Cisco Certified Network Associate (CCNA) Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. For the full version with hundreds of questions, visit:
https://ciscoccna.examzify.com

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

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. **To configure OSPF on Frame Relay interfaces, how can you resolve the non-broadcast issue?**

   A. Use static OSPF neighbors.

   B. Use subnetting.

   C. Enable DHCP on the routers.

   D. Change the encapsulation to PPP.

2. **Which three protocols are considered the main components of the IPsec framework?**

   A. Internet Key Exchange (IKE), Secure Sockets Layer (SSL), Encapsulation Security Payload (ESP)

   B. Encryption Algorithm (EA), Authentication Header (AH), Internet Key Exchange (IKE)

   C. Encapsulation Security Payload (ESP), Authentication Header (AH), Internet Key Exchange (IKE)

   D. Authentication Header (AH), Secure Hash Algorithm (SHA), Internet Key Exchange (IKE)

3. **Which command is used to display access list information?**

   A. #show access-lists ACL NUMBER/NAME

   B. #find access-lists

   C. #display access-lists

   D. #list access-lists

4. **What command would a network administrator use to allow only one Telnet connection and encrypt the password?**

   A. (config)#service password-encryption

   B. (config)#line vty 0

   C. (config)#username USERNAME password PASSWORD

   D. (config-line)#login

5. **What command can be used to test if a configured serial link can forward packets?**

   A. test connection

   B. ping

   C. trace route

   D. check connectivity

6. What is the first command in the DHCP configuration process?

A. (config)#ip dhcp pool POOL NAME

B. (config-line)#login

C. (config)#interface INTERFACE_NAME

D. (config)#router rip

7. Which of the following best describes the function of the Spanning Tree Protocol?

A. To ensure fast data transmission in a network.

B. To prevent loops in network topology.

C. To manage VLAN configurations.

D. To enhance security of a network.

8. What is the primary use of IPsec in secure communications?

A. To encrypt data at rest

B. To provide traffic between two hosts or gateways

C. To backup data securely

D. To manage network load balancing

9. Which three features are added in SNMPv3 over SNMPv2?

A. Message Integrity

B. Compression

C. Authentication

D. Encryption

10. What transport layer protocol should be used to match SMTP traffic in an ACL?

A. UDP

B. TCP

C. ICMP

D. AH

Answers

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

Explanations

1. **To configure OSPF on Frame Relay interfaces, how can you resolve the non-broadcast issue?**

   A. Use static OSPF neighbors.

   B. Use subnetting.

   C. Enable DHCP on the routers.

   D. Change the encapsulation to PPP.

When configuring OSPF (Open Shortest Path First) on Frame Relay interfaces, the primary challenge arises from the non-broadcast characteristic of Frame Relay networks. Unlike broadcast-capable networks, where routers can automatically discover each other, non-broadcast networks require manual configuration of OSPF neighbors. Using static OSPF neighbors allows network administrators to explicitly define the routers that can communicate with each other through their specific Frame Relay addresses. This manual configuration is necessary in non-broadcast environments where OSPF cannot automatically establish adjacencies. By specifying the neighboring routers, OSPF can function effectively over Frame Relay links, ensuring that routing information is shared correctly between them. Other options are not suitable for resolving the non-broadcast issue. Subnetting relates to the division of IP address space into smaller segments but does not address the communication problem between routers on a non-broadcast medium. Enabling DHCP is primarily used for dynamically assigning IP addresses, which is unrelated to the OSPF neighbor discovery mechanism. Changing the encapsulation to PPP (Point-to-Point Protocol) might provide a solution since PPP does support dynamic discovery of neighbors, but it is not necessary when static OSPF neighbors can be defined. Thus, using static OSPF

2. **Which three protocols are considered the main components of the IPsec framework?**

