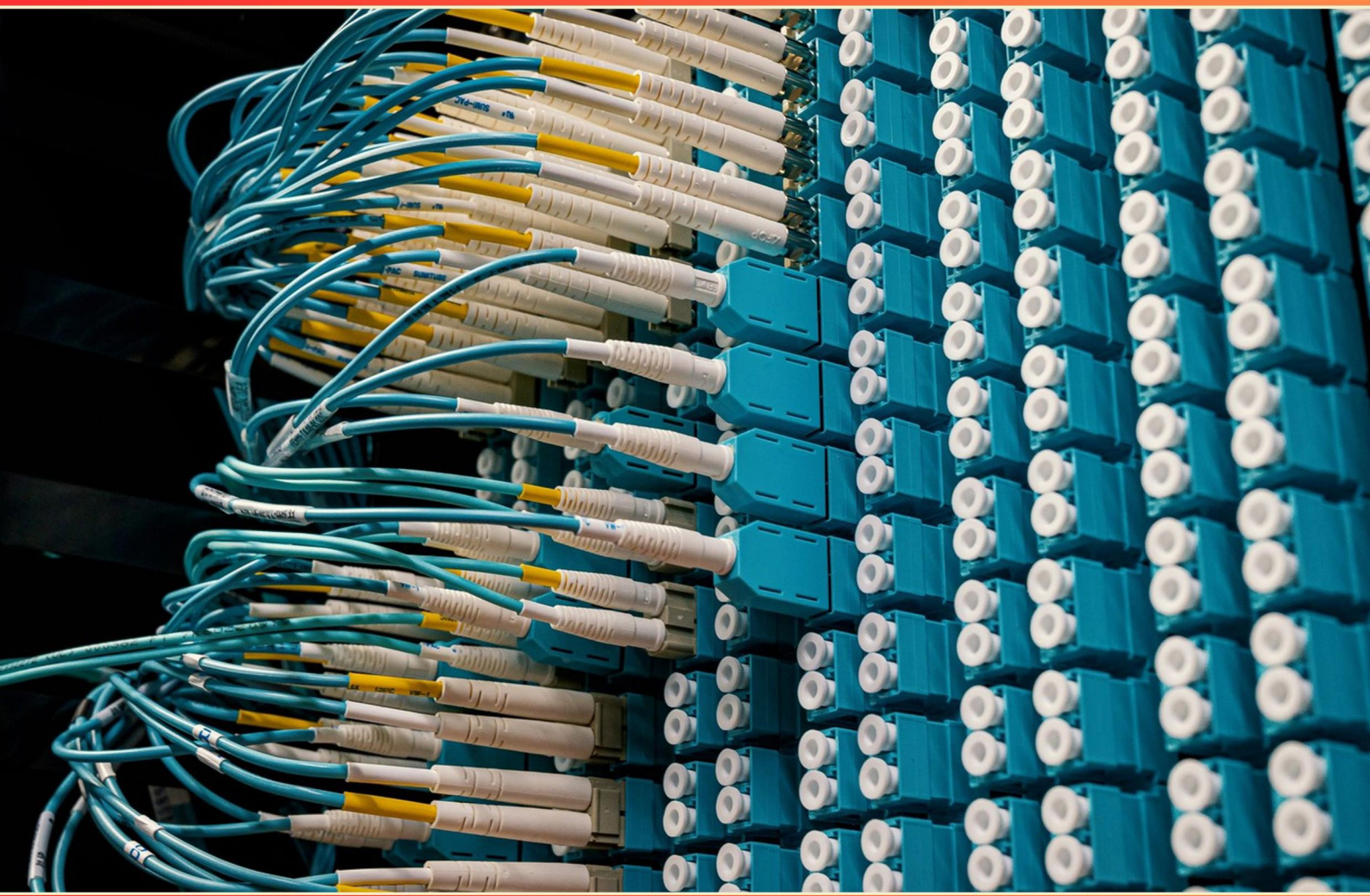
CISCO NETWORKING ESSENTIALS (25B) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cisconetessentials25b.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

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 does the acronym BIOS stand for?

A. Basic Input Output System

B. Binary Input Output Storage

C. Basic Integrated Operating System

D. Binary Integrated Output System

2. What protocol operates at Layer 2 of the OSI model?

A. IP

B. Ethernet

C. TCP

D. UDP

3. Which protocol is used for resolving domain names into IP addresses?

A. ICMP

B. DNS

C. DHCP

D. ARP

4. What is the maximum reach limit for twisted-pair cable?

A. 150 meters

B. 100 meters

C. 200 meters

D. 250 meters

5. What does a PC search for first during startup?

A. Random Access Memory

B. Flash memory

C. Hard drive

D. Network boot server

6. What does DHCP stand for?

A. Dynamic Host Control Protocol

B. Dynamic Host Configuration Protocol

C. Dynamic Hypertext Control Protocol

D. Distributed Host Control Protocol

SAMPLE

7. What type of attack is characterized by overwhelming a system with pings?

A. Phishing

B. Denial of Service - DOS

C. Man-in-the-middle

D. Trojan Horse

8. Which of the following is a method to enhance the security of a wireless network?

A. SSID Visibility

B. Change default passwords

C. MAC Filtering

D. Using public IP addresses

9. What technology allows both IPv6 and IPv4 to be utilized at the same time?

A. Subnetting

B. Dual stack

C. VPN tunneling

D. Gateway translations

10. What type of IP address is routable on the internet?

A. Private IP address

B. Static IP address

C. Public IP address

D. Dynamic IP address

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What does the acronym BIOS stand for?

