# CCNA 3 ENTERPRISE NETWORKING, SECURITY, AND AUTOMATION, VERSION 7.0 PRACTICE EXAM (SAMPLE)

## STUDY GUIDE



## SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

**VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE**

https://ccna3enterprisenetsecautomationv7.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. **Which OSPF database is identical on all converged routers within the same OSPF area?**

   A. Link-state

   B. Routing table

   C. Adjacency database

   D. Forwarding database

2. **What networking trend is being implemented when a data center hosts multiple operating systems on a single CPU for each customer?**

   A. Cloud computing

   B. Virtualization

   C. Load balancing

   D. Network segmentation

3. **What is the primary benefit of using a site-to-site VPN for corporate networks?**

   A. Higher bandwidth

   B. Enhanced security

   C. Cost-effectiveness

   D. Ease of management

4. **What are two benefits of using SNMP traps?**

   A. They increase the frequency of polling.

   B. They eliminate the need for some periodic polling requests.

   C. They enhance data encryption.

   D. They reduce the load on network and agent resources.

5. **Which type of malware is used to control computers in a zombie network?**

   A. Trojan horse

   B. Worm

   C. Botnet

   D. Spyware

SAMPLE

**6. Which OSPFv2 packet is utilized to transmit link state change information?**

A. LSP

B. LSU

C. NTP

D. Link State Update

**7. Which type of VPN is the preferred choice for support and ease of deployment for remote access?**

A. IPSec VPN

B. SSL VPN

C. L2TP VPN

D. PPTP VPN

**8. Which type of traffic is most sensitive to quality issues like latency and jitter?**

A. Data transfer

B. File sharing

C. Voice and video communications

D. Email communication

**9. What are two purposes of launching a reconnaissance attack on a network?**

A. To disrupt network services

B. To gather information about the network and devices

C. To introduce malware

D. To scan for accessibility

**10. What protocol uses agents to collect and store information about managed devices and their operation?**

A. LLDP

B. SNMP

C. RIP

D. OSPF

SAMPLE

# Answers

SAMPLE

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

SAMPLE

# Explanations

SAMPLE

**1. Which OSPF database is identical on all converged routers within the same OSPF area?**

A. Link-state

B. Routing table

C. Adjacency database

D. Forwarding database

*The OSPF database that is identical on all converged routers within the same OSPF area is the link-state database (LSDB). Each router running OSPF within an area builds and maintains this database based on the link-state advertisements (LSAs) that are exchanged among routers. When OSPF routers establish adjacencies, they share information about their own interfaces and their direct connections, which are collected in LSAs. All routers in the same OSPF area will receive these LSAs, allowing them to create an identical link-state database. This uniformity of the LSDB enables each router to compute the best paths through the network using the Dijkstra algorithm, ensuring that they all have a consistent view of the network topology. This synchronization across routers is critical for OSPF's operation, as it allows for accurate and efficient route calculation and ensures that all routers have the same understanding of the available routes and their costs.*

**2. What networking trend is being implemented when a data center hosts multiple operating systems on a single CPU for each customer?**

A. Cloud computing

B. Virtualization

C. Load balancing

D. Network segmentation

*The concept being described is the implementation of virtualization within a data center. Virtualization allows multiple operating systems to run on a single physical CPU through the use of hypervisors. This technology abstracts the hardware layer, enabling the creation of virtual machines (VMs) which can operate independently and run different operating systems as if they were on separate physical machines. Each VM is isolated from others, ensuring that different clients or applications can operate simultaneously without interference. This trend not only maximizes resource utilization by allowing efficient use of the underlying hardware, but also offers benefits in scalability, flexibility, and cost-effectiveness. Organizations can quickly deploy new services, manage workloads more effectively, and reduce hardware costs due to the consolidation of multiple servers onto fewer physical machines. Therefore, virtualization is a key enabler of modern data center architecture and is closely associated with cloud computing as well, but it specifically refers to the technology that allows those multiple systems to exist on a single CPU.*

