CCNA 2 Switching, Routing, and Wireless Essentials, Version 7.0 Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here’s how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don’t just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There’s no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **What is the effect of entering the ip dhcp snooping limit rate 6 configuration command on a switch?**

   A. It disables DHCP snooping on all interfaces

   B. It restricts the number of discovery messages, per second, to be received on the interface

   C. It enables DHCP server functionalities on the switch

   D. It allows unlimited DHCP requests from the interface

2. **What is the purpose of the Spanning Tree Protocol (STP) in a network?**

   A. To provide redundancy in an IP routing protocol

   B. To filter traffic based on MAC addresses

   C. To prevent looped paths in a switched network

   D. To manage VLAN configurations across multiple switches

3. **What must be true for hosts on different VLANs to communicate with each other?**

   A. They must be connected to the same switch

   B. They must have the same IP address

   C. A router or Layer 3 switch must be present

   D. They must use the same protocol

4. **What should a network administrator configure if Host C is unable to ping Host D due to switch issues?**

   A. Change Host C's VLAN

   B. Configure trunk port to dynamic desirable mode

   C. Increase the STP priority

   D. Disable port security features

5. **What is the effect of entering the ip arp inspection validate src-mac configuration command on a switch?**

   A. It checks the source L2 address in the Ethernet header against the sender L2 address in the ARP body

   B. It allows all ARP packets to pass through without validation

   C. It logs all ARP packets received on the switch

   D. It enables ARP forwarding on all interfaces

6. What is the purpose of the command "ip route 0.0.0.0 0.0.0.0 serial 0/1/1"?

A. To direct all traffic specifically to the 10.10.0.0/16 network

B. To create a default route to the Internet

C. To prevent routing loops

D. To configure static routes for local networks

7. Which three configurations are essential for setting up remote management access on a new Cisco switch?

A. IP address, VTY lines, Subnet mask

B. IP address, VTY lines, Default gateway

C. Management IP, Console lines, Default gateway

D. IP address, FastEthernet lines, DHCP settings

8. Which command can be used to verify the current IP address configuration on a switch?

A. show ip route

B. show ip interface brief

C. show interfaces status

D. show running-config

9. What protocol or technology uses source IP to destination IP as a load-balancing mechanism?

A. EtherChannel

B. Spanning Tree Protocol

C. Link Aggregation Control Protocol

D. Virtual Router Redundancy Protocol

10. What happens when the source MAC address of a frame entering a switch appears in the MAC address table associated with a different port?

A. The switch ignores the frame and drops it

B. The switch replaces the old entry and uses the more current port

C. The switch generates an alert for the network administrator

D. The switch disables the port temporarily

Answers

1. B
2. C
3. C
4. B
5. A
6. B
7. B
8. B
9. A
10. B

Explanations

1. What is the effect of entering the ip dhcp snooping limit rate 6 configuration command on a switch?

A. It disables DHCP snooping on all interfaces

B. It restricts the number of discovery messages, per second, to be received on the interface

C. It enables DHCP server functionalities on the switch

D. It allows unlimited DHCP requests from the interface

Entering the command to configure a rate limit for DHCP snooping, such as "ip dhcp snooping limit rate 6," is meant to enhance network security by controlling the amount of DHCP discovery messages handled by a switch interface. Specifically, this command restricts the number of DHCP discovery messages that can be received on the interface to six messages per second. This is important because it helps mitigate the risk of DHCP spoofing attacks, where a malicious device could overwhelm the legitimate DHCP server with a flood of requests to disrupt network service. By setting a limit, the switch can help maintain better performance and stability by preventing excessive traffic and ensuring that only a controlled number of requests are processed. Other options do not align with the intended functionality of this command, as they either imply disabling features or enabling functionalities not related to the limitation of DHCP messages.

2. What is the purpose of the Spanning Tree Protocol (STP) in a network?

A. To provide redundancy in an IP routing protocol

B. To filter traffic based on MAC addresses

C. To prevent looped paths in a switched network

D. To manage VLAN configurations across multiple switches

The Spanning Tree Protocol (STP) is designed specifically to prevent looped paths in a switched network. In Ethernet networks, when there are multiple paths between switches for redundancy, the potential for loops arises. Loops can cause broadcast storms, multiple frame copies, and overall network degradation. STP operates by placing certain ports in a blocking state to eliminate these loops while still providing a single active path between any two network devices in the switched topology. This ensures that there is no infinite loop of data frames circulating through the network, which would consume bandwidth and can lead to network outages. By allowing only a single logical path between switches while maintaining the configuration to quickly adapt in case of a link failure, STP enhances network reliability and helps maintain optimal data flow.

