# 100-101 Q&As

CCNA Interconnecting Cisco Networking Devices 1 (ICND1)

## Pass Cisco 100-101 Exam with 100% Guarantee

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

**https://www.passapply.com/100-101.html**

100% Passing Guarantee
100% Money Back Assurance

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

**QUESTION 1**

Which characteristics are representative of a link-state routing protocol? (Choose three.)

A. provides common view of entire topology

B. exchanges routing tables with neighbors

C. calculates shortest path

D. utilizes event-triggered updates

E. utilizes frequent periodic updates

Correct Answer: ACD

Each of routers running link-state routing protocol learns paths to all the destinations in its "area" so we can say although it is a bit unclear.

Link-state routing protocols generate routing updates only (not the whole routing table) when a change occurs in the network topology so

Link-state routing protocol like OSPF uses Dijkstra algorithm to calculate the shortest path -> . Unlike Distance vector routing protocol (which utilizes frequent periodic updates), link-state routing protocol utilizes event-triggered updates (only

sends update when a change occurs) ->

**QUESTION 2**

Given an IP address of 192.168.1.42 255.255.255.248, what is the subnet address?

A. 192.168.1.8/29

B. 192.168.1.32/27

C. 192.168.1.40/29

D. 192.168.1.16/28

E. 192.168.1.48/29

Correct Answer: C

248 mask uses 5 bits (1111 1000)

.42 IP in binary is (0010 1010)

The base subnet therefore is the lowest binary value that can be written without changing the output of an AND operation of the subnet mask and IP...

1111 1000 AND

0010 1010 equals

0010 1000 - which is .40

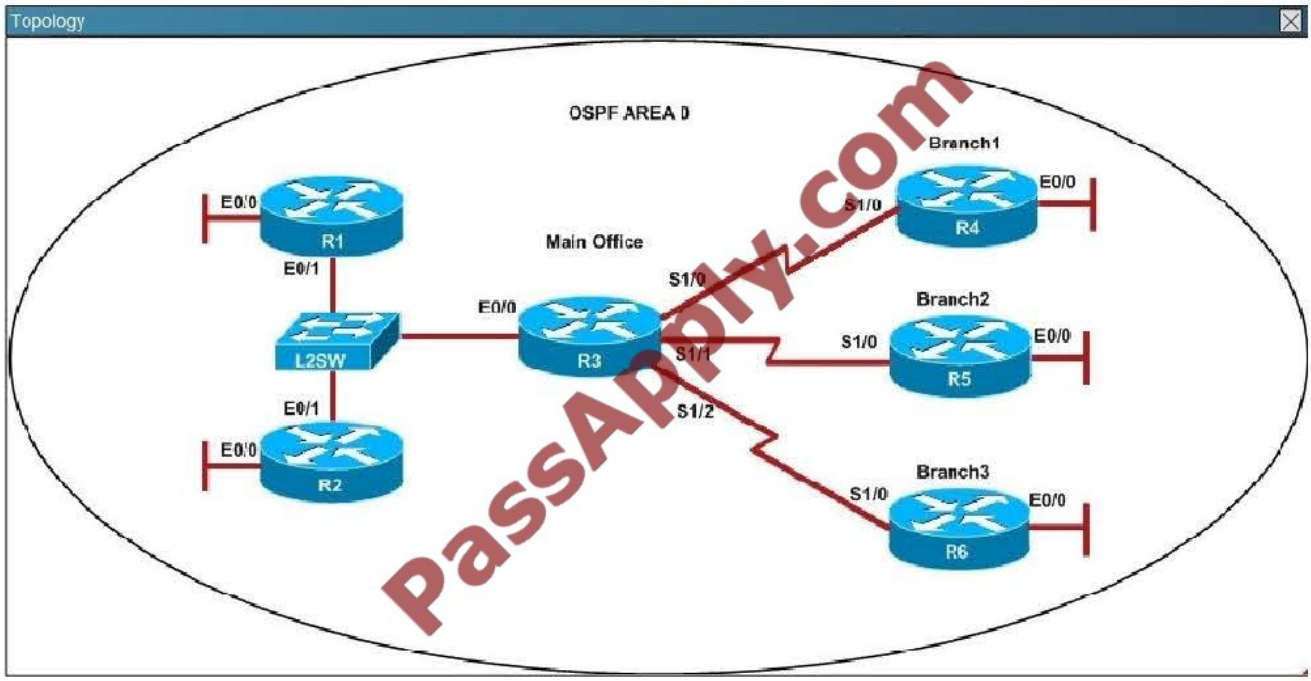
/24 is standard class C mask.

