CISCO CERTIFIED INTERNETWORK EXPERT (CCIE) PRACTICE TEST (SAMPLE)

STUDY GUIDE

Prepare with structure. Pass with confidence

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. **Which three statements about RLDP are true?**

   A. It detects rogue access points that are connected to the wired network

   B. It can detect rogue APs that use WPA encryption

   C. Active Rogue containment can be initiated manually against rogue devices detected on the wired network

   D. The AP is unable to serve clients while the RLDP process is active

2. **Which of these capabilities highlights the difference between user-based policies and traditional network security?**

   A. Policies based on network device location

   B. Policies based on individual user identity

   C. Static user access controls

   D. Generalized security measures

3. **Which Cisco ISE profiler service probe can collect information about Cisco Discovery Protocol?**

   A. SNMP Query

   B. DHCP SPAN

   C. DHCP

   D. HTTP

4. **What are two effects of the given configuration on a Cisco ASA regarding botnet filtering? (Choose two)**

   A. It enables botnet filtering in multiple context mode

   B. It enables botnet filtering in single context mode

   C. It enables the ASA to download the static botnet filter database

   D. It enables the ASA to download the dynamic botnet filter database

5. **Which three commands can you use to configure VXLAN on a Cisco ASA firewall?**

   A. default-mcast-group

   B. set ip next-hop verify-availiability

   C. segment-id

   D. inspect vxlan

6. What is one primary benefit of network summarization?

A. It increases individual subnet size

B. It enhances the detail of routing tables

C. It prevents unnecessary routing updates

D. It allows for automatic IP address assignment

7. What ensures the integrity of data packets in RADIUS communications?

A. Length

B. Authenticator

C. Message-Integrity-Check

D. Type of Service

8. Which two statements about the device configuration are true?

A. The device retains all existing SGT mapping entries for 3 minutes

B. If a peer reconnects to the device within 120 seconds of terminating a CTS-SXP connection, the reconciliation timer starts

C. It sets the internal hold-down timer of the device to 3 minutes

D. If a peer reconnects to the device within 180 seconds of terminating a CTS-SXP connection, the reconciliation timer starts

9. Which two statements about MAB are true? (Choose two)

A. MAC addresses stored in the MAB database can be spoofed

B. It operates at Layer 2 and Layer 3 of the OSI protocol stack

C. It can be used to authenticate network devices and users

D. It serves at the primary authentication mechanism when deployed in conjunction with 802.1x

10. Which statement regarding the match certificate command is accurate?

A. It requires the router clock to be set to function

B. It does not consider date validity of certificates

C. It is executed without checking the peer's certificate

D. It is always effective, regardless of router settings

Answers

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

Explanations

1. Which three statements about RLDP are true?

A. It detects rogue access points that are connected to the wired network

B. It can detect rogue APs that use WPA encryption

C. Active Rogue containment can be initiated manually against rogue devices detected on the wired network

D. The AP is unable to serve clients while the RLDP process is active

Rogue Laptop Detection Protocol (RLDP) is a mechanism designed to enhance the security of wireless networks by identifying unauthorized or rogue access points that connect to the wired network. One of the primary functions of RLDP is to detect rogue access points, which helps in maintaining the integrity and security of the network. This capability makes it essential for network administrators to have a clearer view of what devices are connected to their network, thereby preventing potential security breaches. The statement about RLDP detecting rogue access points connected to the wired network aligns directly with the protocol's purpose. By identifying these unauthorized devices, RLDP helps protect the network from threats that could arise from foreign or unmonitored access points. Furthermore, the ability to identify and track rogue devices allows for a more proactive approach to network security management. In terms of the other statements, while RLDP does provide a mechanism for rogue AP detection, not all encryption types or configurations are captured uniformly across different implementations. Consequently, stating that RLDP can detect rogue APs using WPA encryption may not fully encompass the protocol's intended functionality, especially in varied environments. Active rogue containment being initiated manually signifies an action that can be taken after a rogue is detected, rather than an inherent property of the RLDP process itself.

2. Which of these capabilities highlights the difference between user-based policies and traditional network security?

A. Policies based on network device location

B. Policies based on individual user identity

C. Static user access controls

D. Generalized security measures

User-based policies focus on the identity of the individual user, which differentiates them significantly from traditional network security approaches. Traditional security often centers around the location and configuration of network devices, applying broad measures to parts of the network without considerating who is accessing it. In contrast, user-based policies allow for granular security measures that adapt based on the specific user's role, behavior, and access needs. This personalized approach enhances security by ensuring that users only have access to resources necessary for their work, thereby reducing the potential for unauthorized access or data breaches. This capability is crucial in modern security frameworks that prioritize identity and access management, reflecting a shift towards more dynamic security practices tailored to individual needs rather than static, device-centric controls.

