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

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cisco-internetwork.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

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

SAMPLE

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

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. What is the significance of vPath in Cisco networking?

A. To enable high availability

B. To manage resource allocation

C. To direct traffic between different contexts

D. To separate management and data planes

2. Which statement is true regarding 6to4 tunneling?

A. It provides a /128 address block.

B. The prefix address of the tunnel is determined by the IPv6 configuration on the interface.

C. It supports static routing only.

D. It provides a /48 address block.

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. Which choice describes a functionality of the Cisco ASA Identity Firewall regarding threat identification?

A. It can identify threats quickly based on their URLs

B. It only reacts to detected threats after an event occurs

C. It provides no mechanism for real-time identification

D. It requires specialized training to operate

5. What SNMPv3 command disables descriptive error messages?

A. snmp-server usm cisco

B. snmp-server inform

C. snmp-server infindex persist

D. snmp-server trap link switchover

SAMPLE

6. Which command allows for dynamic NAT configuration on a Cisco router?

A. ip nat inside source list

B. ip nat outside source

C. ip nat inside

D. ip nat pool

7. Which directive of the crypto key encrypt write rsa command on a router is true?

A. The device saves the unlocked encrypted key to the NVRAM

B. The device encrypts and locks the key before authenticating it with an external CA server

C. The device unlocks the encrypted key, but the key is lost when the router is reloaded

D. The device locks the encrypted key and saves it to the NVRAM

8. Which three Cisco attributes for LDAP authorization are supported on the ASA? (Choose three)

A. Authenticated-User-Idle-Timeout

B. Web-VPN-ACL-Filters

C. L2TP-Encryption

D. IPsec-Default-Domain

9. Which address range is representative of Automatic Private IP Addressing?

A. 10.1.x.x

B. 172.10.1.x

C. 169.254.x.x

D. 196.245.x.x

10. 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

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the significance of vPath in Cisco networking?

A. To enable high availability

B. To manage resource allocation

C. To direct traffic between different contexts

D. To separate management and data planes

The significance of vPath in Cisco networking is centered around its function to direct traffic between different contexts. vPath is a critical component of Cisco's application-centric networking approach, specifically in solutions like the Application Centric Infrastructure (ACI). It operates as an intelligent data plane that facilitates the forwarding of packets through the network, particularly in multi-tenant environments where various virtual network segments must interact with one another. By enabling this traffic direction, vPath ensures efficient communication between different virtualized contexts, which is essential for maintaining application performance and responsiveness in a dynamic cloud or data center environment. This capability allows for the seamless routing of traffic to the appropriate services or resources based on defined policies and context information, thus optimizing the networking experience for applications hosted in those environments. The other options, while relevant to networking concepts, do not accurately capture the main purpose of vPath. High availability deals with ensuring systems remain operational, managing resource allocation addresses how resources are distributed and utilized, and separating management and data planes pertains to security and operational efficiency rather than the specific traffic direction capabilities provided by vPath.

2. Which statement is true regarding 6to4 tunneling?

A. It provides a /128 address block.

B. The prefix address of the tunnel is determined by the IPv6 configuration on the interface.

C. It supports static routing only.

D. It provides a /48 address block.

6to4 tunneling is a method that allows IPv6 packets to be transmitted over an IPv4 network by encapsulating them within IPv4 packets. This tunneling technique uses a special IPv6 prefix, specifically the 2002::/16 prefix, which is derived from the IPv4 address of the device that is the tunnel endpoint. When a device that supports 6to4 tunneling is configured, it automatically generates a /48 address block for its interior IPv6 addresses. This means that the device can have up to 65,536 subnets, each with a /64 prefix. The use of a /48 address block maximizes the potential for subnetting and allows for efficient address allocation for multiple networks. The other statements do not correctly represent the 6to4 tunneling method. For instance, stating that the prefix address of the tunnel is determined by the IPv6 configuration on the interface does not hold true, as it is predefined by the 2002::/16 prefix based on the underlying IPv4 address. Furthermore, 6to4 tunneling does not solely support static routing; it is compatible with dynamic routing protocols as well. Lastly, it indeed provides a /48 address block rather than a /128 address block

SAMPLE

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. Which choice describes a functionality of the Cisco ASA Identity Firewall regarding threat identification?

A. It can identify threats quickly based on their URLs

B. It only reacts to detected threats after an event occurs

C. It provides no mechanism for real-time identification

D. It requires specialized training to operate

The Cisco ASA Identity Firewall provides functionality that enables it to quickly identify threats based on their URLs. This capability enhances the firewall's ability to categorize and respond to potential threats by analyzing the URLs associated with network traffic. By focusing on URLs, the ASA Identity Firewall can leverage a vast database of known threats and malicious web domains, allowing it to proactively filter traffic and block harmful content before it reaches the internal network. This approach not only aids in timely threat detection but also reduces the risk of malware infections and data breaches. In contrast to the other options, which highlight limitations or misconceptions about the capabilities of the Cisco ASA, the emphasis on URL-based identification underscores the advanced nature of the Identity Firewall in terms of proactive threat management. It is specifically designed to identify and mitigate threats in real-time, contrary to the implication that it solely reacts after a threat is detected or lacks any real-time identification mechanisms. Additionally, while specialized training might enhance the operator's ability to utilize the features of the ASA, it is not a requirement for basic operation, demonstrating the user-friendly nature of its management and threat identification capabilities.

