Cisco Certified Internetwork Expert (CCIE) 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 identifies a packet as part of a specific multicast address in IPv6?**

   A. The Icmpv6.type value

   B. The source address within the network

   C. The destination IPv6 multicast address

   D. The TCP or UDP port number in the header

2. **Which statement about the Cisco ASA Identity Firewall is true?**

   A. It identifies threats solely based on IP address

   B. It can apply security policies on individual user or user-group basis

   C. It operates only on the application layer

   D. It requires constant updates from the Internet to function

3. **Which filters might be useful in WireShark for troubleshooting IPv6 address assignment?**

   A. Icmpv6.type== 135

   B. Icmpv6.type== 136

   C. Icmpv6.type== 137

   D. Icmpv6.type== 138

4. **In which instance is MAB considered effective?**

   A. When devices do not support 802.1x

   B. Only in wireless networks

   C. When both Layer 2 and Layer 3 are compromised

   D. For devices under heavy load

5. **Which protocol does 802.1X use between the supplicant and the authenticator to authenticate users?**

   A. SNMP

   B. TACACS+

   C. RADIUS

   D. EAP over LAN

6. Which two statements about SPAN sessions are true? (Choose two)

A. A single switch stack can support up to 32 source and RSPAN destination sessions

B. They can monitor sent and received packets in the same session

C. Multiple SPAN sessions can use the same destination port

D. Source ports and source VLANS can be mixed in the same session

7. Which two features help mitigate man-in-the-middle attacks?

A. ARP spoofing

B. ARP sniffing on specific ports

C. DHCP snooping

D. Dynamic ARP inspection

8. What is a key feature of an access point in local mode with wIPS?

A. Detects and logs user activity in real-time

B. Supports enhanced detection of attacks by scanning radio channels for extended periods

C. Connects automatically to the most secure AP available

D. Manages network traffic independently

9. Which two statements about Cisco VSG are true?

A. It uses optional IP-to-virtual machine mappings to simplify management of virtual machines

B. It has built-in intelligence for redirecting traffic and fast-path offload.

C. It can be integrated with VMWare vCenter to provide transparent provisioning of policies and profiles.

D. It uses the Cisco VSG user agent to register with the Cisco Prime Network Services Controller

10. Which two statements are true about the TTL value in an IPv4 header?

A. Its maximum value is 255

B. It is a 4-bit value

C. It can be used for traceroute operations

D. When it reaches 0, it generates an ICMP Type 11 message

Answers

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

Explanations

1. What identifies a packet as part of a specific multicast address in IPv6?

A. The Icmpv6.type value

B. The source address within the network

C. The destination IPv6 multicast address

D. The TCP or UDP port number in the header

In IPv6, packets that are part of a multicast group are identified by their destination IPv6 multicast address. This multicast address is a specific range of addresses designated for groups of devices rather than a single device, allowing efficient data distribution to multiple recipients simultaneously. When an IPv6 packet is sent to a multicast address, it is intended for all members of that multicast group. The unique structure of the multicast address in the IPv6 address space, which begins with the prefix ff00::/8, helps routers and switches know that this packet should be transmitted to multiple interfaces rather than just one. This is key for applications like streaming media or group communication services where the same data needs to be sent to multiple hosts. While other components, such as the ICMPv6 type value, source addresses, and transport layer port numbers, play a role in how packets are processed or routed, they do not serve the specific function of identifying the group of destination devices that the multicast packet is meant for. Therefore, recognizing the destination IPv6 multicast address is critical for handling multicast communication effectively in an IPv6 network.

2. Which statement about the Cisco ASA Identity Firewall is true?

A. It identifies threats solely based on IP address

B. It can apply security policies on individual user or user-group basis

C. It operates only on the application layer

D. It requires constant updates from the Internet to function

The statement regarding the Cisco ASA Identity Firewall being able to apply security policies on an individual user or user-group basis is accurate. This feature showcases the Identity Firewall's capability to enforce specific security rules that are tailored to user profiles, roles, or access levels within an organization. By using identity information, such as Active Directory or RADIUS credentials, the ASA can effectively differentiate between users and apply policies that reflect their unique needs or positions. This functionality enhances network security by ensuring that users only have access to the resources they require, ultimately minimizing risk. In contrast, identifying threats solely based on IP addresses lacks the granularity needed for modern security measures, as it does not consider the identity of users behind those addresses. Operating only on the application layer would limit the firewall's functionality since it interacts across various layers to enforce security. Lastly, the claim about requiring constant updates from the Internet does not reflect its operational design, as while the ASA does benefit from updates for improved security and features, its core identity management capabilities do not rely on continuous Internet connectivity to enforce policies effectively.

