config)#ip sla 1  
 Router(config)#udp jitter 10.0.0.1 source-ip 192.168.1.1
- C)  
 Router(config)#ip sla 1  
 Router(config)#udp-jitter 192.0.2.115 65051
- D)  
 Router(config)#ip sla 1  
 Router(config)#udp jitter 239.1.1.1 65051 end-point list List source-ip 192.168.1.1

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

**Answer: D**

**NEW QUESTION 484**

- (Topic 4)

How does Cisco Express Forwarding switching differ from process switching on Cisco devices?

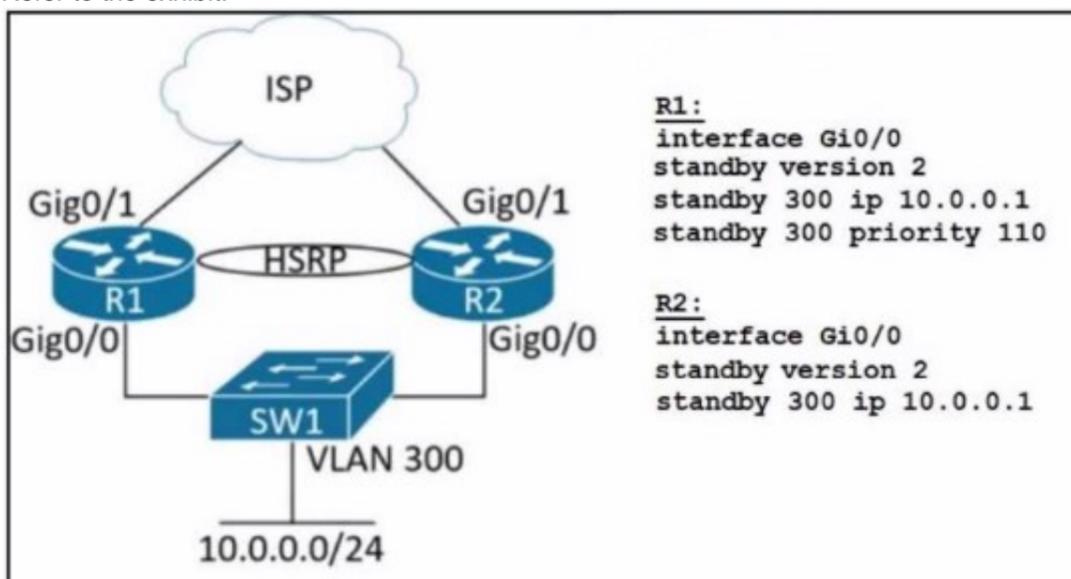
- A. Cisco Express Forwarding switching uses adjacency tables built by the CDP protocol, and process switching uses the routing table.
- B. Cisco Express Forwarding switching uses dedicated hardware processors, and process switching uses the main processor.
- C. Cisco Express Forwarding switching saves memory by storing adjacency tables in dedicated memory on the line cards, and process switching stores all tables in the main memory.
- D. Cisco Express Forwarding switching uses a proprietary protocol based on IS-IS for MAC address lookup, and process switching uses the MAC address table.

**Answer: C**

**NEW QUESTION 485**

- (Topic 4)

Refer to the exhibit.



Refer to the exhibit. An engineer must implement HSRP between two WAN routers. In the event R1 fails and then regains operational status, it must allow 100 seconds for the routing protocol to converge before preemption takes effect. Which configuration is required?

A)

```
R1:
interface Gi0/0
standby 300 preempt
```

```
R2:
interface Gi0/0
standby 300 delay sync 100
```

B)

```
R1:
interface Gi0/0
standby 300 preempt
```

```
R2:
interface Gi0/0
standby 300 delay minimum 100
```

C)

```
R1:
interface Gi0/0
standby 300 preempt
standby 300 delay minimum 100
```

D)

```
R2:
interface Gi0/0
standby 300 preempt
standby 300 delay sync 100
```

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

**Answer:** B**Explanation:**

Option B is the correct configuration to implement HSRP between two WAN routers with the given requirement. The configuration steps are as follows:

- ? Define the HSRP group number and the virtual IP address for the group using the `standby <group> ip <address>` command. In this case, the group number is 300 and the virtual IP address is 10.10.10.1: `standby 300 ip 10.10.10.1`.
- ? Configure HSRP preemption and preemption delay using the `standby <group> preempt [delay [minimum] <seconds>]` command. Preemption allows a router with higher priority to take over the active role from a router with lower priority. Preemption delay is the time that a router waits before taking over the active role in the HSRP group. In this case, the preemption delay is 100 seconds, which means that R1 will wait for 100 seconds before preempting R2 after R1 regains operational status: `standby 300 preempt delay minimum 100`.
- ? Configure the HSRP priority for the router using the `standby <group> priority <value>` command. The priority determines which router is the active router and which router is the standby router. The higher the priority, the more likely the router is to become the active router. In this case, R1 has a priority of 200 and R2 has a priority of 100, which means that R1 is the preferred active router and R2 is the standby router: `standby 300 priority 200` on R1 and `standby 300 priority 100` on R2.

