

➤ **Vendor: Cisco**

➤ **Exam Code: 350-401**

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

➤ **New Updated Questions from [Braindump2go](#) (Updated in [Dec./2020](#))**

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

**QUESTION 146**

Which benefit is offered by a cloud infrastructure deployment but is lacking in an on-premises deployment?

- A. efficient scalability
- B. virtualization
- C. storage capacity
- D. supported systems

**Answer: A**

**QUESTION 147**

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

- A. to connect external Layer 3- network to the SD-Access fabric
- B. to connect wired endpoint to the SD-Access fabric
- C. to advertise fabric IP address space to external network
- D. to connect the fusion router to the SD-Access fabric

**Answer: B**

**QUESTION 148**

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

- A. Cisco Firepower and FireSIGHT
- B. Cisco Stealthwatch system
- C. Advanced Malware Protection
- D. Cisco Web Security Appliance

**Answer: B**

**QUESTION 149**

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

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

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

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

**Answer:** CE

**Explanation:**

There are five basic device roles in the fabric overlay:

- + Control plane node: This node contains the settings, protocols, and mapping tables to provide the endpoint-to-location (EID-to-RLOC) mapping system for the fabric overlay.
- + Fabric border node: This fabric device (for example, core layer device) connects external Layer 3 networks to the SDA fabric.
- + Fabric edge node: This fabric device (for example, access or distribution layer device) connects wired endpoints to the SDA fabric.
- + Fabric WLAN controller (WLC): This fabric device connects APs and wireless endpoints to the SDA fabric.
- + Intermediate nodes: These are intermediate routers or extended switches that do not provide any sort of SD-Access fabric role other than underlay services.

**QUESTION 150**

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

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

**Answer:** C

**QUESTION 151**

What is the role of the RP in PIM sparse mode?

- A. The RP responds to the PIM join messages with the source of requested multicast group
- B. The RP maintains default aging timeouts for all multicast streams requested by the receivers.
- C. The RP acts as a control-plane node and does not receive or forward multicast packets.
- D. The RP is the multicast that is the root of the PIM-SM shared multicast distribution tree.

**Answer:** A

**QUESTION 152**

How does QoS traffic shaping alleviate network congestion?

- A. It drops packets when traffic exceeds a certain bitrate.
- B. It buffers and queue packets above the committed rate.
- C. It fragments large packets and queues them for delivery.
- D. It drops packets randomly from lower priority queues.

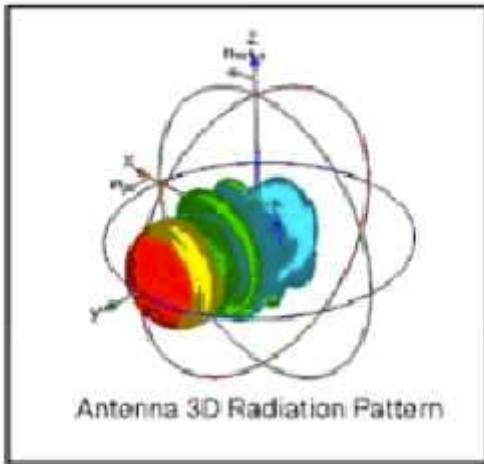
**Answer:** B

**Explanation:**

Traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time. The result of traffic shaping is a smoothed packet output rate

**QUESTION 153**

Refer to the exhibit. Which type of antenna does the radiation pattern represent?



- A. Yagi
- B. multidirectional
- C. directional patch
- D. omnidirectional

**Answer: A**

**QUESTION 154**

Refer to the exhibit. The inside and outside interfaces in the NAT configuration of this device have been correctly identified.

```
access-list 1 permit 172.16.1.0 0.0.0.255
ip nat inside source list 1 interface gigabitethernet0/0 overload
```

What is the effect of this configuration?

- A. dynamic NAT
- B. NAT64
- C. PAT
- D. static NAT

**Answer: C**

**QUESTION 155**

What does the Cisco DNA Center use to enable the delivery of applications through a network and to yield analytics for innovation?

- A. process adapters
- B. Command Runner
- C. intent-based APIs
- D. domain adapters

**Answer: C**

**QUESTION 156**

Why is an AP joining a different WLC than the one specified through option 43?

- A. The WLC is running a different software version.
- B. The API is joining a primed WLC