3. Which filters might be useful in WireShark for troubleshooting IPv6 address assignment?

A. Icmpv6.type== 135

B. Icmpv6.type== 136

C. Icmpv6.type== 137

D. Icmpv6.type== 138

The filter that highlights ICMPv6 type 136 is useful for troubleshooting IPv6 address assignment as it corresponds to Router Advertisement (RA) messages. These messages are essential in the Stateless Address Autoconfiguration (SLAAC) process, which enables devices to automatically configure their IPv6 addresses. When a device connects to a network, it listens for Router Advertisements from neighboring routers. These advertisements convey important information such as the network prefix and various configuration settings needed for the device to generate its own IPv6 address. By applying this filter in Wireshark, you can observe the Router Advertisements being sent on the network and verify whether the proper configuration is taking place or if there are issues affecting the address assignment process. The other ICMPv6 message types, while significant in the IPv6 protocol suite, relate to different aspects of the protocol. Type 135 is related to Neighbor Solicitation, which is used to discover other nodes on the link and resolve their link-layer addresses. Type 137 corresponds to the Node Information Query, while type 138 deals with Node Information Response messages. Though useful for broader troubleshooting, these are less directly related to the address assignment problem being investigated.

4. In which instance is MAB considered effective?

A. When devices do not support 802.1x

B. Only in wireless networks

C. When both Layer 2 and Layer 3 are compromised

D. For devices under heavy load

MAB, or MAC Authentication Bypass, is particularly effective when devices do not support 802.1X authentication. This scenario is common in situations involving legacy devices such as printers, IP phones, and some IoT devices that lack the capability to participate in 802.1X protocols. In these cases, MAB allows for the identification and authentication of devices based on their MAC addresses, enabling network access without requiring the device to support the more sophisticated authentication methods like 802.1X. The implementation of MAB provides a way to still secure the network while accommodating devices that may not have the necessary functionality for traditional authentication methods. By ensuring that authorized MAC addresses are permitted access, MAB can help maintain a level of security on the network, even when full 802.1X capabilities are not present. In contrast, the other scenarios do not align with the primary function or effectiveness of MAB. For example, MAB is not limited to wireless networks; it is applicable in wired scenarios as well. Additionally, addressing security breaches at Layer 2 and Layer 3 requires broader measures beyond what MAB offers, and heavy load conditions on devices are not a factor that enhances the effectiveness of MAC Authentication Bypass.

5. Which protocol does 802.1X use between the supplicant and the authenticator to authenticate users?

A. SNMP

B. TACACS+

C. RADIUS

D. EAP over LAN

802.1X is a network access control protocol that is widely used to provide a framework for authenticating devices and users wishing to connect to a network. The protocol establishes an authentication mechanism using a client (the supplicant), a network device (the authenticator), and an authentication server. In this context, EAP (Extensible Authentication Protocol) plays a crucial role. Specifically, EAP enables the authentication process to be encapsulated within 802.1X frames, allowing various authentication methods to be used seamlessly. The specific variant of EAP used in this layer is often referred to as EAP over LAN (EAPOL). This method allows the client to communicate directly with the authenticator to exchange authentication information. By utilizing EAP over LAN, the process provides a flexible and efficient way to authenticate users in a network, ensuring that only authorized devices and users gain access. The other protocols mentioned, while significant in different contexts, do not serve the same purpose in the 802.1X authentication process as EAP does. For instance, while RADIUS can be used as an authentication server, the core communication mechanism between the supplicant and authenticator specifically utilizes EAPOL frames to facilitate the authentication dialogue.

6. Which two statements about SPAN sessions are true? (Choose two)

A. A single switch stack can support up to 32 source and RSPAN destination sessions

B. They can monitor sent and received packets in the same session

C. Multiple SPAN sessions can use the same destination port

D. Source ports and source VLANS can be mixed in the same session

The statement about monitoring sent and received packets in the same session is true because a SPAN (Switched Port Analyzer) session can indeed be configured to capture traffic in both directions from a source port. This capability is crucial for comprehensive network traffic analysis, as it allows network administrators to monitor not just outbound traffic but inbound traffic as well, providing a complete view of the traffic patterns on that port. In addition to this statement, the option regarding the mixing of source ports and source VLANs in the same SPAN session is also true. SPAN sessions are versatile enough to aggregate traffic from multiple source ports and to monitor traffic from different VLANs simultaneously. This allows a network engineer to analyze a diverse range of traffic and troubleshoot issues more effectively. The other alternatives do not align with the functionalities of SPAN sessions as well. For instance, while multiple SPAN sessions can indeed use the same destination port, each SPAN session itself must be carefully managed to avoid any potential traffic contention that could lead to packet loss or improper monitoring. The architecture generally prefers to have unique dedicated destination ports for clearer analysis.