3. Which Cisco ISE profiler service probe can collect information about Cisco Discovery Protocol?

A. SNMP Query

B. DHCP SPAN

C. DHCP

D. HTTP

The Cisco ISE profiler service probe that can collect information about Cisco Discovery Protocol (CDP) is SNMP Query. CDP is a Layer 2 protocol used to share information about network devices. The SNMP (Simple Network Management Protocol) Query can be utilized to request this specific information from the devices in the network, as CDP runs on Cisco devices, and their information can be extracted via SNMP traffic. The SNMP Query sends requests to devices to gather various operational data, including the CDP information that shows how devices connect with one another. Other options, while relevant in different contexts, do not specifically collect CDP information. For instance, DHCP (Dynamic Host Configuration Protocol) primarily deals with IP address assignment and does not inherently provide details related to CDP. The DHCP SPAN (Switched Port Analyzer) is useful for monitoring traffic, but it won't directly facilitate CDP information gathering. HTTP is a protocol for transferring data over the web and is not utilized for collecting device-specific network protocols such as CDP. Hence, the use of the SNMP Query is most appropriate for this particular task within the context of profiling network devices and understanding their interconnectivity through CDP.

4. What are two effects of the given configuration on a Cisco ASA regarding botnet filtering? (Choose two)

A. It enables botnet filtering in multiple context mode

B. It enables botnet filtering in single context mode

C. It enables the ASA to download the static botnet filter database

D. It enables the ASA to download the dynamic botnet filter database

The effect of enabling botnet filtering in multiple context mode on a Cisco ASA is that it allows the device to apply botnet filtering across different security contexts, effectively managing and monitoring traffic for multiple virtual firewalls within a single physical appliance. This capability enhances security by permitting the ASA to identify and block traffic that is attempting to communicate with known botnet servers, protecting all contexts individually without needing separate configurations for each one. While the claim that it enables botnet filtering in multiple context mode is a valid outcome of the configuration, botnet filtering is also available in single context mode, where the entire device operates as a single firewall with no separate contexts, simplifying management in smaller environments or simpler configurations. Thus, both single and multiple context configurations can support botnet filtering, making the choice of enabling this feature in a single context mode equally plausible. The ability to download the static or dynamic botnet filter databases directly relates to the ASA's capacity to update its knowledge base for improved effectiveness in identifying threats. However, unless the configuration clearly indicates that it pertains to either static or dynamic databases, this aspect should be examined separately from the context in which the ASA operates. The dynamic database allows for more immediate updates and responses to emerging threats, while static databases rely on periodic

5. Which three commands can you use to configure VXLAN on a Cisco ASA firewall?

A. default-mcast-group

B. set ip next-hop verify-availiability

C. segment-id

D. inspect vxlan

To configure VXLAN (Virtual Extensible LAN) on a Cisco ASA firewall, one effective command is the default-mcast-group. This command is essential because it allows you to specify the multicast group address used for VXLAN traffic, which plays a crucial role in the encapsulation and transmission of the Layer 2 Ethernet frames over Layer 3 networks. By defining a default multicast group, you ensure that all VXLAN segments can correctly address and send their traffic, which is foundational to the functionality of VXLAN. Using multicast for VXLAN is significant as it allows for efficient replication of broadcast, unknown unicast, and multicast traffic within a VXLAN segment without overwhelming the network. Proper configuration of the multicast group is critical for establishing the desired communication patterns between endpoints in different VXLAN segments. In addition to the default-mcast-group, other commands like segment-id help in identifying the specific VXLAN segment (often referred to as a Virtual Network Identifier, or VNI), and the inspect vxlan command is used for traffic inspection. However, the choice of default-mcast-group directly relates to configuring multicast requirements, making it a primary command for setting up VXLAN functionality on the Cisco ASA firewall.

6. What is one primary benefit of network summarization?

A. It increases individual subnet size

B. It enhances the detail of routing tables

C. It prevents unnecessary routing updates

D. It allows for automatic IP address assignment

Network summarization is a technique employed in routing to combine multiple contiguous subnets into a single summarized route. This approach primarily contributes to the efficiency of the routing process by reducing the number of routes a router has to maintain and advertise. One of the primary benefits of network summarization is that it minimizes the amount of routing information shared across a network. By summarizing routes, routers can prevent unnecessary routing updates. When a summarized route is announced, it includes the information for all the underlying subnets, which means that less detailed information needs to be sent across the network. This leads to decreased network congestion and reduced strain on router resources, as fewer individual routing entries need to be managed and processed. While other choices may discuss aspects of networking, they do not capture this critical function of network summarization in the way that preventing unnecessary routing updates does. For instance, increasing individual subnet sizes or enhancing the detail of routing tables is contrary to the purpose of summarization, which is to simplify and consolidate routing information. Additionally, while automatic IP address assignment is an important networking concept, it does not relate directly to the benefits of summarization. Thus, the primary benefit lies in reducing the complexity and overhead of routing updates through effective summarization.