   A. Internet Key Exchange (IKE), Secure Sockets Layer (SSL), Encapsulation Security Payload (ESP)

   B. Encryption Algorithm (EA), Authentication Header (AH), Internet Key Exchange (IKE)

   C. Encapsulation Security Payload (ESP), Authentication Header (AH), Internet Key Exchange (IKE)

   D. Authentication Header (AH), Secure Hash Algorithm (SHA), Internet Key Exchange (IKE)

The correct response identifies three key protocols that are integral to the IPsec framework. Encapsulation Security Payload (ESP) provides confidentiality, integrity, and authenticity for IP packets. It achieves this by encrypting the payload of the packets, ensuring that data cannot be intercepted and read by unauthorized parties. Additionally, it can provide authentication for the packets to verify their integrity. Authentication Header (AH) is another critical component, primarily focusing on providing message integrity and authenticity. It does this by creating a hash of the packet's header and payload, allowing the receiving device to verify that the packet has not been altered during transmission. Internet Key Exchange (IKE) plays a crucial role in the setup and management of security associations (SAs) between devices. It facilitates the negotiation of the cryptographic keys and the parameters required to establish a secure connection. The combination of these three protocols—ESP for confidentiality, AH for integrity, and IKE for key exchange—forms the foundation of the IPsec framework, enabling secure communication over potentially insecure networks like the Internet.

3. Which command is used to display access list information?

A. #show access-lists ACL NUMBER/NAME

B. #find access-lists

C. #display access-lists

D. #list access-lists

The command used to display access list information is indeed the one that begins with "show." In Cisco devices, the "show" command is integral for retrieving current operational data from the network device, including configuration settings and statistics. The specific syntax of "show access-lists ACL NUMBER/NAME" allows the user to target a specific access list by its identifier or name, which provides detailed information about the rules and conditions defined within that access list. This information can include permit and deny statements, source and destination addresses, and any associated network services, making it essential for troubleshooting and understanding network behavior. The other commands presented do not correctly reflect the syntax or functionality as per Cisco IOS conventions. The "find," "display," and "list" commands are not standard Cisco commands and would not provide the necessary information regarding access lists. Only the "show" command effectively communicates with the device's operating system to pull information about access lists. This reinforces the importance of recognizing command syntax and understanding how to gather configuration details on Cisco devices during network management and troubleshooting tasks.

4. What command would a network administrator use to allow only one Telnet connection and encrypt the password?

A. (config)#service password-encryption

B. (config)#line vty 0

C. (config)#username USERNAME password PASSWORD

D. (config-line)#login

The correct command to allow only one Telnet connection and ensure that the password is encrypted is related to the service password-encryption command. When this command is configured, it encrypts all plaintext passwords in the configuration file, thereby enhancing the security of the passwords used for accessing the device, including those for Telnet sessions. While the service password-encryption command secures passwords, managing Telnet connections is also critical. It is worth noting that to limit the number of concurrent Telnet connections, the network administrator would typically need to configure the terminal lines directly under-line vty settings and set appropriate limits. However, the command that directly contributes to password encryption—enhancing overall security—is indeed the service password-encryption command.   In this context, while options related to line configuration or user authentication are relevant to session management, they do not specifically pertain to encrypting passwords alone, nor do they focus solely on limiting Telnet connections. The intention of the question is geared towards encryption, making the first command the most appropriate choice.

5. What command can be used to test if a configured serial link can forward packets?

A. test connection

B. ping

C. trace route

D. check connectivity

The command that is used to test if a configured serial link can forward packets is "ping." This command sends Internet Control Message Protocol (ICMP) echo request messages to the target host, and if the serial link is operational and configured correctly, the target will send back an echo reply. This is a basic yet effective way to verify that the network path is functional and that the packets can reach their destination. Using ping provides valuable feedback on packet loss, latency, and the accessibility of the serial link or device in question. When you ping an IP address associated with a serial connection, it helps ensure that the connection is capable of transmitting data, confirming the link is not only established but also fully operational for packet forwarding. The other options do not directly accomplish this specific task. For instance, "test connection" and "check connectivity" are not standard commands found in Cisco IOS. The "traceroute" command allows you to see the path packets take to a destination and can indicate where failures occur, but it is not a straightforward test of whether a specific link can forward packets.

6. What is the first command in the DHCP configuration process?

A. (config)#ip dhcp pool POOL NAME

B. (config-line)#login

C. (config)#interface INTERFACE_NAME

D. (config)#router rip

The command to initiate the DHCP configuration process is to define a DHCP pool, which is accomplished with the command that specifies the pool name. When you start configuring DHCP on a Cisco router, this is the very first step; it tells the router to create a pool of IP addresses that will be available for client devices on the network. This command essentially lays the groundwork for all subsequent DHCP configurations, such as defining the range of IP addresses, lease times, and additional options. The other choices pertain to different configuration contexts and are not relevant to starting the DHCP process. For example, configuring an interface is important for interface settings but not for setting up DHCP. Similarly, the command related to RIP (Routing Information Protocol) is focused on routing rather than DHCP configuration. Therefore, defining the DHCP pool is the necessary first step to establish DHCP services within a network setup.

