350-401 Q&As

Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) & CCIE Enterprise Infrastructure & CCIE Enterprise Wireless

Pass Cisco 350-401 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/350-401.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

Correct Answer: D

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.

QUESTION 2

Which function does a fabric edge node perform in an SD-Access deployment?

A. Connects the SD-Access fabric to another fabric or external Layer 3 networks.

B. Connects endpoints to the fabric and forwards their traffic.

C. Provides reachability border nodes in the fabric underlay.

D. Encapsulates end-user data traffic into LISP.

Correct Answer: B

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,

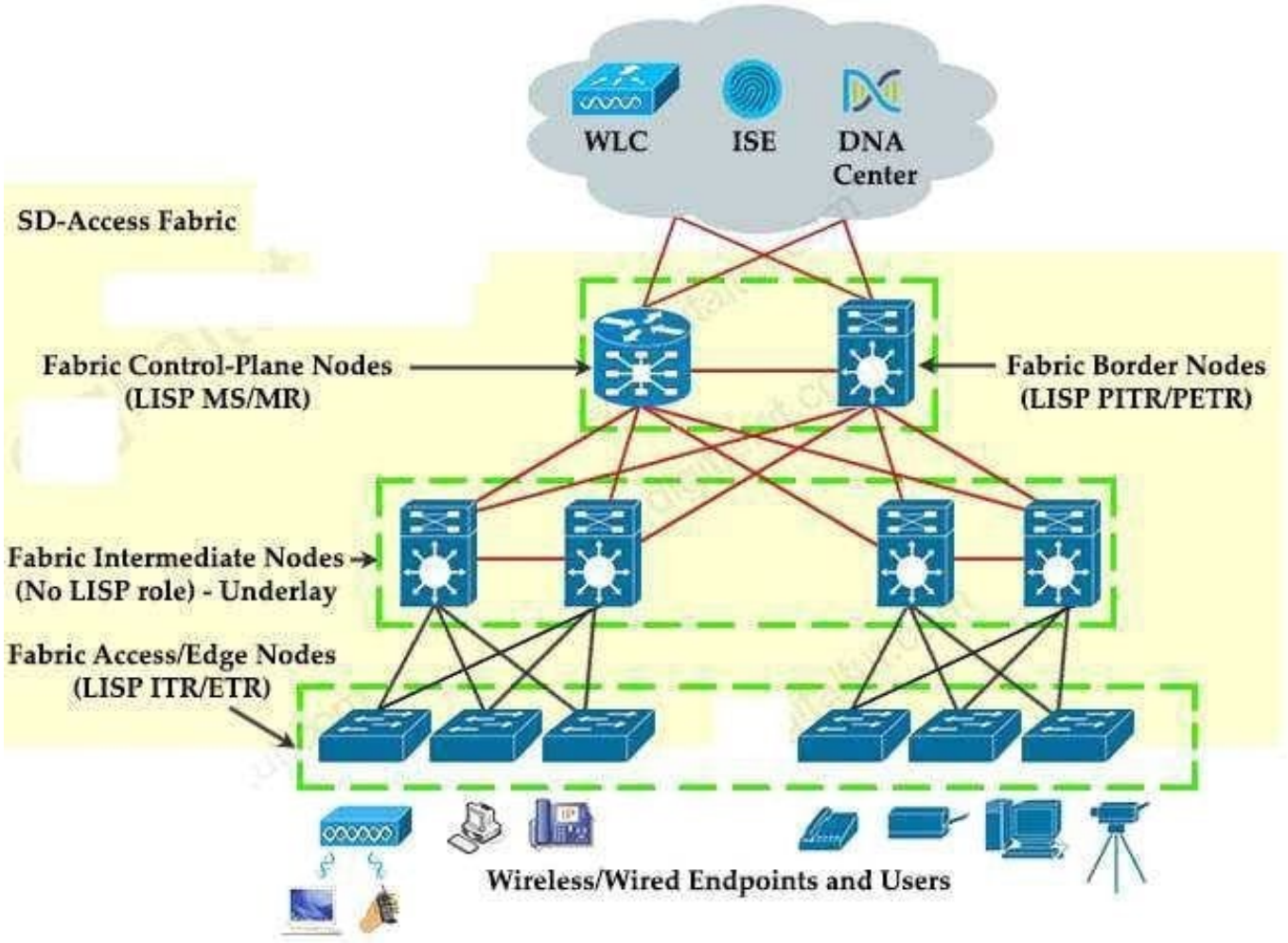
access or distribution layer device) connects wired endpoints to the SDA fabric.