Option A is incorrect because it does not configure HSRP preemption and preemption delay, which are required by the question. Without preemption, R2 will remain the active router even if R1 has a higher priority and regains operational status. Without preemption delay, R1 will attempt to preempt R2 immediately, which may cause routing instability.

Option C is incorrect because it configures HSRP preemption delay with the `reload` keyword, which means that the delay period applies only to the first interface-up event after the router has reloaded. This does not meet the requirement of the question, which states that the delay period should apply to any interface-up event after R1 fails and then regains operational status.

Option D is incorrect because it configures HSRP preemption delay with the `sync` keyword, which means that the delay period applies only to the first interface-up event after the router has reloaded, and only if such an event occurs within 360 seconds from reload. This does not meet the requirement of the question, which states that the delay period should apply to any interface-up event after R1 fails and then regains operational status, and without any time limit. References: 1: Configuring HSRP, 2: HSRP Configuration Guide

**NEW QUESTION 486**

- (Topic 4)

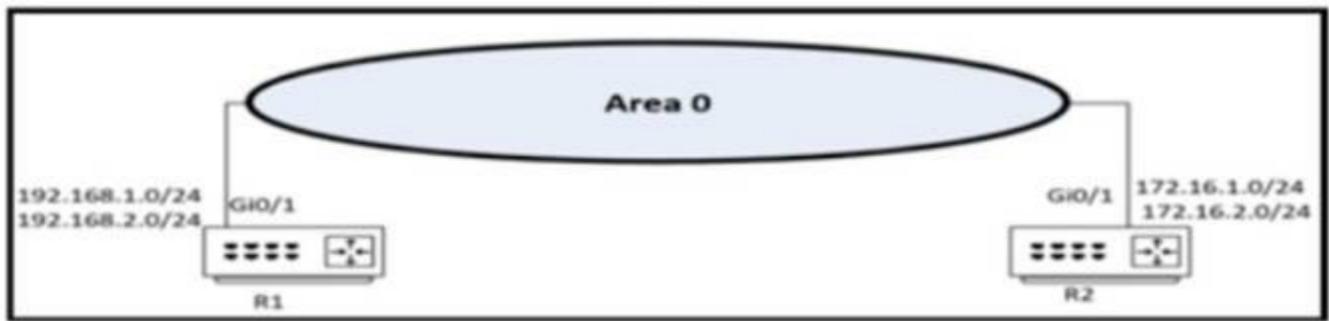
Which NTP mode must be activated when using a Cisco router as an NTP authoritative server?

- A. primary
- B. server
- C. broadcast client
- D. peer

Answer: D

**NEW QUESTION 490**

- (Topic 4)



Refer to the exhibit. Which two configurations enable R1 and R2 to advertise routes into OSPF? (Choose two)

A)

```
R2
router ospf 0
network 172.16.1.0 255.255.255.0 area 0
network 172.16.2.0 255.255.255.0 area 0
```

B)

```
R2
router ospf 0
network 172.16.1.0 0.0.0.255 area 0
network 172.16.2.0 255.255.255.0 area 0
```

C)

```
R1
router ospf 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
```

D)

```
R2
router ospf 0
network 172.16.1.0 0.0.0.255 area 0
network 172.16.2.0 0.0.0.255 area 0
```

E)

```
R1
router ospf 0
network 192.168.1.0 255.255.255.0 area 0
network 192.168.2.0 255.255.255.0 area 0
```

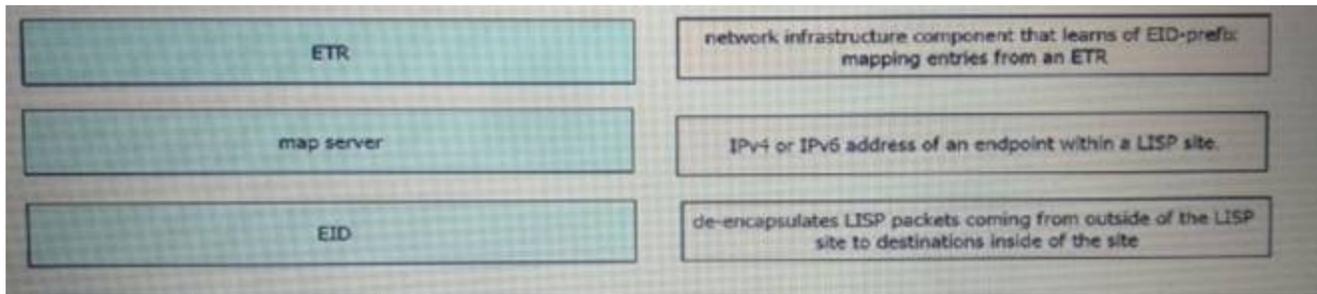
- A. Option A
- B. Option B
- C. Option C
- D. Option DE) Option E