3. What must be true for hosts on different VLANs to communicate with each other?

A. They must be connected to the same switch

B. They must have the same IP address

C. A router or Layer 3 switch must be present

D. They must use the same protocol

For hosts on different VLANs to communicate with each other, a router or Layer 3 switch must be present to perform inter-VLAN routing. VLANs (Virtual Local Area Networks) logically segment a network, allowing devices within the same VLAN to communicate directly, while isolating traffic from devices in different VLANs. Since VLANs create separate broadcast domains, devices in different VLANs cannot communicate directly without routing. A router or Layer 3 switch functions to route traffic between these separated broadcast domains. By performing this routing, it allows the necessary traffic to flow between hosts that are on different VLANs, enabling communication. This is essential for maintaining network organization, security, and traffic management. The other options do not address the requirement for inter-VLAN communication effectively. Being connected to the same switch does not solve the isolation issue posed by VLANs. Having the same IP address would not facilitate communication across different networks and is generally discouraged as it can lead to address conflicts. Finally, using the same protocol is irrelevant, as VLAN communication strictly relies on routing capabilities, rather than protocol compatibility.

4. What should a network administrator configure if Host C is unable to ping Host D due to switch issues?

A. Change Host C's VLAN

B. Configure trunk port to dynamic desirable mode

C. Increase the STP priority

D. Disable port security features

The correct choice involves configuring a trunk port to dynamic desirable mode, which is pivotal in ensuring proper VLAN communication across switches. In a scenario where Host C cannot ping Host D due to issues related to the switch, it's likely that the VLANs the hosts are on are not properly communicating with each other. This could be due to the fact that the connecting port between switches is not properly set to allow VLAN traffic. By configuring the trunk port to dynamic desirable mode, the switch port will actively attempt to negotiate trunking with the attached device. This mode is part of Dynamic Trunking Protocol (DTP), which allows the port to dynamically establish a trunk link if the other end supports it. If Host C and Host D are in different VLANs, ensuring that the trunking is configured correctly allows traffic for those VLANs to traverse the link between switches, thus enabling proper communication. VLAN configuration is essential for network segmentation and ensuring that devices on different VLANs can communicate under the right circumstances, and dynamic desirable mode helps facilitate that process by managing how VLAN information is passed between the switches.

5. What is the effect of entering the ip arp inspection validate src-mac configuration command on a switch?

A. It checks the source L2 address in the Ethernet header against the sender L2 address in the ARP body

B. It allows all ARP packets to pass through without validation

C. It logs all ARP packets received on the switch

D. It enables ARP forwarding on all interfaces

Entering the command to validate the source MAC address in ARP packets on a switch serves a very specific security purpose. This command ensures that the source Layer 2 (L2) address found in the Ethernet frame header is consistent with the sender L2 address specified in the ARP protocol data within the packet. By performing this check, the switch enhances its protection against ARP spoofing or poisoning attacks, where an attacker sends fraudulent ARP messages onto a network. When the switch verifies that these two addresses match, it can prevent malicious users from intercepting traffic or redirecting network communications. The other choices do not accurately describe the function of the command. Some imply a lack of validation or unnecessary logging, which does not align with the intent of ARP inspection features designed to secure the network. This validation improves the reliability and integrity of ARP communications within the network.

6. What is the purpose of the command "ip route 0.0.0.0 0.0.0.0 serial 0/1/1"?

A. To direct all traffic specifically to the 10.10.0.0/16 network

B. To create a default route to the Internet

C. To prevent routing loops

D. To configure static routes for local networks

The command "ip route 0.0.0.0 0.0.0.0 serial 0/1/1" is designed to establish a default route in a router's routing table. A default route is a type of static route that directs packets destined for any network that does not have a specific route in the routing table to a designated next-hop interface. The use of the address 0.0.0.0 with the subnet mask 0.0.0.0 indicates that this route applies to any destination address, effectively serving as a catch-all route. In this case, the command specifies that all traffic that does not match a more specific route should be forwarded out of the serial interface labeled 0/1/1. This configuration is essential for directing outbound traffic to the Internet, where there is typically no specific route for all possible external addresses. By setting up this default route, the router can handle traffic intended for destinations not explicitly defined in its routing table, thus ensuring connectivity with external networks, including the Internet. This command is integral in scenarios where a device needs to communicate with a variety of networks beyond its directly connected segments, streamlining routing by providing a simple fallback option.

