CISCO CERTIFIED NETWORK PROFESSIONAL PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://ccnp.examzify.com

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

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 a unique feature of Path Vector Protocols?

A. They are primarily used for LAN configurations

B. They are limited by the number of routers

C. They track hop count based on autonomous systems

D. They work only within a single administrative domain

2. What command is used to display a message of the day on a Cisco device?

A. banner motd

B. message of the day

C. motd banner

D. banner message

3. How long is the default timeout period before declaring a failed Active Virtual Forwarder (AVF) dead?

A. 600 seconds

B. 14,400 seconds

C. 30,000 seconds

D. 60,000 seconds

4. Which command is used to enable BPDU Guard globally?

A. spanning-tree portfast bpduguard default

B. spanning-tree guard loop

C. spanning-tree bpduguard enable

D. spanning-tree loopguard default

5. What command is used to configure trunk encapsulation to dot1q?

A. switchport trunk encapsulation ISL

B. switchport trunk encapsulation dot1q

C. trunk encapsulation dot1q

D. set trunk encapsulation dot1q

6. How does a switch flush MAC addresses from non-edge designated ports?

A. By rebooting the switch

B. By sending out a TC BPDU

C. By issuing a shutdown command

D. By clearing the MAC address table manually

7. In VRRP, what priority value is considered the default and highest for determining the master router?

A. 1

B. 100

C. 254

D. 255

8. Which of the following is a characteristic of NAT64 technology?

A. It requires static configurations

B. It can dynamically translate IPv6 to IPv4

C. It does not provide scalability

D. It operates only with Layer 3 protocols

9. What does the 'Protect' action do in port security?

A. Shuts down the port

B. Discards any violating traffic without counting

C. Keeps a violation count

D. Allows all traffic without restrictions

10. What action does a switch take when a port enters the errdisabled state?

A. Reboots the switch

B. Enables all ports

C. Shuts down the offending port

D. Resets all configurations

Answers

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

Explanations

1. What is a unique feature of Path Vector Protocols?

A. They are primarily used for LAN configurations

B. They are limited by the number of routers

C. They track hop count based on autonomous systems

D. They work only within a single administrative domain

Path Vector Protocols are designed to maintain the path information that gets updated dynamically as routing information changes. A unique feature of these protocols is their ability to track the paths taken by data packets based on autonomous systems. This means that rather than merely relying on hop counts between routers, Path Vector Protocols maintain a complete list of the autonomous systems (AS) through which a route passes. This is crucial for managing routing policies and preventing routing loops in inter-domain routing scenarios, as each AS can enforce its own policies and preferences. Understanding this path tracking is vital, especially in the context of the Border Gateway Protocol (BGP), which is the most well-known Path Vector Protocol. It helps in making routing decisions based on the entire path taken, rather than just the number of hops. This characteristic draws a clear line between Path Vector Protocols and other types of protocols, enhancing their effectiveness in large and complex network architectures where different administrative domains interact.

2. What command is used to display a message of the day on a Cisco device?

A. banner motd

B. message of the day

C. motd banner

D. banner message

The command used to display a message of the day on a Cisco device is "banner motd." This command is specifically designed to set up a message that will be shown to users when they connect to the device via console or remote access. The "motd" stands for "message of the day," and it allows network administrators to communicate important messages, warnings, or information to users. When executing the command, the administrator will follow it by specifying the text of the message, which can include various formats and delimiters to ensure the message is interpreted correctly by the system. This command is a fundamental aspect for management visibility and can enhance security by conveying essential information to users. Other terms like "message of the day" or "motd banner" might reference the function or concept but are not valid commands in the Cisco command line. Similarly, "banner message" does not correspond to the correct syntax recognized by Cisco's operating systems. Understanding the precise command structure is critical for effective configuration and management of Cisco devices.

