

➤ **Vendor: Cisco**

➤ **Exam Code: 350-401**

➤ **Exam Name: Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [Jan./2021](#))**

[Visit Braindump2go and Download Full Version 350-401 Exam Dumps](#)

QUESTION 275

How does the EIGRP metric differ from the OSPF metric?

- A. The EIGRP metric is calculated based on bandwidth only. The OSPF metric is calculated on delay only.
- B. The EIGRP metric is calculated based on delay only. The OSPF metric is calculated on bandwidth and delay.
- C. The EIGRP metric is calculated based on bandwidth and delay. The OSPF metric is calculated on bandwidth only.
- D. The EIGRP metric is calculated based on hop count and bandwidth. The OSPF metric is calculated on bandwidth and delay.

Answer: C

Explanation:

By default, EIGRP metric is calculated:

metric = bandwidth + delay

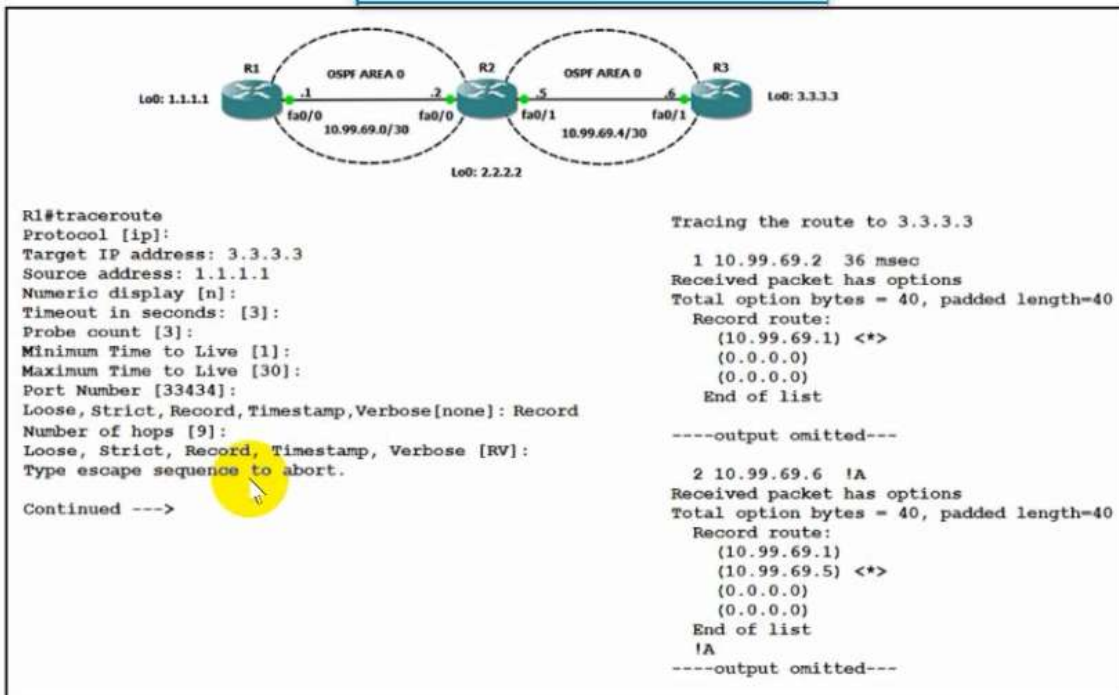
While OSPF is calculated by:

OSPF metric = Reference bandwidth / Interface bandwidth in bps (Or Cisco uses 100Mbps (108) bandwidth as reference bandwidth. With this bandwidth, our equation would be:

Cost = 108/interface bandwidth in bps)

QUESTION 276

Refer to the exhibit. 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

Explanation:

We see in the traceroute result the packet could reach 10.99.69.5 (on R2) but it could not go any further so we can deduce an ACL on R3 was blocking it. Note: Record option displays the address(es) of the hops (up to nine) the packet goes through.

QUESTION 277

What is used to validate the authenticity of the client and is sent in HTTP requests as a JSON object?

