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. Don’t worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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 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

2. **What impact does TACACS+ have regarding console port access?**

   A. Local database is the sole authentication method

   B. Authentication is managed through the TACACS+ server

   C. Only level 15 users can access the console

   D. It disables all other authentication methods

3. **Which two statements about 802.1x components are true? (Choose two)**

   A. The certificates used in the client-server authentication process are stored on the access switch

   B. The access layer switch is the policy enforcement point

   C. The RADIUS server is the policy enforcement point

   D. The RADIUS server is the policy information point

4. **Which statement regarding routing functions of Cisco ASA running software version 9.2 is true?**

   A. The ASA supports policy-based routing with route maps

   B. In a failover pair of ASAs, the standby firewall establishes a peer relationship with OSPF neighbors

   C. The translation table cannot override the routing table for new connections

   D. Routes to the Null0 interface cannot be configured to black-hole traffic

5. **Which setting determines the prefix address of a 6to4 tunnel?**

   A. Static configuration set in the router.

   B. The IPv6 configuration to the interface.

   C. The DHCP server settings.

   D. The address of the terminating node.

6. Which feature does Cisco VSG utilize to redirect traffic on Cisco Nexus 1000V Series Switch?

A. VPC

B. VDC

C. VEM

D. vPath

7. 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

8. What does IGMPv2 allow a switch to do regarding multicast group management?

A. Allow data forwarding to unused multicast streams

B. Detect IGMPv2 leave group messages

C. Store IGMPv2 join messages in the CAM table

D. Optimize multicast traffic across all VLANs

9. Which command is used to enable 802.1x authorization on an interface?

A. authentication port-control auto

B. aaa authorization auth-proxy default

C. aaa authorization network default group tacacs+

D. authentication control-direction both

10. What is the effect of the given configuration in the exhibit?

A. It creates a default class

B. It creates a resource class

C. It oversubscribes VPN sessions for the given class

D. It allows each context to utilize all available resources

Answers

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

Explanations

1. 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.

2. What impact does TACACS+ have regarding console port access?

A. Local database is the sole authentication method

B. Authentication is managed through the TACACS+ server

C. Only level 15 users can access the console

D. It disables all other authentication methods

TACACS+ (Terminal Access Controller Access-Control System Plus) is a protocol that provides centralized authentication, authorization, and accounting services for users who access network devices. When it comes to console port access on network devices, TACACS+ plays a critical role in managing user authentication. The correct choice indicates that authentication for console access is handled by the TACACS+ server. This centralizes the management of user credentials and access permissions, allowing administrators to have a unified approach to securing access across multiple devices. By using TACACS+, all authentication requests made when accessing the console port are sent to the TACACS+ server, which authenticates the user based on the credentials stored in its database. This enhances security compared to local authentication, allowing administrators to enforce policies and maintain control over user access. Other choices describe aspects that do not fully reflect the capabilities of TACACS+ in the context of console access. For instance, stating that the local database is the sole authentication method contradicts the essence of TACACS+, which is designed to centralize and enhance authentication methods. Additionally, the statement about level 15 users implies a limitation that could restrict user access without acknowledging the flexibility provided by TACACS+. Finally, asserting that TACACS+ disables all other authentication methods overlooks

3. Which two statements about 802.1x components are true? (Choose two)

A. The certificates used in the client-server authentication process are stored on the access switch

B. The access layer switch is the policy enforcement point

C. The RADIUS server is the policy enforcement point

D. The RADIUS server is the policy information point

The statement regarding the access layer switch as the policy enforcement point is accurate because, in an 802.1X authentication framework, the access layer switch plays a critical role in controlling port access based on authentication results. When a device attempts to connect to the network, the access switch is responsible for determining whether the device is granted access or denied, thus enforcing the security policy in place. It effectively acts as a gatekeeper, allowing only authenticated devices to access the network resources while blocking unauthorized ones. The role of the access switch as the policy enforcement point highlights its function in the overall architecture of 802.1X, where it interfaces directly with endpoints and serves to uphold security measures as dictated by the organization's policies. This is essential for implementing network access control, ensuring that only devices that are properly authenticated can utilize network services. In contrast, the RADIUS server, while essential in handling authentication, authorization, and accounting (AAA), serves more as the policy information point, where it processes requests from the access switch and provides the necessary decisions based on stored policies. Thus, the correct identification of the access switch in this context emphasizes its pivotal function within the 802.1X deployment for enforcing network access decisions.

4. Which statement regarding routing functions of Cisco ASA running software version 9.2 is true?

A. The ASA supports policy-based routing with route maps

B. In a failover pair of ASAs, the standby firewall establishes a peer relationship with OSPF neighbors

C. The translation table cannot override the routing table for new connections

D. Routes to the Null0 interface cannot be configured to black-hole traffic

The statement that routes to the Null0 interface cannot be configured to black-hole traffic is not accurate. In routing, the Null0 interface is commonly used to discard or "black-hole" unwanted traffic. When a route is configured to point to Null0, it effectively signifies that any traffic matching that route should simply be discarded. This is typically utilized to prevent routing loops or to manage unwanted traffic flows. The other statements highlight various aspects of Cisco ASA functionality, but the assertion regarding the Null0 interface specifically addresses its purpose in managing unwanted traffic. In an ASA environment, the Null0 route plays a critical role and can indeed be employed to black-hole traffic, effectively terminating specific pathways without forwarding them. Therefore, understanding the specifics of how the Null0 interface operates allows an individual to manage routing behaviors within the ASA effectively and utilize the interface appropriately when configuring network traffic management strategies.