7. Which three configurations are essential for setting up remote management access on a new Cisco switch?

A. IP address, VTY lines, Subnet mask

B. IP address, VTY lines, Default gateway

C. Management IP, Console lines, Default gateway

D. IP address, FastEthernet lines, DHCP settings

To enable remote management access on a Cisco switch, establishing the IP address, configuring VTY (Virtual Terminal) lines, and setting up a default gateway are crucial components. The IP address configuration allows the switch to be identifiable and reachable within a network. Without an IP address, remote devices cannot communicate with the switch, preventing remote management. VTY lines are essential for configuring remote access to the switch via protocols such as SSH or Telnet. These lines define the number of simultaneous remote management connections that can be made to the switch, enabling users to login and manage the switch settings remotely. The default gateway is necessary for packets destined for other networks to be routed correctly. If a remote management request originates from a different subnet, the switch must know where to send packets that should leave its local subnet. The default gateway serves this purpose, allowing the switch to communicate beyond its local network. In summary, an IP address makes the switch reachable, VTY lines facilitate remote access, and a default gateway enables communication with devices outside the local network, all of which are fundamental for managing a Cisco switch remotely.

8. Which command can be used to verify the current IP address configuration on a switch?

A. show ip route

B. show ip interface brief

C. show interfaces status

D. show running-config

The command that can be used to verify the current IP address configuration on a switch is "show ip interface brief." This command provides a concise overview of all the interfaces on the switch, displaying their current status (whether they are up or down), as well as the assigned IP addresses and whether those interfaces have been configured with a specific IP address. This is particularly useful for quickly assessing the IP configurations of a switch's interfaces without delving into the detailed output of each interface. Using this command helps network administrators quickly identify any interfaces that may not have been assigned an IP address or that are not operational, facilitating efficient troubleshooting and network management. Additionally, it consolidates vital information into an easily readable format, making it a preferred choice for verifying current IP settings. Other commands, while useful for different aspects of networking or configuration, do not provide this specific overview of IP address settings in such a straightforward manner. For instance, "show ip route" focuses on the routing table, "show interfaces status" provides details about the interface status without IP address information, and "show running-config" presents the entire configuration but can be overwhelming when you are just looking for IP address information. Thus, "show ip interface brief" is expressly designed for verifying the IP

9. What protocol or technology uses source IP to destination IP as a load-balancing mechanism?

A. EtherChannel

B. Spanning Tree Protocol

C. Link Aggregation Control Protocol

D. Virtual Router Redundancy Protocol

The correct answer is EtherChannel, as it utilizes a load-balancing mechanism based on the source IP address and the destination IP address. This protocol allows for the aggregation of multiple physical Ethernet links into a single logical link, providing enhanced bandwidth and redundancy. When traffic passes through an EtherChannel, the device evaluates the source and destination IP addresses to distribute the traffic load evenly across the available physical links. This efficient distribution helps optimize network performance and improves overall throughput by taking advantage of parallel data transmission. In contrast, Spanning Tree Protocol is primarily used to prevent loops in network topologies by creating a loop-free logical structure; it does not perform load balancing based on IP addresses. Link Aggregation Control Protocol acts as a control protocol for the aggregation but does not determine load balancing based on source and destination IPs. Virtual Router Redundancy Protocol focuses on providing failover redundancy in network routing but does not directly involve load balancing across multiple links. Thus, EtherChannel is specifically designed for the purpose of load balancing using source and destination IPs.

10. What happens when the source MAC address of a frame entering a switch appears in the MAC address table associated with a different port?

A. The switch ignores the frame and drops it

B. The switch replaces the old entry and uses the more current port

C. The switch generates an alert for the network administrator

D. The switch disables the port temporarily

When a frame enters a switch and its source MAC address is already in the MAC address table associated with a different port, the switch will replace the old entry and update it to reflect the more current port. This behavior is crucial for maintaining an accurate understanding of which devices are connected to which ports at any given time. This updating process occurs because switches rely on the MAC address table to forward frames efficiently. When a frame is received, the switch checks the source MAC address. If that address is already listed in the MAC address table but associated with a different port, the switch assumes that the device has moved to this new port, and it updates the table accordingly. This ensures that future frames destined for that MAC address are sent to the correct port, maintaining optimal network performance and ensuring communication continuity. The other choices do not align with how switches function in this scenario. Ignoring the frame would disrupt communications, generating an alert is typically not part of standard switch operations for such events, and disabling the port is an extreme measure that a switch generally does not take in these circumstances.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://ccna2switchingroutingwirelessessentialsv7.examzify.com

We wish you the very best on your exam journey. You've got this!