Adding the 5 bits from the .248 mask gives /29

**QUESTION 3**

Scenario

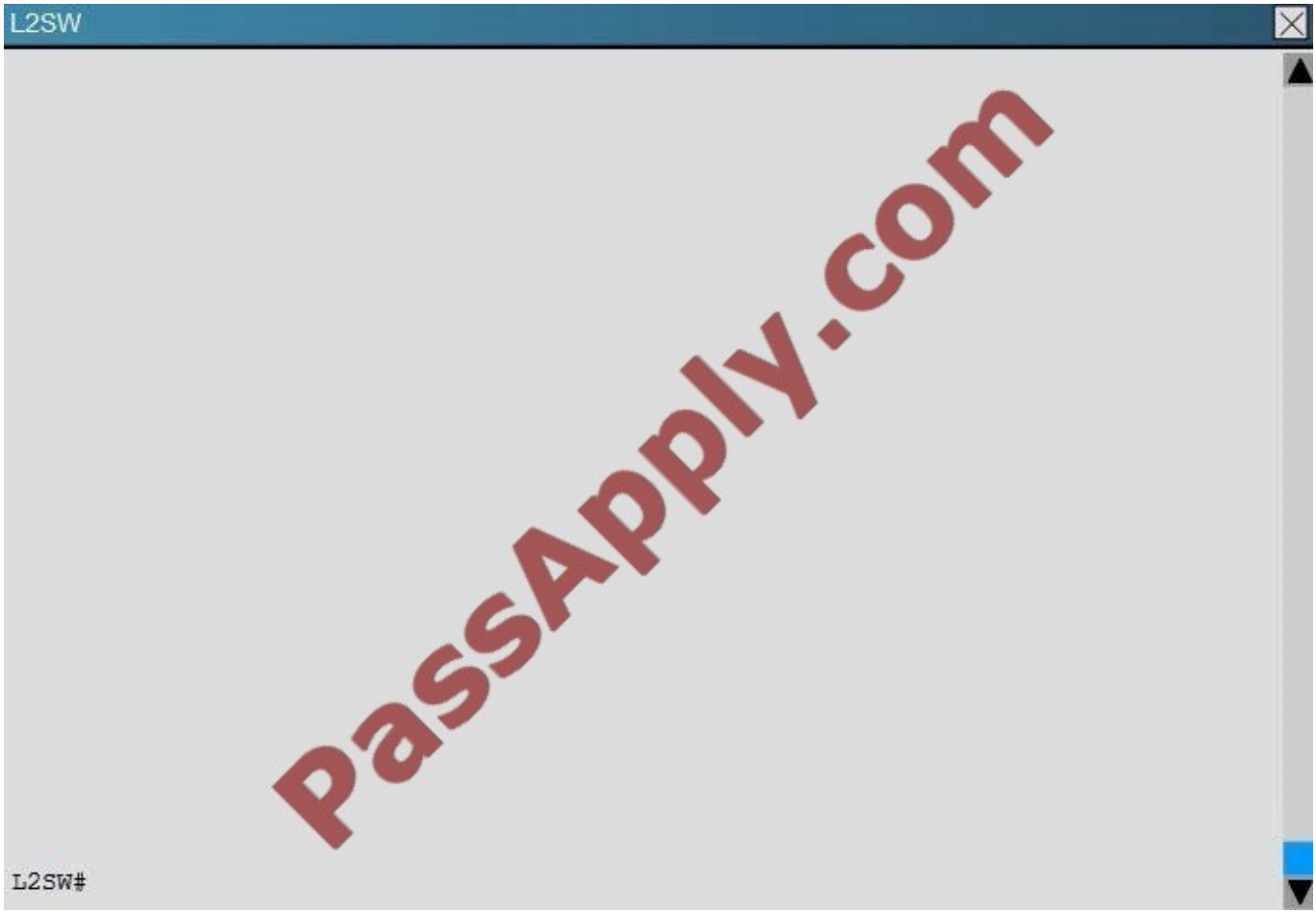
Refer to the topology. Your company has decided to connect the main office with three other remote branch offices using point-to-point serial links. You are required to troubleshoot and resolve OSPF neighbor adjacency issues between the main office and the routers located in the remote branch offices.




R4
R4#
PassApply.com


R5
R5#
PassApply.com


R6
R6#
PassApply.com




An OSPF neighbor adjacency is not formed between R3 in the main office and R6 in the Branch3 office. What is causing the problem?