SAMPLE

## 3. What is the primary benefit of using a site-to-site VPN for corporate networks?

A. Higher bandwidth

B. Enhanced security

C. Cost-effectiveness

D. Ease of management

*The primary benefit of using a site-to-site VPN for corporate networks is enhanced security. A site-to-site VPN creates a secure tunnel between two or more geographically separated networks, allowing data to be transmitted over the internet in a protected manner. This means sensitive corporate data remains encrypted and secure from eavesdropping or interception while traveling across public or untrusted networks. In addition to providing endpoint-to-endpoint encryption, site-to-site VPNs utilize strong encryption protocols, authentication methods, and often support measures like firewalls, further bolstering the security posture of the corporate network. This enhanced security is especially important for organizations that handle confidential information or need to comply with regulatory requirements. While factors such as bandwidth, cost-effectiveness, and ease of management may play a role in the decision to implement a VPN, they do not fundamentally address the primary goal of maintaining the confidentiality, integrity, and availability of data transmitted between different corporate sites.*

## 4. What are two benefits of using SNMP traps?

A. They increase the frequency of polling.

B. They eliminate the need for some periodic polling requests.

C. They enhance data encryption.

D. They reduce the load on network and agent resources.

*Using SNMP traps provides significant benefits, with one of the key advantages being that they eliminate the need for some periodic polling requests. SNMP (Simple Network Management Protocol) traps enable devices on a network to send asynchronous notifications to a management system when certain events occur or thresholds are reached. This means that instead of continuously polling the devices to check their status—which can consume network bandwidth and processing power—devices can proactively report changes or issues as they happen. This proactive communication reduces the necessity for regular polling of every device, allowing for a more efficient management strategy. Another major benefit of utilizing SNMP traps is that they reduce the load on both network and agent resources. Because traps are sent only when an event occurs, they conserve bandwidth and processing resources that would otherwise be consumed by continuous polling, making the overall management setup more efficient and responsive. This benefit is particularly important in large networks with numerous devices, where the overhead of constant polling could lead to degraded performance and increased latency. In summary, the elimination of the need for some periodic polling requests paired with reduced load on resources are two primary advantages of implementing SNMP traps in network management.*

SAMPLE

## 5. Which type of malware is used to control computers in a zombie network?

A. Trojan horse

B. Worm

C. Botnet

D. Spyware

*The correct choice, which is botnet, refers to a collection of compromised devices that are controlled by a central command, often without the knowledge of the device owners. A botnet is typically created when malware infects devices, turning them into "zombies." This allows an attacker to control these devices remotely and carry out various malicious activities, such as launching Distributed Denial of Service (DDoS) attacks, sending spam, or stealing information. Understanding the function of a botnet highlights its significance in the context of cybersecurity threats. Devices in a botnet can be manipulated to coordinate actions, making them a powerful tool for cybercriminals to exert control over multiple machines. The other types of malware mentioned do not serve the same purpose. Trojan horses are designed to appear as legitimate software to deceive users into installing them, but they do not inherently create a network of controlled devices. Worms are self-replicating malware that spread without user intervention but do not necessarily control other devices like a botnet does. Spyware is meant to gather information from a user's device without their consent, focusing on data theft rather than the orchestration of a network of compromised machines.*

## 6. Which OSPFv2 packet is utilized to transmit link state change information?

A. LSP

B. LSU

C. NTP

D. Link State Update

*The OSPFv2 packet that is utilized to transmit link state change information is the Link State Update (LSU) packet. This packet plays a critical role in the OSPF routing protocol as it is responsible for conveying the Link State Advertisements (LSAs) from one router to another. When there is a change in the network topology, such as a link going up or down, routers generate LSAs that describe their state and the network's current configuration. These LSAs are then encapsulated within the LSU packets and sent to neighboring routers. Upon receiving LSU packets, routers can update their link state databases and recalculate their routing tables accordingly. This mechanism allows OSPF to quickly adapt to network changes and maintain accurate routing information across the entire OSPF area. In contrast, the other options do not accurately represent the function of OSPFv2 packets used for transmitting link state information.*