SAMPLE

5. What SNMPv3 command disables descriptive error messages?

A. snmp-server usm cisco

B. snmp-server inform

C. snmp-server infindex persist

D. snmp-server trap link switchover

Disabling descriptive error messages in SNMPv3 can be achieved through specific configurations in the SNMP engine's User-based Security Model (USM). The command relevant to this action is the one that modifies the behavior of error message reporting. The choice that correctly addresses the requirement to disable descriptive error messages is the command that utilizes USM features. When the command is executed in this context, it can limit the information that is disclosed in error messages. This is important for security reasons, as detailed error messages could potentially expose sensitive information about the network or devices. Alternatives like the command related to informing or trapping do not focus on the descriptive aspects of error messages or managing how error conditions are reported, which is the primary goal of the inquiry. These commands typically involve the handling of notifications and traps rather than adjusting the verbosity or detail of error messages presented by the SNMP agent. Therefore, focusing on the USM-related command aligns best with the requirement to control error messaging behavior effectively.

6. Which command allows for dynamic NAT configuration on a Cisco router?

A. ip nat inside source list

B. ip nat outside source

C. ip nat inside

D. ip nat pool

The command that facilitates dynamic NAT configuration on a Cisco router is "ip nat inside source list." This command specifies an access control list (ACL) that identifies the internal IP addresses that will be translated to the public IP addresses. By using this command, the router can dynamically map multiple internal addresses to a pool of public addresses based on the rules defined in the ACL. When dynamic NAT is configured, routers provide a way for internal devices to communicate with external networks (like the Internet) by translating their private IP addresses into public IPs as needed. The command indicates the internal network that needs NAT, allowing for the dynamic allocation of the public addresses from the pool. In contrast, the other command options serve different purposes within NAT configuration. While "ip nat outside source" is related to static NAT configurations or configuring NAT for traffic going to an outside source, "ip nat inside" merely indicates which interfaces are considered part of the inside network without specifying dynamic NAT. Similarly, "ip nat pool" is used to define a range of public IP addresses available for NAT translations but does not configure the actual mapping process. Thus, "ip nat inside source list" is specifically the command that initiates the dynamic translation process by referencing the ACL that identifies the traffic

SAMPLE

7. Which directive of the crypto key encrypt write rsa command on a router is true?

A. The device saves the unlocked encrypted key to the NVRAM

B. The device encrypts and locks the key before authenticating it with an external CA server

C. The device unlocks the encrypted key, but the key is lost when the router is reloaded

D. The device locks the encrypted key and saves it to the NVRAM

The directive of the crypto key encrypt write rsa command that is true emphasizes that the device is designed to save the unlocked encrypted key to non-volatile random access memory (NVRAM). This is significant because it ensures that the key persists through device reboots or power cycles. When the router runs the command, it takes the key, encrypts it, and then writes that encrypted version into NVRAM, where it can be retrieved later without needing to generate a new key or lose access to the encrypted data. This process allows for secure storage of cryptographic keys, enabling ongoing secure communications without the need for regeneration after a reboot, which is crucial for maintaining system integrity and security in network configurations. The chosen answer reflects the router's functioning concerning key management and encryption practices.

8. Which three Cisco attributes for LDAP authorization are supported on the ASA? (Choose three)

A. Authenticated-User-Idle-Timeout

B. Web-VPN-ACL-Filters

C. L2TP-Encryption

D. IPsec-Default-Domain

The attributes supported for LDAP authorization on the ASA provide essential functionalities for managing user sessions and access. The choice of Authenticated-User-Idle-Timeout is particularly important because it defines how long an authenticated user can remain idle before the session is terminated. This is crucial in maintaining security by ensuring that inactive sessions do not remain accessible indefinitely, reducing the risk of unauthorized access. The design of LDAP authorization on the ASA includes various mechanisms to enhance security and manage user access based on specific requirements. Understanding these attributes in the context of LDAP helps in fine-tuning the security posture of the network. Items like Web-VPN-ACL-Filters, L2TP-Encryption, and IPsec-Default-Domain are linked to specific configurations and protocols that do not play a role in LDAP authorization, making them less relevant in this context. Recognizing the characteristics of each attribute is fundamental for properly configuring and leveraging Cisco ASA for secure access management within a network utilizing LDAP.

SAMPLE

9. Which address range is representative of Automatic Private IP Addressing?

A. 10.1.x.x

B. 172.10.1.x

C. 169.254.x.x

D. 196.245.x.x

Automatic Private IP Addressing (APIPA) is a feature used by devices to automatically assign themselves an IP address from a predefined range when a DHCP server is not available. The specific address range for APIPA is 169.254.0.1 to 169.254.255.254, which allows devices on the same local network to communicate without a manual configuration or a DHCP server. Choosing the address range of 169.254.x.x correctly identifies this APIPA range. When a device detects that it cannot reach a DHCP server within a specified time frame, it selects an IP address from this range to ensure local communication with other devices that may also have self-assigned addresses. This functionality is crucial in local networks where communication must still occur even without a central IP addressing service. Other options represent different types of IP addressing. For instance, addresses starting with 10.1.x.x belong to the Class A private address space, while those in the range of 172.10.1.x fall into the Class B private address space. The 196.245.x.x addresses indicate public IP addresses that are routable on the Internet. Thus, these options do not pertain to the self-assigned IP addresses specified by the APIPA

10. 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.

SAMPLE

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!

SAMPLE