- A. SSH
- B. HTTPS
- C. JVT
- D. TLS

Answer: B

Explanation:

<https://developer.atlassian.com/server/crowd/json-requests-and-responses/>

QUESTION 278

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

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

Answer: A

Explanation:

[350-401 Exam Dumps](#) [350-401 Exam Questions](#) [350-401 PDF Dumps](#) [350-401 VCE Dumps](#)

<https://www.braindump2go.com/350-401.html>

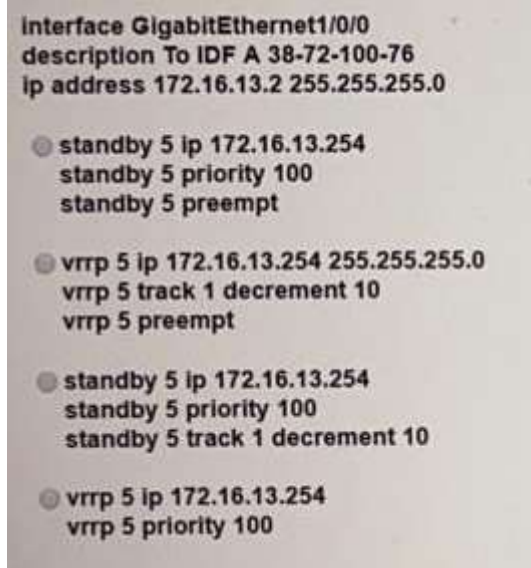
Cisco DNA Center allows customers to manage their non-Cisco devices through the use of a Software Development Kit (SDK) that can be used to create Device Packages for third-party devices.

Reference: <https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/multivendor-support-southbound>

QUESTION 279

An engineer is configuring GigabitEthernet1/0/0 for VRRP. When the router has the highest priority In group 5, It must assume the master role.

Which command set should the engineer add to the configuration to accomplish this task?



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

Answer: B

QUESTION 280

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

- A. fabric control plane node
- B. fabric wireless controller
- C. fabric border node
- D. fabric edge node.

Answer: A

Explanation:

SD-Access Wireless Architecture Control Plane Node - A Closer Look Fabric Control-Plane Node is based on a LISP Map Server / Resolver Runs the LISP Endpoint ID Database to provide overlay reachability information + A simple Host Database, that tracks Endpoint ID to Edge Node bindings (RLOCs) + Host Database supports multiple types of Endpoint ID (EID), such as IPv4 /32, IPv6 /128* or MAC/48 + Receives prefix registrations from Edge Nodes for wired clients, and from Fabric mode WLCs for wireless clients + Resolves lookup requests from FE to locate Endpoints + Updates Fabric Edge nodes, Border nodes with wireless client mobility and RLOC information

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/latam/docs/2018/pdf/BRKEWN-2020.pdf>

QUESTION 281

What is the responsibility of a secondary WLC?

[350-401 Exam Dumps](#) [350-401 Exam Questions](#) [350-401 PDF Dumps](#) [350-401 VCE Dumps](#)

<https://www.braindump2go.com/350-401.html>

- 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

Explanation:

When the primary controller (WLC-1) goes down, the APs automatically get registered with the secondary controller (WLC-2). The APs register back to the primary controller when the primary controller comes back on line. Reference: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/69639-wlc-failover.html>

QUESTION 282

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

- A. TCP
- B. OMP
- C. UDP
- D. BGP

Answer: B

Explanation:

Cisco SD-WAN uses Overlay Management Protocol (OMP) which manages the overlay network. OMP runs between the vSmart controllers and WAN Edge routers (and among vSmarts themselves) where control plane information, such as the routing, policy, and management information, is exchanged over a secure connection.

QUESTION 283

In a Cisco Catalyst switch equipped with two supervisor modules an administrator must temporarily remove the active supervisor from the chassis to perform hardware maintenance on it. Which mechanism ensure that the active supervisor removal is not disruptive to the network operation?

- A. NSF/NSR
- B. SSO
- C. HSRP
- D. VRRP

Answer: B

Explanation:

Stateful Switchover (SSO) provides protection for network edge devices with dual Route Processors (RPs) that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.

Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SY/configuration/guide/sy_swcg/stateful_switchover.html

QUESTION 284

Which deployment option of Cisco NGFW provides scalability?

- A. tap
- B. inline tap
- C. high availability
- D. clustering

Answer: D

Explanation:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/asa-cluster-solution.html>

Clustering lets you group multiple Firepower Threat Defense (FTD) units together as a single logical device. Clustering is only supported for the FTD device on the Firepower 9300 and the Firepower 4100 series. A cluster provides all the

[350-401 Exam Dumps](#) [350-401 Exam Questions](#) [350-401 PDF Dumps](#) [350-401 VCE Dumps](#)

<https://www.braindump2go.com/350-401.html>

convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices.