7. Which of the following best describes the function of the Spanning Tree Protocol?

A. To ensure fast data transmission in a network.

B. To prevent loops in network topology.

C. To manage VLAN configurations.

D. To enhance security of a network.

The function of the Spanning Tree Protocol (STP) is primarily to prevent loops in network topology. In a network with switches, loops can form when there are multiple pathways between devices, potentially causing broadcast storms and overwhelming the network. STP helps by identifying and disabling redundant links, thus preventing these loops while still allowing for redundancy where necessary. This ensures a stable and efficient network topology. While ensuring fast data transmission, managing VLAN configurations, and enhancing security are important aspects of network management, they are not the primary functions of STP. Instead, STP specifically addresses the problem of network loops, which is crucial for maintaining network stability and performance.

8. What is the primary use of IPsec in secure communications?

A. To encrypt data at rest

B. To provide traffic between two hosts or gateways

C. To backup data securely

D. To manage network load balancing

The primary use of IPsec in secure communications involves providing protection for traffic between two hosts or gateways. IPsec is a suite of protocols that operates at the network layer and is designed to secure Internet Protocol communications by authenticating and encrypting each IP packet in a communication session. When data is transmitted over the Internet or any network, it can be vulnerable to interception and tampering. With IPsec, two endpoints—commonly routers or firewalls—can establish a secure tunnel that ensures that all data sent across this tunnel is encrypted, maintaining confidentiality, authenticity, and integrity. This is crucial for applications such as Virtual Private Networks (VPNs), where users need secure access to a remote network. The other options do not accurately reflect the primary role of IPsec. For example, while options discussing data encryption at rest, backup security, or network load balancing are important concepts in a broader security and networking context, they do not pertain specifically to the function that IPsec is designed to serve. IPsec's main focus is clearly on securing traffic in transit between two network nodes, which makes it vital for establishing secure communication channels over potentially insecure networks.

9. Which three features are added in SNMPv3 over SNMPv2?

A. Message Integrity

B. Compression

C. Authentication

D. Encryption

The correct answer highlights key enhancements introduced in SNMPv3 that provide significant improvements in security and management capabilities compared to its predecessor, SNMPv2. Message integrity ensures that the messages sent between the SNMP manager and agents have not been altered in transit. This feature helps prevent unauthorized modifications to SNMP messages, thereby fostering trust in the integrity of the management data. Authentication is crucial in SNMPv3 as it verifies the identity of the entities communicating over the network. This prevents unauthorized users from accessing or manipulating network management data, ensuring that only legitimate components can send or receive SNMP messages. Encryption is another important enhancement found in SNMPv3, which provides confidentiality by encrypting the messages exchanged between network devices. This helps protect sensitive information from eavesdropping or interception by unauthorized parties, making it difficult for attackers to gain insight into network management activities. While compression is a feature that could theoretically be desirable, it is not a part of the security enhancements specifically included in SNMPv3. Therefore, the focus remains on the core attributes of message integrity, authentication, and encryption as transformative features that cater to the evolved security landscape in network management.

10. What transport layer protocol should be used to match SMTP traffic in an ACL?

A. UDP

B. TCP

C. ICMP

D. AH

The correct choice is TCP because the Simple Mail Transfer Protocol (SMTP) operates over the Transmission Control Protocol (TCP). SMTP is responsible for sending and receiving emails, and it typically uses TCP port 25 for its communication.   TCP is a connection-oriented protocol, which means it establishes a reliable connection between the sender and receiver before data can be transmitted. This reliability is crucial for email communication, where packet loss could mean that email messages do not arrive correctly or at all. In contrast, the other protocols listed serve different purposes. UDP (User Datagram Protocol) is connectionless and is typically used for applications where speed is more critical than reliability, such as video streaming or online gaming, making it unsuitable for matching SMTP traffic. ICMP (Internet Control Message Protocol) is used primarily for diagnostic and control purposes, such as ping operations, rather than for data transmission like email. AH (Authentication Header) is an extension of the IP protocol for providing authentication and integrity but does not specifically deal with the transport of data such as SMTP does.   Thus, for configuring an Access Control List (ACL) to match SMTP traffic, TCP is the appropriate protocol to specify.

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://ciscoccna.examzify.com

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