7. Which two features help mitigate man-in-the-middle attacks?

A. ARP spoofing

B. ARP sniffing on specific ports

C. DHCP snooping

D. Dynamic ARP inspection

Dynamic ARP Inspection (DAI) plays a crucial role in mitigating man-in-the-middle attacks by preventing the manipulation of ARP (Address Resolution Protocol) messages in a network. ARP is used to map IP addresses to MAC addresses, and attackers can exploit this by sending fraudulent ARP messages, redirecting traffic to their devices and thereby intercepting or modifying communication. DAI works by ensuring that only trusted ARP packets are allowed through the switch's ports, thus validating ARP requests and replies against a trusted database, often populated by DHCP Snooping. While it is indeed true that DHCP Snooping itself helps secure the network by ensuring that only authorized DHCP servers can distribute IP addresses, it's the combination of DHCP Snooping with Dynamic ARP Inspection that robustly reinforces the network against potential man-in-the-middle threats. DHCP Snooping essentially ensures the integrity of the IP address assignment, and when used with DAI, it ties ARP mappings to legitimate IP-to-MAC bindings, substantially reducing the risk of ARP spoofing. Opposing options, such as ARP spoofing and ARP sniffing, do not offer protective measures; instead, they are techniques used in attacks. Thus, they do not contribute to network security against man

8. What is a key feature of an access point in local mode with wIPS?

A. Detects and logs user activity in real-time

B. Supports enhanced detection of attacks by scanning radio channels for extended periods

C. Connects automatically to the most secure AP available

D. Manages network traffic independently

The key feature of an access point in local mode with wireless Intrusion Prevention System (wIPS) revolves around its capability to enhance security through extended scanning of radio channels. This advanced feature allows the access point to monitor for unauthorized access points, rogue devices, and wireless attacks over a prolonged period. By performing comprehensive scans, it can identify and respond to potential threats effectively, ensuring a more robust security posture for the network. This characteristic of extended detection is crucial for maintaining the integrity of wireless networks, as it helps in preemptive identification and mitigation of malicious activities. Such a secure monitoring method is essential in environments where security is a paramount concern, helping to safeguard sensitive data and maintain compliance with various standards. The other options reflect functionalities that, while important, do not accurately capture the essence of wIPS in local mode. Activities like securing connections or managing traffic do not define the core role of wIPS, which is primarily focused on maintaining a vigilant security posture through ongoing environmental assessments.

9. Which two statements about Cisco VSG are true?

A. It uses optional IP-to-virtual machine mappings to simplify management of virtual machines

B. It has built-in intelligence for redirecting traffic and fast-path offload.

C. It can be integrated with VMWare vCenter to provide transparent provisioning of policies and profiles.

D. It uses the Cisco VSG user agent to register with the Cisco Prime Network Services Controller

The correct choice highlights the integration capabilities of Cisco VSG with VMWare vCenter, which is essential for enhancing virtualization management. By integrating with vCenter, Cisco VSG allows for the seamless provisioning of security policies and profiles, which aligns with the operational needs of virtual environments. This integration enables network policies to be applied transparently as virtual machines are provisioned and moved, thereby improving security without manual reconfiguration. This aspect is crucial because in virtualized environments, managing security policies consistently across dynamically changing resources can be challenging. Cisco VSG's ability to work alongside vCenter helps automate and streamline this process, allowing organizations to maintain robust security postures without adding significant operational overhead. The focus on integration, especially in environments using VMware technologies, demonstrates the value Cisco VSG brings to the virtualization landscape, enabling organizations to enforce security measures that scale alongside their virtual workloads seamlessly. This approach enhances operational efficiency and security management in the context of rapidly changing virtual infrastructures.

10. Which two statements are true about the TTL value in an IPv4 header?

A. Its maximum value is 255

B. It is a 4-bit value

C. It can be used for traceroute operations

D. When it reaches 0, it generates an ICMP Type 11 message

The statement that the Time to Live (TTL) value in an IPv4 header can be used for traceroute operations is accurate. In the case of the traceroute utility, each packet is sent with a TTL value that is incremented with each successive packet. This process allows the packets to be routed through a sequence of network devices (routers), and each router decrements the TTL by one. When the TTL reaches zero, the router drops the packet and sends back an ICMP Type 11 message to the source. This message indicates that the TTL has expired and provides the source with the IP address of the router that dropped the packet. This mechanism allows the traceroute command to map out the path packets take to a destination IP, revealing each hop along the way. The other statements about the TTL value do not hold true. The maximum value of TTL is indeed 255, but it is important to note that TTL is actually an 8-bit field within the IPv4 header. Therefore, while there can be confusion regarding its bit size and operations, the correct understanding of TTL is critical for network diagnostics and understanding routing behaviors.

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!