Answer: CD

**NEW QUESTION 492**

DRAG DROP - (Topic 4)

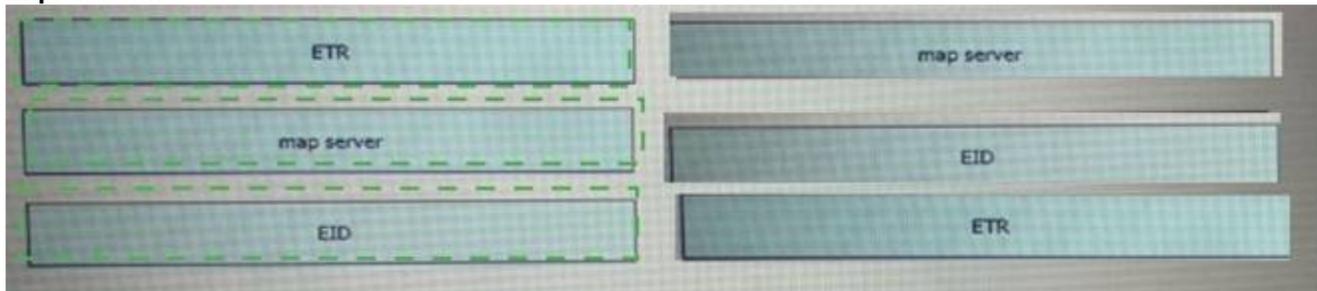
Drag and drop the LISP components on the left to the correct description on the right.



- A. Mastered
- B. Not Mastered

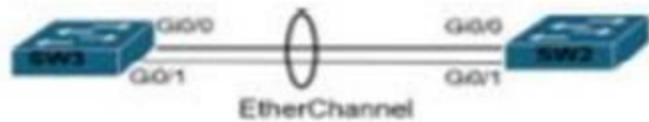
Answer: A

Explanation:



**NEW QUESTION 495**

- (Topic 4)  
Refer to the exhibit.



```
SW2# show ip interface brief | include Port
Port-channell unassigned YES unset down down
SW2# show etherchannel summary
Flags: D - down P - bundled 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
M - not in use, minimum links not met
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(S D ) PAgP Gi0/0(I) Gi0/1(I)

SW3# show etherchannel summary
Flags: D - down P - bundled 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
M - not in use, minimum links not met
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(S D ) LACP Gi0/0(I) Gi0/1(I)
```

```
Current configuration : 142 bytes
vrf definition STAFF
!
!
interface GigabitEthernet1
 vrf forwarding STAFF
 no ip address
 negotiation auto
 no mop enabled
 no mop sysid
end
```

An engineer must assign an IP address of 192.168.1.1/24 to the GigabitEthernet1 interface. Which two commands must be added to the existing configuration to accomplish this task? (Choose two.)

- A. Router(config-vrf)#ip address 192.168.1.1 255.255.255.0
- B. Router(config-vrf)#address-family ipv4
- C. Router(config-if)#address-family ipv4
- D. Router(config-vrf)#address-family ipv6
- E. Router(config-if)#ip address 192.168.1.1 255.255.255.0

Answer: BE

**NEW QUESTION 496**

- (Topic 4)

```

1 def main():
2     vlans = {'vlan10':'192.168.1.0',
3             'vlan20':'192.168.2.0',
4             'vlan30':'192.168.3.0' }
5     vlans_key(vlans)
6
7 def vlans_key(vlans):
8     for key in vlans.keys():
9         print(str(key) + ' ' + str(vlans[key]))
10
11 if __name__ == '__main__':
12     main()

```

Refer to the exhibit. What is printed to the console when this script is run?