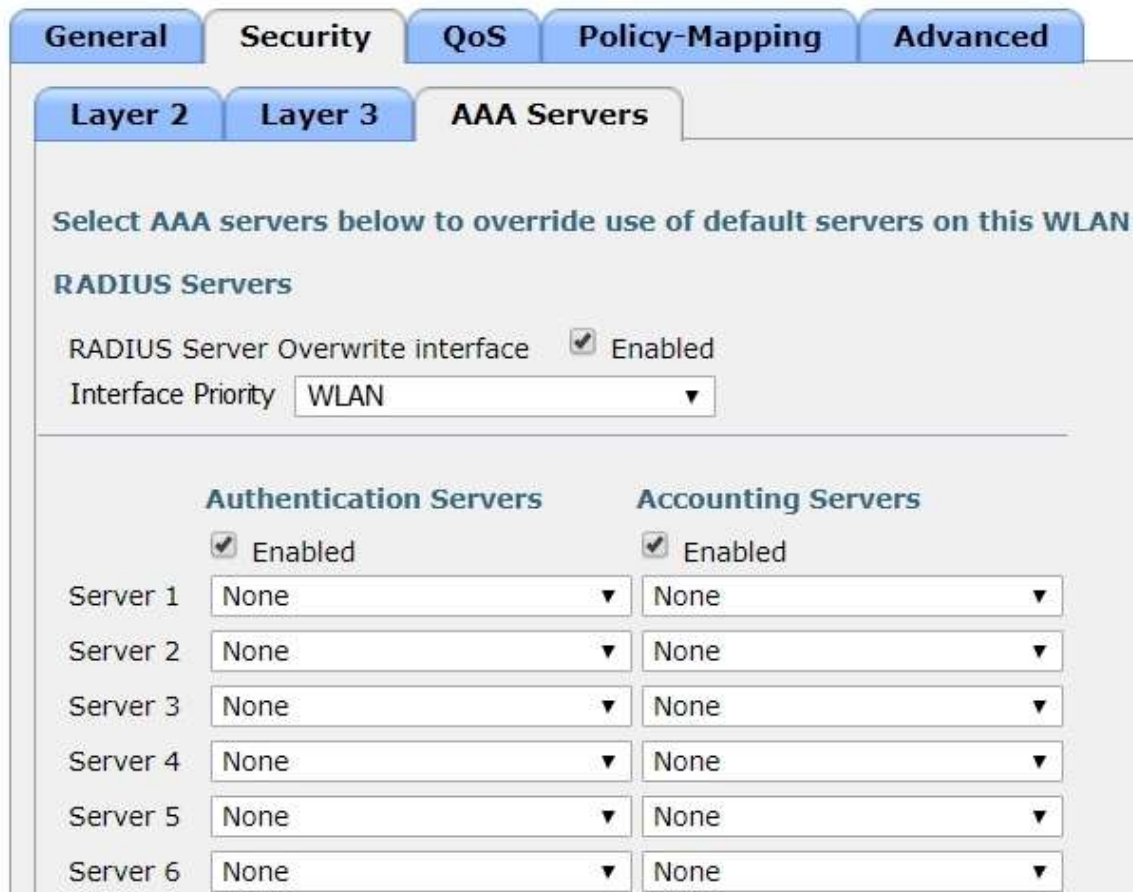
- C. The AP multicast traffic unable to reach the WLC through Layer 3.
- D. The APs broadcast traffic is unable to reach the WLC through Layer 2.

**Answer: B**

#### QUESTION 157

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

**WLANs > Edit 'Guest\_Wireless'**



The screenshot shows the 'AAA Servers' configuration page for the 'Guest\_Wireless' WLAN. The 'RADIUS Servers' section is active, showing 'RADIUS Server Overwrite interface' set to 'Enabled' and 'Interface Priority' set to 'WLAN'. Below this, there are two columns: 'Authentication Servers' and 'Accounting Servers'. Both columns have a checkbox for 'Enabled' which is checked. Each column contains a table with 6 rows, labeled 'Server 1' through 'Server 6'. Each row has a dropdown menu currently set to 'None'.

Authentication Servers		Accounting Servers	
<input checked="" type="checkbox"/> Enabled	None	<input checked="" type="checkbox"/> Enabled	None
Server 1	None	Server 1	None
Server 2	None	Server 2	None
Server 3	None	Server 3	None
Server 4	None	Server 4	None
Server 5	None	Server 5	None
Server 6	None	Server 6	None

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

**Answer: A**

#### QUESTION 158

An engineer must protect their company against ransom ware attacks. Which solution allows the engineer to block the execution stage and prevent file encryption?

- A. Use Cisco AMP deployment with the Malicious Activity Protection engine enabled.
- B. Use Cisco AMP deployment with the Exploit Prevention engine enabled.
- C. Use Cisco Firepower and block traffic to TOR networks.
- D. Use Cisco Firepower with Intrusion Policy and snort rules blocking SMB exploitation.

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

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

**Answer: A**

**QUESTION 159**

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

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

Which action reduces the user impact?

- A. increase the AP heartbeat timeout
- B. increase BandSelect
- C. enable coverage hole detection
- D. increase the dynamic channel assignment interval

**Answer: D**

**QUESTION 160**

Which algorithms are used to secure REST API from brute attacks and minimize the impact?

- A. SHA-512 and SHA-384
- B. MD5 algorithm-128 and SHA-384
- C. SHA-1, SHA-256, and SHA-512
- D. PBKDF2, BCrypt, and SCrypt

**Answer: D**

**Explanation:**

One of the best practices to secure REST APIs is using password hash. Passwords must always be hashed to protect the system (or minimize the damage) even if it is compromised in some hacking attempts. There are many such hashing algorithms which can prove really effective for password security e.g. PBKDF2, bcrypt and scrypt algorithms. Other ways to secure REST APIs are: Always use HTTPS, Never expose information on URLs (Usernames, passwords, session tokens, and API keys should not appear in the URL), Adding Timestamp in Request, Using OAuth, Input Parameter Validation.

Reference: <https://restfulapi.net/security-essentials/>

We should not use MD5 or any SHA (SHA-1, SHA-256, SHA-512...) algorithm to hash password as they are not totally secure.

Note: A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.