QUESTION 285

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

- A. DHCP
- B. VXLAN
- C. SXP
- D. LISP

Answer: D

Explanation:

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

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

QUESTION 286

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

- A.

```
class-map match-all CoPP_SSH
match access-group name CoPP_SSH
!
Policy-map CoPP_SSH
class CoPP_SSH police cir 100000
exceed-action drop
!!!
Interface GigabitEthernet0/1
ip address 209.165.200.225 255.255.255.0
ip access-group CoPP_SSH out
duplex auto
speed auto
media-type rj45
service-policy input CoPP_SSH
!
ip access-list extended CoPP_SSH
permit tcp any any eq 22
!
```
- B.

```
class-map match-all CoPP_SSH
match access-group name CoPP_SSH
!
Policy-map CoPP_SSH
class CoPP_SSH
police cir CoPP_SSH
exceed-action drop
!
Interface GigabitEthernet0/1
ip address 209.165.200.225 255.255.255.0
ip access-group ?out
duplex auto
speed auto
media-type rj45
service-policy input CoPP_SSH
!
ip access-list extended CoPP_SSH
deny tcp any any eq 22
!
```
- C.

```
class-map match-all CoPP_SSH
```

[350-401 Exam Dumps](#) [350-401 Exam Questions](#) [350-401 PDF Dumps](#) [350-401 VCE Dumps](#)

<https://www.braindump2go.com/350-401.html>

```
match access-group name CoPP_SSH
```

```
!
```

```
Policy-map CoPP_SSH
```

```
class CoPP_SSH
```

```
police cir 100000
```

```
exceed-action drop
```

```
!
```

```
!
```

```
!
```

```
Control-plane
```

```
service-policy input CoPP_SSH
```

```
!
```

```
ip access-list extended CoPP_SSH
```

```
permit tcp any any eq 22
```

```
!
```

D. class-map match-all CoPP_SSH

```
match access-group name CoPP_SSH
```

```
!
```

```
Policy-map CoPP_SSH
```

```
class CoPP_SSH
```

```
police cir 100000 exceed-action drop
```

```
!
```

```
Control-plane transit
```

```
service-policy input CoPP_SSH
```

```
!
```

```
ip access-list extended CoPP_SSH
```

```
permit tcp any any eq 22
```

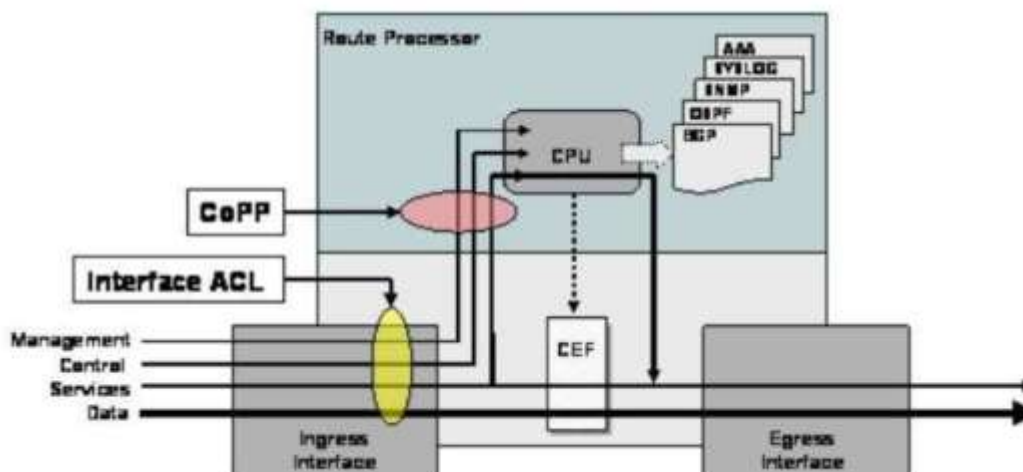
```
!
```

Answer: C

Explanation:

CoPP protects the route processor on network devices by treating route processor resources as a separate entity with its own ingress interface (and in some implementations, egress also). CoPP is used to police traffic that is destined to the route processor of the router such as:

- + routing protocols like OSPF, EIGRP, or BGP.
- + Gateway redundancy protocols like HSRP, VRRP, or GLBP.
- + Network management protocols like telnet, SSH, SNMP, or RADIUS.



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