- A. a key-value pair in tuple type
- B. a key-value pair in list type
- C. a key-value pair in string type
- D. an error

Answer: C

**NEW QUESTION 499**

- (Topic 4)

<pre> R2#show ip ospf neighbor R2#show ip ospf interface fastEthernet 1/1 FastEthernet1/1 is up, line protocol is up Internet Address 192.168.0.5/30, Area 0 Process ID 1, Router ID 10.0.0.5, Network Type BROADCAST, Cost: 1 Transmit Delay is 1 sec, State DR, Priority 1 Designated Router (ID) 10.0.0.5, Interface address 192.168.0.5 No backup designated router on this network Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40 Hello due in 00:00:00 Supports Link-local Signaling (LLS) Cisco NSF helper support enabled IETF NSF helper support enabled Index 2/2, flood queue length 0 Next 0x0(0)/0x0(0) Last flood scan length is 0, maximum is 0 Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 0, Adjacent neighbor count is 0 Suppress hello for 0 neighbor(s) R2#ping 192.168.0.6 df-bit size 1500  Type escape sequence to abort. Sending 5, 1500-byte ICMP Echos to 192.168.0.6, timeout is 2 seconds: Packet sent with the DF bit set !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/16 ms </pre>	<pre> R3#show ip ospf neighbor R3#show ip ospf interface fastEthernet 1/1 FastEthernet1/1 is up, line protocol is up Internet Address 192.168.0.6/29, Area 0 Process ID 1, Router ID 10.0.0.3, Network Type BROADCAST, Cost: 1 Transmit Delay is 1 sec, State DR, Priority 1 Designated Router (ID) 10.0.0.3, Interface address 192.168.0.6 No backup designated router on this network Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40 Hello due in 00:00:06 Supports Link-local Signaling (LLS) Cisco NSF helper support enabled IETF NSF helper support enabled Index 2/2, flood queue length 0 Next 0x0(0)/0x0(0) Last flood scan length is 0, maximum is 0 Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 0, Adjacent neighbor count is 0 Suppress hello for 0 neighbor(s) R3#ping 192.168.0.5 df-bit size 1500  Type escape sequence to abort. Sending 5, 1500-byte ICMP Echos to 192.168.0.5, timeout is 2 seconds: Packet sent with the DF bit set !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/20 ms </pre>
---	---

Refer to the exhibit. Why does the OSPF neighborhood fail between the two interfaces?

- A. The IP subnet mask is not the same.
- B. There is a mismatch in the OSPF interface network type.
- C. The OSPF timers are different.
- D. The MTU is not the same.

Answer: A

**NEW QUESTION 503**

- (Topic 4)

How does a Type 1 hypervisor function?

- A. It runs directly on a physical server and depends on a previously installed operating system.
- B. It runs directly on a physical server and includes its own operating system.
- C. It runs on a virtual server and depends on a previously installed operating systems
- D. It runs on a virtual server and includes its own operating system.

Answer: B

**Explanation:**

A type 1 hypervisor, also known as a bare-metal or native hypervisor, runs directly on the physical server and its underlying hardware. It does not depend on a previously installed operating system, but rather includes its own operating system that is designed to run virtual machines. A type 1 hypervisor provides excellent performance and stability, as it has direct access to the hardware resources and can allocate them to the virtual machines. A type 1 hypervisor is typically used in enterprise environments, where multiple virtual machines run on a single server.

Reference: What is a Hypervisor? Types of Hypervisors 1 & 2 - phoenixNAP

**NEW QUESTION 505**

- (Topic 2)

What occurs when a high bandwidth multicast stream is sent over an MVPN using Cisco hardware?

- A. The traffic uses the default MDT to transmit the data only if it is a (S,G) multicast route entry
- B. A data MDT is created to if it is a (\*, G) multicast route entries
- C. A data and default MDT are created to flood the multicast stream out of all PIM-SM neighbors.
- D. A data MDT is created to allow for the best transmission through the core for (S, G) multicast route entries.

Answer: D

#### NEW QUESTION 509

- (Topic 2)

```
RP/0/0/CPU0:BRDR-1#show route ipv4 0.0.0.0
Routing entry for 0.0.0.0/0
  Known via "bgp 65001", distance 20, metric 0, candidate default path
  Tag 65002, type external
  Installed Jan  2 08:40:59.889 for 00:01:18
  Routing Descriptor Blocks
    100.65.19.1, from 100.65.19.1, BGP external
    Route metric is 0
  No advertising protos.

RP/0/0/CPU0:BRDR-1#show run router ospf
router ospf 1
 redistribute bgp 65001 route-policy BGP-TO-OSPF
 area 0
  mpls traffic-eng
  interface Loopback0
  interface GigabitEthernet0/0/0/0.92
  interface GigabitEthernet0/0/0/0.3132
  mpls traffic-eng router-id Loopback0

RP/0/0/CPU0:BRDR-1#show rpl route-policy BGP-TO-OSPF
route-policy BGP-TO-OSPF
  if destination in (0.0.0.0/0) then
    set metric-type type-1
  endif
  set metric-type type-2
  set ospf-metric 100
end-policy
```

Refer to the exhibit. Router BRDR-1 is configured to receive the 0.0.0.0/0 and 172.17.1.0/24 network via BGP and advertise them into OSPF area 0. An engineer has noticed that the OSPF domain is receiving only the 172.17.1.0/24 route and default route 0.0.0.0/0 is still missing. Which configuration must engineer apply to resolve the problem?