7. What ensures the integrity of data packets in RADIUS communications?

A. Length

B. Authenticator

C. Message-Integrity-Check

D. Type of Service

In RADIUS (Remote Authentication Dial-In User Service) communications, the integrity of data packets is ensured by the use of an authenticator. The authenticator serves as a unique value that is calculated based on the content of the message, the secret shared between the client and server, and a timestamp. This means that if any part of the packet is altered during transmission, the authenticator will not match when it reaches its destination, indicating that the packet has been tampered with. This mechanism effectively protects against certain attacks, such as packet sniffing and replay attacks, by providing a way to confirm that the message came from a legitimate source and has not been altered in transit. The importance of the authenticator in ensuring data integrity makes it a critical element in RADIUS communications. The other choices do not specifically guarantee the integrity of the packets in the context of RADIUS. While the length might help in defining the packet structure, it does not ensure integrity. Message-Integrity-Check (MIC) is a term associated with different protocols, like EAP (Extensible Authentication Protocol), rather than RADIUS itself. Type of Service is related to the prioritization of traffic over a network rather than the integrity of the communication. Thus, the use

8. Which two statements about the device configuration are true?

A. The device retains all existing SGT mapping entries for 3 minutes

B. If a peer reconnects to the device within 120 seconds of terminating a CTS-SXP connection, the reconciliation timer starts

C. It sets the internal hold-down timer of the device to 3 minutes

D. If a peer reconnects to the device within 180 seconds of terminating a CTS-SXP connection, the reconciliation timer starts

The statement regarding the reconciliation timer starting when a peer reconnects to the device within 120 seconds of terminating a Context-based Access Control Security Exchange Protocol (CTS-SXP) connection is correct because it aligns with the operational parameters of CTS-SXP sessions. In this context, the reconciliation timer is designed to streamline the process of re-establishing connections and ensuring that security group tag (SGT) mappings are maintained efficiently. When a peer reconnects within this specific time frame, the device relies on the stale mapping entries, allowing for a quicker re-establishment of those security relationships without needing to perform a full mapping from scratch. In contrast, other statements pertain to either incorrect timing or misunderstandings about the holding patterns of SGT mappings. Retaining entries for a specified period or adjusting internal timers not congruent with established protocols misses the exact timing definition and operational behavior outlined by CTS-SXP standards, which are critical for maintaining effective network security in environments utilizing security group tagging.

9. Which two statements about MAB are true? (Choose two)

A. MAC addresses stored in the MAB database can be spoofed

B. It operates at Layer 2 and Layer 3 of the OSI protocol stack

C. It can be used to authenticate network devices and users

D. It serves at the primary authentication mechanism when deployed in conjunction with 802.1x

MAB, or Mac Authentication Bypass, is primarily used for authenticating devices based on their MAC addresses when they are unable to perform 802.1x authentication. One critical aspect of MAB is that MAC addresses stored in its database can be spoofed by malicious users. This vulnerability arises because an attacker can adopt the MAC address of a legitimate device, thereby gaining unauthorized access to the network. Hence, the statement regarding the potential for MAC address spoofing is correct. Additionally, MAB can indeed authenticate network devices and users. It serves as an alternative authentication method that allows non-802.1x capable devices, like printers or cameras, to access the network based solely on their MAC addresses. This means that MAB is capable of authenticating devices in situations where more sophisticated methods are not applicable, emphasizing its utility in diverse network environments. While it is true that MAB operates primarily at Layer 2 of the OSI model, its focus does not extend effectively into Layer 3; rather, it is a simpler process that mainly relies on MAC addresses rather than integrating deeper into the TCP/IP stack for authentication. Furthermore, although MAB can theoretically be utilized alongside 802.1x, it does not serve as the primary mechanism when

10. Which statement regarding the match certificate command is accurate?

A. It requires the router clock to be set to function

B. It does not consider date validity of certificates

C. It is executed without checking the peer's certificate

D. It is always effective, regardless of router settings

The statement that the match certificate command requires the router clock to be set to function is accurate because the command is contingent on the validation processes that depend on the system clock. The functionality of many authentication protocols, including those that employ certificates, often involves time-sensitive aspects to ensure that a certificate is valid during its period of effectiveness. If the router's clock is not correctly set, it can lead to misinterpretations of the validity of the certificates, potentially allowing expired or otherwise invalid certificates to pass validation, or rejecting valid certificates because the system believes they are not within the valid date range. In contrast, options that state the command does not consider date validity of certificates or is executed without checking the peer's certificate miss the mark. The command's primary purpose is to match and validate certificates effectively, which inherently includes verifying date validity and examining peer certificates. Finally, suggesting that the command is always effective regardless of router settings misrepresents the operational dependencies, as various settings or configurations can significantly impact the implementation and effectiveness of certificate-related commands.

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://cisco-internetwork.examzify.com

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