SAMPLE

## 7. Which type of VPN is the preferred choice for support and ease of deployment for remote access?

A. IPSec VPN

B. SSL VPN

C. L2TP VPN

D. PPTP VPN

*The preferred choice for support and ease of deployment for remote access is an SSL VPN. SSL VPNs use the Secure Sockets Layer (SSL) protocol to provide secure access over the internet, allowing remote users to connect to corporate networks without requiring a full VPN client installation. This makes it particularly user-friendly, as it typically only requires a web browser for users to establish a secure tunnel to access resources. One of the primary advantages of SSL VPNs is that they can support a wide range of devices and operating systems, including smartphones and tablets, which are less commonly supported by traditional VPN protocols. Additionally, because they can operate over HTTPS, SSL VPNs can easily traverse firewalls and NAT (Network Address Translation) devices, simplifying configuration and deployment in various environments. Furthermore, SSL VPNs can provide granular access controls, allowing for different levels of access based on user roles or specific applications, which enhances security without complicating the user experience. This adaptability and ease of use, combined with strong encryption, make SSL VPNs a preferred option for organizations looking to provide secure remote access to their employees.*

## 8. Which type of traffic is most sensitive to quality issues like latency and jitter?

A. Data transfer

B. File sharing

C. Voice and video communications

D. Email communication

*Voice and video communications are the types of traffic most sensitive to quality issues such as latency and jitter because they rely on real-time data transmission. In these applications, maintaining a constant flow of data is crucial to ensure a clear and uninterrupted experience. Latency, which refers to the delay before data starts to transfer, can lead to noticeable delays in conversations, making it difficult for participants to engage in natural dialogue. Jitter, the variation in packet arrival times, can cause choppy audio or video, leading to a disruptive user experience. In contrast, other types of traffic like data transfer, file sharing, and email communication can tolerate some delays and variations in data delivery, as these applications often involve buffering or retransmission of data. For instance, a file transfer session can experience delays without significantly impacting the overall outcome, since the transfer can pause and pick up again. Therefore, while all types of network traffic have some sensitivity to quality issues, voice and video communications demand the highest level of performance to function effectively.*

SAMPLE

## 9. What are two purposes of launching a reconnaissance attack on a network?

A. To disrupt network services

B. To gather information about the network and devices

C. To introduce malware

D. To scan for accessibility

*Launching a reconnaissance attack on a network primarily aims to gather information about the network and its connected devices. This phase is critical for attackers as it allows them to identify potential vulnerabilities, understand the network structure, and determine the types and configurations of devices present. Through various techniques such as scanning and probing, attackers can collect data about IP addresses, open ports, operating systems, and the services running on different devices within the network. This information is essential for planning subsequent steps in an attack, making it the foundation for exploiting vulnerabilities and gaining unauthorized access. In contrast, disrupting network services or introducing malware are more aggressive actions meant to compromise or harm the network itself. Though scanning for accessibility can aid in reconnaissance, the broader purpose of a reconnaissance attack is to gather detailed information rather than focusing solely on access. Therefore, the primary objective of reconnaissance attacks is to collect valuable information that can inform further attacks, which is why gathering information about the network and devices is a fundamental purpose.*

## 10. What protocol uses agents to collect and store information about managed devices and their operation?

A. LLDP

B. SNMP

C. RIP

D. OSPF

*The correct choice is SNMP, which stands for Simple Network Management Protocol. SNMP is designed to manage devices on IP networks by allowing administrators to monitor and control network devices such as servers, routers, switches, and printers. SNMP employs a client/server architecture that includes agents and a network management system (NMS). The agents run on the managed devices and are responsible for collecting and storing information about the device's operational state and performance metrics. This information is typically stored in a Management Information Base (MIB), and the NMS can query the agents to retrieve data, set configuration parameters, and receive alerts for specific events or traps. Due to its versatility and widespread support, SNMP has become the standard for network management. It allows for efficient monitoring and management of complex network environments, making it easier for network administrators to ensure devices are functioning correctly and to troubleshoot issues as they arise. LLDP (Link Layer Discovery Protocol) is primarily used for discovering neighboring devices on a local network. RIP (Routing Information Protocol) and OSPF (Open Shortest Path First) are routing protocols focused on the exchange of routing information between routers but do not provide capabilities for monitoring and managing network devices in the way that SNMP does.*

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://ccna3enterprisenetsecautomationv7.examzify.com

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

SAMPLE