- router ospf 1  
default-information originate always  
end
- router ospf 1  
redistribute bgp 65001 metric 100 route-policy BGP-TO-OSPF  
end
- router ospf 1  
default-metric 100  
end
- router ospf 1  
default-information originate  
end

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

Answer: D

#### NEW QUESTION 514

- (Topic 2)

What is the function of cisco DNA center in a cisco SD-access deployment?

- A. It is responsible for routing decisions inside the fabric
- B. It is responsible for the design, management, deployment, provisioning and assurance of the fabric network devices.
- C. It possesses information about all endpoints, nodes and external networks related to the fabric
- D. It provides integration and automation for all nonfabric nodes and their fabric counterparts.

**Answer: B**

#### NEW QUESTION 517

- (Topic 2)

Refer to the exhibit.

```
monitor session 1 source vlan 10 - 12 rx
monitor session 1 destination interface gigabitethernet0/1
```

An engineer must configure a SPAN session. What is the effect of the configuration?

- A. Traffic sent on VLANs 10, 11, and 12 is copied and sent to interface g0/1.
- B. Traffic sent on VLANs 10 and 12 only is copied and sent to interface g0/1.
- C. Traffic received on VLANs 10, 11, and 12 is copied and sent to Interface g0/1.
- D. Traffic received on VLANs 10 and 12 only is copied and sent to interface g0/1.

**Answer: C**

#### NEW QUESTION 520

- (Topic 2)

Which new enhancement was implemented in Wi-Fi 6?

- A. Wi-Fi Protected Access 3
- B. 4096 Quadrature Amplitude Modulation Mode
- C. Channel bonding
- D. Uplink and Downlink Orthogonal Frequency Division Multiple Access

**Answer: D**

#### NEW QUESTION 522

- (Topic 2)

Which OSPF networks types are compatible and allow communication through the two peering devices?

- A. broadcast to nonbroadcast
- B. point-to-multipoint to nonbroadcast
- C. broadcast to point-to-point
- D. point-to-multipoint to broadcast

**Answer: A**

#### Explanation:

The following different OSPF types are compatible with each other:

+ Broadcast and Non-Broadcast (adjust hello/dead timers)

+ Point-to-Point and Point-to-Multipoint (adjust hello/dead timers)

Broadcast and Non-Broadcast networks elect DR/BDR so they are compatible. Point- topoint/multipoint do not elect DR/BDR so they are compatible.

#### NEW QUESTION 525

- (Topic 2)

An engineer is configuring local web authentication on a WLAN. The engineer chooses the Authentication radio button under the Layer 3 Security options for Web Policy. Which device presents the web authentication for the WLAN?

- A. ISE server
- B. local WLC
- C. RADIUS server
- D. anchor WLC

**Answer: B**

#### Explanation:

"The next step is to configure the WLC for the Internal web authentication. Internal web authentication is the default web authentication type on WLCs."

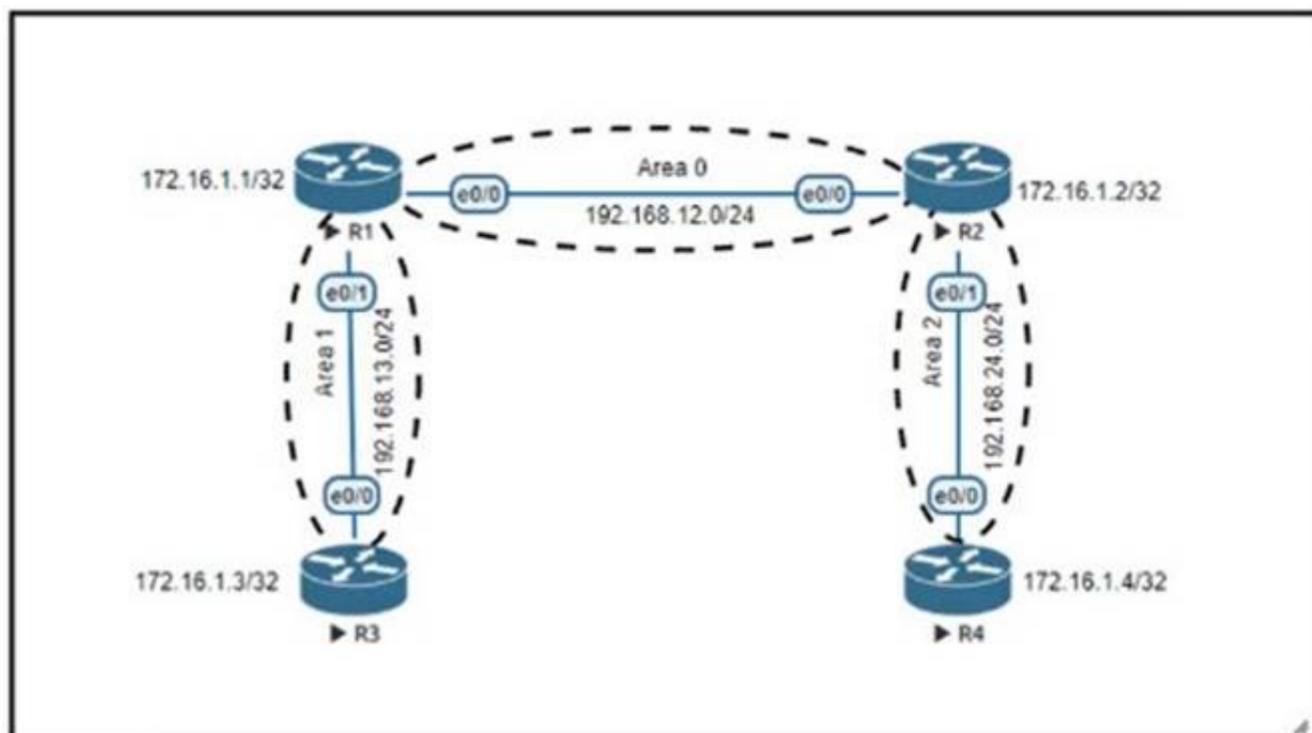
In step 4 of the link above, we will configure Security as described in this question. Therefore we can deduce this configuration is for Internal web authentication.