3. How long is the default timeout period before declaring a failed Active Virtual Forwarder (AVF) dead?

A. 600 seconds

B. 14,400 seconds

C. 30,000 seconds

D. 60,000 seconds

The correct answer is based on the standard configuration for Active Virtual Forwarder (AVF) timeout periods in Cisco networking environments. The default timeout period for declaring a failed AVF as dead is indeed 14,400 seconds, which translates to 4 hours. This duration allows the network to maintain normal operations and reliability during transient failures while also ensuring that the forwarding roles can transition effectively if an AVF becomes unresponsive for a significant length of time. Understanding this value is essential for network engineers focusing on high availability and resilience. The extended timeout period helps to avoid unnecessary failover in cases where an AVF might briefly lose connectivity or experience a momentary disruption. A shorter timeout could lead to frequent failovers, causing instability and performance issues in the network. Therefore, the 14,400 seconds buffer is designed to balance responsiveness with system stability.

4. Which command is used to enable BPDU Guard globally?

A. spanning-tree portfast bpduguard default

B. spanning-tree guard loop

C. spanning-tree bpduguard enable

D. spanning-tree loopguard default

The command that enables BPDU Guard globally is "spanning-tree portfast bpduguard default." This command is crucial for enhancing the stability and security of a network by preventing Bridge Protocol Data Units (BPDUs) from being sent on ports configured with PortFast. When BPDU Guard is enabled, any port configured for PortFast that receives a BPDU will be placed into an error-disabled state, effectively protecting the network from potential loops and misconfigurations caused by erroneous or malicious devices connecting to these ports. This global setting provides a safeguard against scenarios where an end device may inadvertently send BPDUs, which can disrupt the normal operation of the Spanning Tree Protocol (STP). By utilizing this command, network administrators can enforce BPDU Guard on all relevant interfaces automatically, rather than managing each interface individually. The other commands listed serve different purposes, such as enabling loop guard or configuring BPDU guard on individual interfaces rather than globally. Understanding the specific uses and implications of these commands is essential in managing a secure and efficient network environment.

5. What command is used to configure trunk encapsulation to dot1q?

A. switchport trunk encapsulation ISL

B. switchport trunk encapsulation dot1q

C. trunk encapsulation dot1q

D. set trunk encapsulation dot1q

The command to configure trunk encapsulation to dot1q is accurately identified as "switchport trunk encapsulation dot1q." This command is part of the interface configuration mode in Cisco IOS, where you specify how the switch will identify and encapsulate VLAN traffic on trunk ports. Using dot1q (IEEE 802.1Q) is advantageous because it is a widely accepted standard for VLAN tagging, allowing multiple VLANs to be carried over a single physical link. When the appropriate command is entered, the switch recognizes the encapsulation method to use for traffic passing over the trunk link, enabling devices on different VLANs to communicate effectively. The other options either reference incorrect encapsulation methods or are not valid commands for configuring trunk encapsulation. For instance, the mention of ISL (Inter-Switch Link) is outdated as ISL is a Cisco proprietary encapsulation method that is not as commonly used today. Additionally, commands that do not use the correct syntax for configuring trunk encapsulation do not achieve the desired configuration. Thus, the choice that specifies "switchport trunk encapsulation dot1q" is the correct and effective command for setting up dot1q encapsulation on a trunk link.

6. How does a switch flush MAC addresses from non-edge designated ports?

A. By rebooting the switch

B. By sending out a TC BPDU

C. By issuing a shutdown command

D. By clearing the MAC address table manually

When a switch needs to flush MAC addresses from non-edge designated ports, it utilizes the concept of a Topology Change Notification (TCN) Bridge Protocol Data Unit (BPDU). This mechanism is part of the Spanning Tree Protocol (STP) operation, which helps maintain a loop-free topology in Ethernet networks. When a topology change occurs, such as a link failure or a port going up or down, the switch sends out a TC BPDU to notify all other switches in the network segment about this change. Upon receiving this notification, the other switches will perform an operation to update their MAC address tables. This typically involves flushing the MAC addresses learned on ports affected by the change, which effectively refreshes the network knowledge and corresponds to the updated topology. In contrast, rebooting the switch would clear the entire MAC address table, but it is not a selective flush associated with specific ports. Issuing a shutdown command on a port disables that port but does not actively manage the MAC address table related to non-edge ports. Clearing the MAC address table manually requires administrative action and does not automatically respond to topology changes, making it impractical for dynamic network environments.

