200-301 Q&As

Implementing and Administering Cisco Solutions (CCNA) (Include Newest Simulation Labs)

Pass Cisco 200-301 Exam with 100% Guarantee

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

https://www.geekcert.com/200-301.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 two capabilities of Cisco DNA Center make it more extensible? (Choose two.)

A. REST APIs that allow for external applications to interact natively with Cisco DNA Center

B. adapters that support all families of Cisco IOS Software

C. SDKs that support interaction with third-party network equipment

D. modular design that is upgradable as needed

E. customized versions for small, medium, and large enterprises

Correct Answer: AC

Cisco DNA Center offers 360-degree extensibility through four distinct types of platform capabilities:

1.

Intent-based APIs leverage the controller and enable business and IT applications to deliver intent to the network and to reap network analytics and insights for IT and business innovation.

2.

Process adapters, built on integration APIs, allow integration with other IT and network systems to streamline IT operations and processes.

3.

Domain adapters, built on integration APIs, allow integration with other infrastructure domains such as data center, WAN, and security to deliver a consistent intent-based infrastructure across the entire IT environment.

4.

SDKs allow management to be extended to third-party vendor\\'s network devices to offer support for diverse environments.

Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-cent-platf-aag-cte-en.html

QUESTION 2

Which QoS traffic handling technique retains excess packets in a queue and reschedules these packets for later transmission when the configured maximum bandwidth has been surpassed?

A. weighted random early detection

B. traffic policing

C. traffic shaping

D. traffic prioritization

Correct Answer: C

QUESTION 3

A client experiences slow throughput from a server that is directly connected to the core switch in a data center. A network engineer finds minimal latency on connections to the server, but data transfers are unreliable, and the output of the show Interfaces counters errors command shows a high FCS-Err count on the interface that is connected to the server. What is the cause of the throughput issue?

A. high bandwidth usage

B. a physical cable fault

C. a speed mismatch

D. a cable that is too long

Correct Answer: B

The cause of the throughput issue described in the scenario is a physical cable fault.

The scenario mentions that the network engineer found minimal latency on connections to the server, but data transfers are unreliable, and the output of the "show interfaces counters errors" command shows a high FCS-Err count on the

interface that is connected to the server. FCS-Err (Frame Check Sequence error) indicates that there is a physical issue with the cable, such as noise or interference, that is causing the data transfer errors.

A speed mismatch or high bandwidth usage may cause slow throughput or delays, but it would not cause FCS-Err errors. Similarly, a cable that is too long may cause signal attenuation, but it would not cause FCS-Err errors.

QUESTION 4

Which two statements about EtherChannel technology are true? (Choose two.)

A. EtherChannel provides increased bandwidth by bundling existing FastEthernet or Gigabit Ethernet interfaces into a single EtherChannel.

B. STP does not block EtherChannel links.

C. You can configure multiple EtherChannel links between two switches, using up to a limit of sixteen physical ports.

D. EtherChannel does not allow load sharing of traffic among the physical links within the EtherChannel.

E. EtherChannel allows redundancy in case one or more links in the EtherChannel fail.

Correct Answer: AE

QUESTION 5

What are two differences between WPA2 and WPA3 wireless security? (Choose two.)

A. WPA2 uses 192-bit key encryption, and WPA3 requires 256-bit key encryption.

B. WPA3 uses AES for stronger protection than WPA2, which uses SAE.

C. WPA2 uses 128-bit key encryption, and WPA3 supports 128-bit and 192-bit key encryption.

D. WPA3 uses SAE for stronger protection than WPA2, which uses AES.

E. WPA3 uses AES for stronger protection than WPA2, which uses TKIP.

Correct Answer: CD