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

#### NEW QUESTION 530

- (Topic 2)

Refer to the exhibit.



An engineer must create a configuration that prevents R3 from receiving the LSA about 172.16.1.4/32. Which configuration set achieves this goal?

- On R1  
**ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32**  
**ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32**  
  
**router ospf 200**  
**area 1 filter-list prefix INTO-AREA1 out**
- On R3  
**ip access-list standard R4\_L0**  
**deny host 172.16.1.4**  
**permit any**  
  
**router ospf 200**  
**distribute-list R4\_L0 in**
- On R1  
**ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32**  
**ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32**  
  
**router ospf 200**  
**area 1 filter-list prefix INTO-AREA1 in**
- On R3  
**ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32**  
**ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32**  
  
**router ospf 200**  
**area 1 filter-list prefix INTO-AREA1 in**

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

Answer: B

**NEW QUESTION 532**

- (Topic 2)

```
RP/0/0/CPU0:R2#debug isis adjacencies
RP/0/0/CPU0:Apr 2 20:57:00.421 : isis[1010]: RECV P2P IIH (L2)
from GigabitEthernet0/0/0/0 SNPA fal6.3ebe.a7bc: System ID R2,
Holdtime 30, length 1429
RP/0/0/CPU0:Apr 2 20:57:01.761 : isis[1010]: SEND P2P IIH (L1)
on GigabitEthernet0/0/0/0: Holdtime 30s, Length 41
```

Refer to the exhibit. A network operator is attempting to configure an IS-IS adjacency between two routers, but the adjacency cannot be established. To troubleshoot the problem, the operator collects this debugging output. Which interfaces are misconfigured on these routers?

- A. The peer router interface is configured as Level 1 only, and the R2 interface is configured as Level 2 only
- B. The R2 interface is configured as Level 1 only, and the Peer router interface is configured as Level 2 only
- C. The R2 interface is configured as point-to-point, and the peer router interface is configured as multipoint.

D. The peer router interface is configured as point-as-point, and the R2 interface is configured as multipoint.

Answer: C

**NEW QUESTION 536**

- (Topic 2)

A network engineer configures a WLAN controller with increased security for web access. There is IP connectivity with the WLAN controller, but the engineer cannot start a management session from a web browser. Which action resolves the issued

- A. Disable JavaScript on the web browser
- B. Disable Adobe Flash Player
- C. Use a browser that supports 128-bit or larger ciphers.
- D. Use a private or incognito session.

Answer: C

**NEW QUESTION 540**

- (Topic 2)

A network administrator is implementing a routing configuration change and enables routing debugs to track routing behavior during the change. The logging output on the terminal is interrupting the command typing process. Which two actions can the network administrator take to minimize the possibility of typing commands incorrectly? (Choose two.)