7. In VRRP, what priority value is considered the default and highest for determining the master router?

A. 1

B. 100

C. 254

D. 255

In VRRP (Virtual Router Redundancy Protocol), the default priority value for determining the master router is indeed 100, but it's important to distinguish the different priority levels and their implications. The priority values range from 1 to 255, where the value 255 is the highest possible priority that can be assigned to a router. The router with the highest priority becomes the master router, which is responsible for forwarding packets for the virtual IP address managed by the VRRP group. While the default priority is set to 100, it can be adjusted, and higher configured values make a router more likely to take over as the master if there is a need for failover protection. Therefore, while the default is 100, the highest possible priority, which takes precedence in the election process, is actually 255. Understanding this hierarchy of values is crucial for network design, especially when configuring redundancy and failover mechanisms in a network environment where a VRRP is implemented.

8. Which of the following is a characteristic of NAT64 technology?

A. It requires static configurations

B. It can dynamically translate IPv6 to IPv4

C. It does not provide scalability

D. It operates only with Layer 3 protocols

NAT64 technology is designed to facilitate communication between IPv6 and IPv4 networks, primarily allowing IPv6-enabled clients to access IPv4 services seamlessly. The characteristic that it can dynamically translate IPv6 to IPv4 is central to its purpose. This dynamic translation enables IPv6-only devices to communicate with IPv4-only services without requiring extensive configurations or changes to existing infrastructure. This capability is especially critical in the context of transitioning to IPv6, as it allows for gradual migration strategies where both protocols can coexist, thereby ensuring continuity and accessibility of resources during the transition period. By leveraging DNS64, NAT64 can efficiently resolve IPv4 addresses and assist in the translation process dynamically, making it a flexible solution for dual-stack networks. Other characteristics mentioned in the options do not accurately reflect the functionality of NAT64; for example, it does not require static configurations and can easily handle various requests, promoting scalability. Additionally, while NAT64 operates primarily at the Layer 3 network layer to facilitate IP address translation, it is not limited solely to Layer 3, since transport layer protocols and others can also interact within the NAT64 framework.

9. What does the 'Protect' action do in port security?

A. Shuts down the port

B. Discards any violating traffic without counting

C. Keeps a violation count

D. Allows all traffic without restrictions

The 'Protect' action in port security is designed to enhance the security of a network by controlling access based on the MAC addresses of devices connected to the switch port. When the 'Protect' action is configured on a port, it effectively discards any traffic from devices that are not recognized or that violate the port security policy. Importantly, this action does not count the number of violations; it silently drops the unauthorized traffic without generating any notification or logs about the incident. This mechanism is particularly useful in environments where a low level of disruption is desired, as it helps maintain network integrity while reducing administrative overhead. By choosing to discard unauthorized traffic without creating a count of violations, administrators can prevent unwanted access without being inundated with alerts about every single infringement, allowing for a more streamlined approach to network security.

10. What action does a switch take when a port enters the errdisabled state?

A. Reboots the switch

B. Enables all ports

C. Shuts down the offending port

D. Resets all configurations

When a switch port enters the errdisabled state, it is a protective mechanism that indicates there is a problem detected on that port, such as a violation of network policies or protocol issues. In this state, the switch disables the affected port to prevent any further network disruptions or problems that could affect overall network performance. By shutting down the offending port, the switch is able to isolate the issue, allowing administrators to investigate and address the problem without impacting the rest of the network. Once the issue is resolved, network administrators can manually re-enable the port, restoring functionality. This action is an essential part of maintaining network stability, as it helps prevent misconfigurations or security violations from affecting other parts of the network.

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://ccnp.examzify.com

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