A. There is an area ID mismatch.

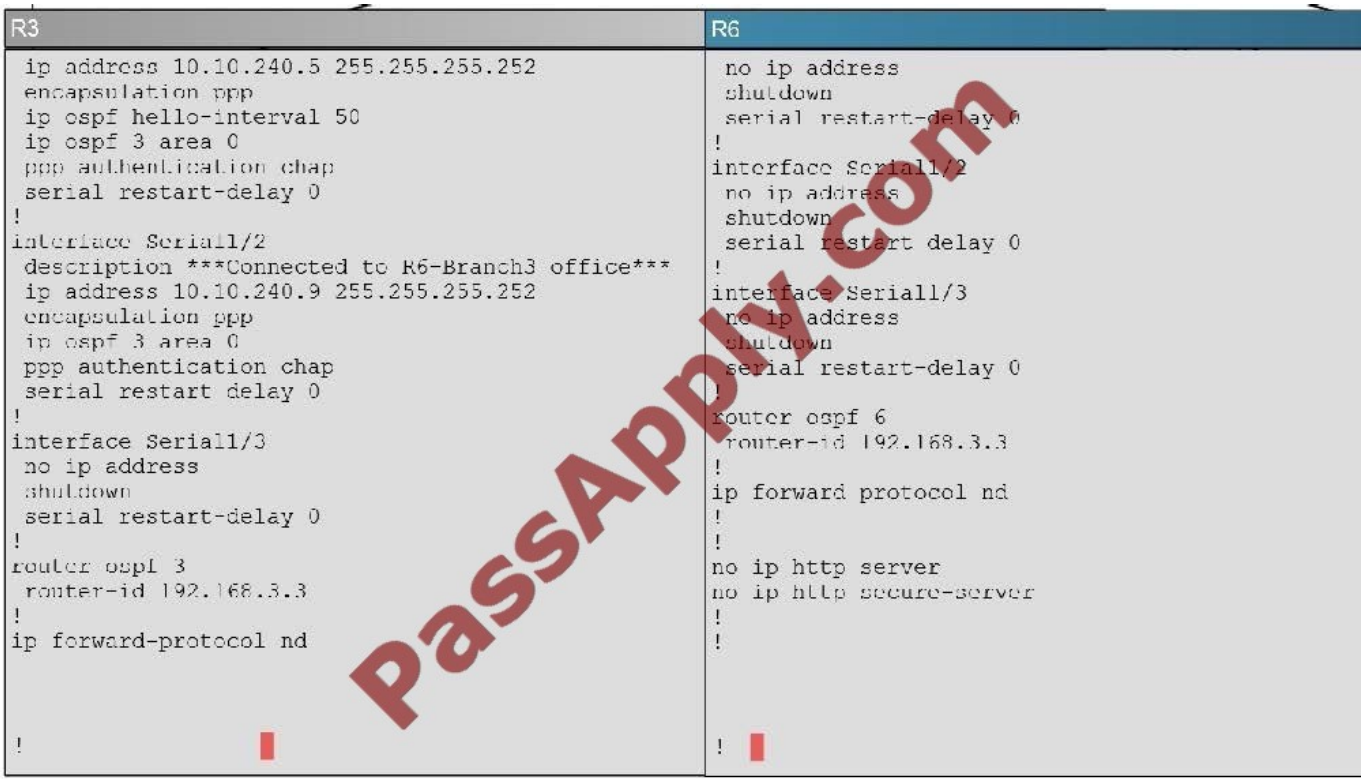
B. There is a PPP authentication issue; the username is not configured on R3 and R6.

C. There is an OSPF hello and dead interval mismatch.

D. The R3 router ID is configured on R6.

Correct Answer: D

Using the show running-config command we see that R6 has been incorrectly configured with the same router ID as R3 under the router OSPF process.






**QUESTION 4**

If a host experiences intermittent issues that relate to congestion within a network while remaining connected, what could cause congestion on this LAN?

A. half-duplex operation

B. broadcast storms

C. network segmentation

D. multicasting

Correct Answer: B

A broadcast storm can consume sufficient network resources so as to render the network unable to transport normal traffic.

**QUESTION 5**

From which of the following attacks can Message Authentication Code (MAC) shield your network?

A. DoS

B. DDoS

C. spoofing

D. SYN floods

Correct Answer: C

Message Authentication Code (MAC) can shield your network from spoofing attacks. Spoofing, also known as masquerading, is a popular trick in which an attacker intercepts a network packet, replaces the source address of the packets header with the address of the authorized host, and reinserts fake information which is sent to the receiver. This type of attack involves modifying packet contents. MAC can prevent this type of attack and ensure data integrity by ensuring that no data has changed. MAC also protects against frequency analysis, sequence manipulation, and ciphertext-only attacks. MAC is a secure message digest that requires a secret key shared by the sender and receiver, making it impossible for sniffers to change both the data and the MAC as the receiver can detect the changes. A denial-of-service (DoS) attack floods the target system with unwanted requests, causing the loss of service to users. One form of this attack generates a flood of packets requesting a TCP connection with the target, tying up all resources and making the target unable to service other requests. MAC does not prevent DoS attacks. Stateful packet filtering is the most common defense against a DoS attack. A Distributed Denial of Service attack (DDoS) occurs when multiple systems are used to flood the network and tax the resources of the target system. Various intrusion detection systems, utilizing stateful packet filtering, can protect against DDoS attacks. In a SYN flood attack, the attacker floods the target with spoofed IP packets and causes it to either freeze or crash. A SYN flood attack is a type of denial of service attack that exploits the buffers of a device that accept incoming connections and therefore cannot be prevented by MAC. Common defenses against a SYN flood attack include filtering, reducing the SYN- RECEIVED timer, and implementing SYN cache or SYN cookies.