- A. Configure the logging synchronous global configuration command
- B. Configure the logging delimiter feature
- C. Configure the logging synchronous command under the vty
- D. Press the TAB key to reprint the command in a new line
- E. increase the number of lines on the screen using the terminal length command

Answer: CD

**NEW QUESTION 544**

- (Topic 2)

Refer to the exhibit.

```
R1#show ip bgp
BGP table version is 32, local router ID is 192.168.101.5
Status codes: S suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
   Network        Next Hop         Metric  LocPrf  Weight  Path
*   192.168.102.0  192.168.101.18   80
*                   192.168.101.14   80      80
*                   192.168.101.10
*>                  192.168.101.2    32768
*                   192.168.101.6    80      80
```

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: A

**Explanation:**

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

Path Selection Attributes: Weight > Local Preference > Originate > AS Path > Origin > MED > External > IGP Cost > eBGP Peering > Router ID

BGP prefers the path with highest weight but the weights here are all 0 (which indicate all routes that are not originated by the local router) so we need to check the Local Preference.

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 547**

- (Topic 4)

Refer to the exhibit.



A client requests a new SSID that will use web-based authentication and external RADIUS servers. Which Layer 2 security mode must be selected?

- A. WPA + WPA2
- B. WPA2 + WPA3
- C. Static WEP
- D. None

**Answer:** A

**NEW QUESTION 549**

- (Topic 4)

A company recently decided to use RESTCONF instead of NETCONF and many of their NETCONF scripts contain the operation `<edit-config>(operation="create")`. Which RESTCONF operation must be used to replace these statements?

- A. POST
- B. GET
- C. PUT
- D. CREATE

**Answer:** A

**NEW QUESTION 552**

- (Topic 4)

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

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

**Answer:** AE

**NEW QUESTION 553**

- (Topic 4)

Refer to the exhibit.

```
DSW1#sh spanning-tree
MST1
Spanning tree enabled protocol mstp
Root ID    Priority    32769
Address    001b.7363.4300
Cost       2
Port       13 (FastEthernet1/0/11)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
Address    001b.0d8e.e080
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface      Role  Sts Cost      Prio.Nbr Type
-----
Fa1/0/7        Desg FWD 2         128.9   P2p Bound (PVST)
Fa1/0/10       Desg FWD 2         128.12  P2p Bound (PVST)
Fa1/0/11       Root FWD 2         128.13  P2p
Fa1/0/12       Altn BLK 2         128.14  P2p

DSW1#sh spanning-tree mst
##### MST1    vlans mapped: 10,20
Bridge        address 001b.0d8e.e080 priority 32769 (32768 sysid 1)
Root          address 001b.7363.4300 priority 32769 (32768 sysid 1)
              port   Fa1/0/11 cost 2 rem hops 19

... output omitted
```

Which two commands ensure that DSW1 becomes root bridge for VLAN 10 and 20?

- A. spanning-tree mst 1 priority 1
- B. spanning-tree mst 1 root primary
- C. spanning-tree mstp vlan 10,20 root primary
- D. spanning-tree mst vlan 10,20 priority root
- E. spanning-tree mst 1 priority 4096

Answer: BE

**NEW QUESTION 554**

- (Topic 4)

General	Security	QoS	Policy-Mapping	Advanced
Profile Name	<input type="text" value="Cisco"/>			
Type	WLAN			
SSID	<input type="text" value="Cisco"/>			
Status	<input checked="" type="checkbox"/> Enabled			
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)			
Radio Policy	<input type="text" value="All"/>			
Interface/Interface Group(G)	<input type="text" value="management"/>			
Multicast Vlan Feature	<input type="checkbox"/> Enabled			
Broadcast SSID	<input checked="" type="checkbox"/> Enabled			
NAS-ID	<input type="text" value="none"/>			