+

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 3

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

A. The RP responds to the PIM join messes 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.

Correct Answer: D

Multicast Distribution Shared Tree - Unlike source trees that have their root at the source, shared trees use a single common root placed at some chosen point in the network. This shared root is called a rendezvous point (RP).

Source:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-5/configuration_guide/ip_mcast_rtng/b_165_ip_mcast_rtng_9300_cg/b_165_ip_mcast_rtng _9300_9500_cg_chapter_0100.html
https://netcraftsmen.com/

pim-sparse-mode/

QUESTION 4

Refer to the exhibit.

```
R1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 65001
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.2    4        65002       0       0        1    0    0 00:00:15 Idle
R1#show ip interface brief | include 192.168.12
FastEthernet0/0            192.168.12.1    YES NVRAM  up                    up

R2#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 65002
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.1    4        65001       0       0        1    0    0 00:01:00 Idle (Admin)
R2#show ip interface brief | include 192.168.12
Ethernet0/0                192.168.12.2    YES NVRAM  up                    up
R2#ping 192.168.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

R1 and R2 are directly connected, but the BGP session does not establish. Which action must be taken to build an eBGP session?

A. Configure ip route 1.1.1.1 0.0.0.0 192.168.12.1 on R2.

B. Configure neighbor 192.168.12.1 activate under R2 BGP process.

C. Configure neighbor 2.2.2.2 remote-as 65002 under R1 BGP process.

D. Configure no neighbor 192.168.12.1 shutdown under R2 BGP process.

Correct Answer: D

Reference: https://www.noction.com/blog/debug-bgp-states#:~:text=Idle%20(Admin)%20means%20that%20the,!andtext=This%20is%20a%20good%20way,BGP%20section%20of%20the%20configuration

QUESTION 5

Refer to the exhibit.

```
switch1(config)# interface GigabitEthernet 1/1
switch1(config-if)# switchport mode trunk
switch1(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70-90
switch1(config)# exit
switch1(config)# monitor session 1 source vlan 10
switch1(config)# monitor session 1 destination remote vlan 70


switch2(config)# interface GigabitEthernet 1/1
switch2(config-if)# switchport mode trunk
switch2(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,80-90
switch2(config)# exit
switch2(config)# monitor session 2 source remote vlan 70
switch2(config)# monitor session 2 destination interface GigabitEthernet1/1
```

A network administrator configured RSPAN to troubleshoot an issue between switchl and switch2. The switches are connected using interface GigabitEthernet 1/1 An external packet capture device is connected to swich2 interface GigabitEthernet1/2 Which two commands must be added to complete this configuration? (Choose two)

A. switch2(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70-80

B. switch2(config)# monitor session 1 source remote vlan 70 switch2(config)# monitor session 1 destination interface GigabitEthernet1/2

C. switch1(config)# interface GigabitEthernet 1/1 switch1(config-if)# switchport mode access switch1(config-if)# switchport access vlan 10 switch2(config)# interface GigabitEthernet 1/1 switch2(config-if)# switchport mode access switch2(config-if)# switchport access vlan 10

D. switch2(config)# monitor session 2 destination vlan 10

E. switch2(config)# monitor session 1 source remote vlan 70 switch2(config)# monitor session 1 destination interface GigabitEthernet1/1

Correct Answer: AB