5. Which setting determines the prefix address of a 6to4 tunnel?

A. Static configuration set in the router.

B. The IPv6 configuration to the interface.

C. The DHCP server settings.

D. The address of the terminating node.

The prefix address of a 6to4 tunnel is determined by the IPv6 configuration applied to the interface. In a 6to4 tunnel, the IPv6 addresses that are assigned to the interface are derived from the IPv4 address of the router. Specifically, the first 48 bits of the IPv6 address are fixed and reserved for 6to4 (2002::/16), while the subsequent 32 bits come from the IPv4 address in its hexadecimal format. When configuring a 6to4 tunnel, the interface must be set up correctly to include the appropriate IPv6 address that combines the designated prefix with the IPv4 address. This allows the tunnel to encapsulate IPv6 packets within IPv4 for transmission across the IPv4 internet. Other options, while relevant to networking, do not play a direct role in determining the prefix address for a 6to4 tunnel. Static configuration in the router can set various parameters but does not specifically dictate the prefix for 6to4 tunneling. DHCP server settings typically involve address assignment for dynamic IP addressing, particularly for IPv4, and do not influence a 6to4 tunnel's prefix address. Similarly, the address of the terminating node is part of the connection but is not

6. Which feature does Cisco VSG utilize to redirect traffic on Cisco Nexus 1000V Series Switch?

A. VPC

B. VDC

C. VEM

D. vPath

Cisco VSG (Virtual Security Gateway) uses vPath as its key feature for redirecting traffic within the Cisco Nexus 1000V Series Switch. vPath is a virtualized function that allows for the dynamic redirection of traffic, enabling the seamless integration of security services into the virtualized data center environment. It essentially functions as a bypass mechanism that directs the traffic to the VSG's virtual appliances for inspection and security processing. Implementing vPath allows for better scalability and flexibility as it adapts to the shifting workloads in virtual environments. Moreover, it provides an elegant way to incorporate various security policies and controls at the virtual network level without introducing significant overhead or disruption to the user experience. This alignment with virtualized infrastructure means that security can be integrated deeply into the fabric of the network, ensuring that all traffic can be monitored and controlled effectively. In contrast, the other options refer to different features that do not specifically relate to traffic redirection: VPC (Virtual Port Channel) focuses on link aggregation for enhanced redundancy and bandwidth, VDC (Virtual Device Context) is about partitioning a physical switch into multiple logical devices with separate resources, and VEM (Virtual Ethernet Module) is connected to the control plane but does not directly handle traffic redirection

7. 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.

8. What does IGMPv2 allow a switch to do regarding multicast group management?

A. Allow data forwarding to unused multicast streams

B. Detect IGMPv2 leave group messages

C. Store IGMPv2 join messages in the CAM table

D. Optimize multicast traffic across all VLANs

IGMPv2, or Internet Group Management Protocol version 2, enables switches to efficiently manage multicast group membership on a local network. When a device wishes to leave a multicast group, it sends a leave group message. IGMPv2 allows the switch to detect these leave messages, which is crucial for managing the multicast traffic flow. When the switch becomes aware that there are no longer any devices interested in a particular multicast stream, it can stop forwarding that data to the relevant ports, thus optimizing network resources by ensuring that multicast traffic is only sent to devices that need it. This capability enhances the overall efficiency of multicast routing, as it reduces unnecessary traffic on the network, enabling better performance and resource utilization. By accurately detecting when devices leave multicast groups, the network is able to adapt dynamically to changing group memberships, ensuring that multicast data is delivered only where it is actively requested.

9. Which command is used to enable 802.1x authorization on an interface?

A. authentication port-control auto

B. aaa authorization auth-proxy default

C. aaa authorization network default group tacacs+

D. authentication control-direction both

Enabling 802.1x authorization on an interface is accomplished with the command that specifically sets the port control mechanism for authentication. The command "authentication port-control auto" configures the interface to automatically control access based on the authentication state of the device connected to it. When this command is applied, the switch interface will enter a state allowing or denying access based on the result of the IEEE 802.1x authentication process. If a device connects, the switch will begin the authentication process, and depending on whether the authentication is successful or fails, the switch port will react accordingly by either granting access to the VLAN or placing the port in a restricted state. This command is essential for implementing secure access control on a network, as it ensures that only devices that have been authenticated are granted access to the network resources, enhancing security measures against unauthorized access.

10. What is the effect of the given configuration in the exhibit?

A. It creates a default class

B. It creates a resource class

C. It oversubscribes VPN sessions for the given class

D. It allows each context to utilize all available resources

The correct choice is that the configuration creates a resource class. In the context of networking and specifically in models like Cisco's, resource classes are used to define how resources such as bandwidth and hardware are allocated and managed for specific traffic types or user groups. By creating a resource class, the configuration essentially groups certain types of traffic or user sessions, allowing for more organized and efficient resource management. This is particularly important in environments where multiple types of traffic need to coexist and where prioritizing certain types of traffic (like voice over data) is crucial for maintaining quality of service. The other options do not accurately reflect the implications of the configuration. The idea of creating a default class typically refers to a generic handling of all unmatched traffic, rather than classifying resources for specific uses. Similarly, oversubscribing VPN sessions would imply that available resources are being spread too thin, which runs contrary to the intention of establishing clear resource classifications. Lastly, allowing each context to utilize all available resources speaks more to a uniform allocation rather than the detailed management that a resource class provides, which is focused on organizing resources effectively rather than permitting unrestricted access to all resources.

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!