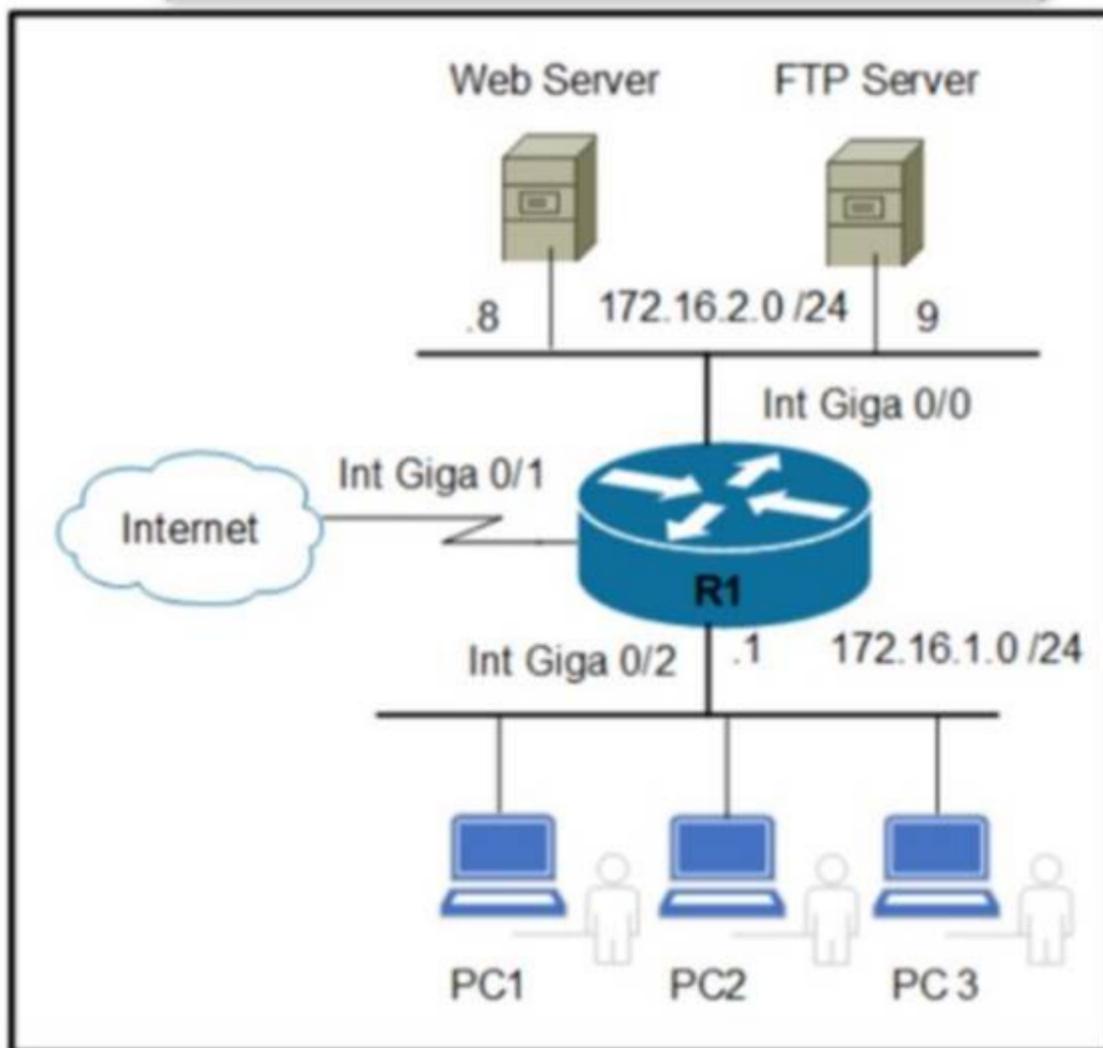
Refer to the exhibit. Clients report that they cannot connect to this SSID using the provided PSK. Which action will resolve this issue?

- A. Apply the correct interface to this WLAN.
- B. Apply the changes this SSID.
- C. Select the PSK under authentication key management.
- D. Define the correct Radio Policy.

Answer: A

**NEW QUESTION 556**

- (Topic 4)



Refer to the exhibit. An engineer must allow the FTP traffic from users on 172.16.1.0 /24 to 172.16.2.0 /24 and block all other traffic. Which configuration must be applied?

- A)
 

```
R1(config)# access-list 120 deny any any
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 21
R1(config)#interface giga 0/0
R1(config-if)#ip access-group 120 out
```
- B)
 

```
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255
R1(config)#interface giga 0/2
R1(config-if)#ip access-group 120 in
```
- C)
 

```
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 20
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 21
R1(config)#interface giga 0/2
R1(config-if)#ip access-group 120 in
```
- D)
 

```
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255
R1(config)# access-list 120 permit udp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255
R1(config)#interface giga 0/2
R1(config-if)#ip access-group 120 out
```

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

Answer: B

**NEW QUESTION 561**

- (Topic 4)  
 Refer to the exhibit.

```
R1#show access-list 100
Extended IP access list 100
 10 deny ip any any
 20 permit ip 192.168.0.0 0.0.255.255 any
 30 permit ip any 192.168.0.0 0.0.255.255
```

Extended access-list 100 is configured on interface GigabitEthernet 0/0 in an inbound direction, but it does not have the expected behavior of allowing only packets to or from 192.168.0.0/16. Which command set properly configures the access list?

- A. R1(config)#no access-list 100 seq 10 R1(config)#access-list 100 seq 40 deny ip any any
- B. R1(config)#ip access-list extended 100 R1(config-ext-nacl)#no 10
- C. R1(config)#no access-list 100 deny ip any any
- D. R1(config)#ip access-list extended 100 R1(config-ext-nacl)#5 permit to any any

**Answer:** A

#### NEW QUESTION 565

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 350-401 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 350-401 Product From:

<https://www.2passeasy.com/dumps/350-401/>

### Money Back Guarantee

#### **350-401 Practice Exam Features:**

- \* 350-401 Questions and Answers Updated Frequently
- \* 350-401 Practice Questions Verified by Expert Senior Certified Staff
- \* 350-401 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 350-401 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year