A. Basic Input Output System

B. Binary Input Output Storage

C. Basic Integrated Operating System

D. Binary Integrated Output System

The acronym BIOS stands for Basic Input Output System. This foundational software is essential for a computer's boot process, as it initializes hardware components after the computer is powered on and loads the operating system. The BIOS firmware is stored on a chip located on the motherboard, allowing the computer to perform necessary checks and configuration of hardware during the startup phase. It provides the interface for communication between the operating system and the hardware components of the computer, facilitating the function of keyboards, hard drives, and display units. Understanding the role of the BIOS is crucial in networking and IT environments, as issues related to hardware detection and system startup often necessitate troubleshooting BIOS configurations.

2. What protocol operates at Layer 2 of the OSI model?

A. IP

B. Ethernet

C. TCP

D. UDP

Ethernet is the protocol that operates at Layer 2 of the OSI model, which is the Data Link layer. This layer is responsible for node-to-node data transfer and for handling error correction from the Physical layer, ensuring that data packets are delivered between devices on the same local network. Ethernet defines the framing, addressing, and error detection methods for data as it traverses a physical medium. The Data Link layer creates a reliable communication channel for the devices connected to the same local area network, facilitating the transfer of data frames. This includes MAC (Media Access Control) addressing, which is essential for identifying devices on the network and ensuring that data is directed to the correct destination. In contrast, the other protocols listed operate at different layers of the OSI model. IP (Internet Protocol) works at Layer 3, which is the Network layer responsible for routing packets across multiple networks. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) operate at Layer 4, known as the Transport layer, where they manage end-to-end communication and data flow between host applications. Understanding these distinctions is crucial when analyzing network protocols and their respective roles within the OSI framework.

SAMPLE

3. Which protocol is used for resolving domain names into IP addresses?

A. ICMP

B. DNS

C. DHCP

D. ARP

The protocol that is specifically designed for resolving domain names into IP addresses is the Domain Name System (DNS). This system plays a crucial role in the functioning of the internet, as it allows users to access websites using human-readable domain names (like www.example.com) instead of having to remember numeric IP addresses (such as 192.0.2.1). When a user types a domain name into a web browser, the DNS protocol is invoked to translate that domain name into the corresponding IP address, enabling the connection to the correct server. This translation process is essential for locating and accessing resources on the internet efficiently. Other protocols mentioned have their respective roles but do not perform name resolution. For instance, Internet Control Message Protocol (ICMP) is primarily used for sending error messages and operational queries, the Dynamic Host Configuration Protocol (DHCP) is responsible for automatically assign IP addresses to devices on a network, and Address Resolution Protocol (ARP) is used to map IP addresses to physical MAC addresses on a local network. These functions are vital for network operations, but they do not facilitate the translation of domain names to IP addresses like DNS does.

4. What is the maximum reach limit for twisted-pair cable?

A. 150 meters

B. 100 meters

C. 200 meters

D. 250 meters

Twisted-pair cabling, which includes types like Category 5e, Category 6, and Category 6a, generally has a maximum reach limit of 100 meters for Ethernet connections. This length is considered standard for maintaining signal integrity in networking applications. Beyond this distance, the signal can begin to degrade due to attenuation and interference, which can lead to communication errors and reduced network performance. The 100-meter limit encompasses the total distance allowed for horizontal cabling, which includes both the lengths of the cable run from the networking device, as well as any additional patch cables used to connect to wall outlets. Adhering to this distance ensures that the network operates effectively and reliably, making it a crucial guideline for network design and installation.

SAMPLE

5. What does a PC search for first during startup?

A. Random Access Memory

B. Flash memory

C. Hard drive

D. Network boot server

During startup, a PC primarily searches for the operating system to load, which is typically stored in flash memory if the device uses solid-state drives or in other forms of non-volatile memory depending on the architecture. Flash memory is where the firmware, such as the BIOS or UEFI, resides. This firmware initializes the hardware components of the PC and conducts the Power-On Self-Test (POST) to ensure everything is functioning properly. After this initialization, the system will look for bootable devices to determine where to find the operating system. Though the hard drive is commonly used for this purpose, the initial firmware and boot sequence begin with the system's flash memory, as that is where the critical startup instructions are stored. Those instructions include search mechanisms for the operating system, whether it's on a hard drive, solid-state drive, or remotely located server. Other options like Random Access Memory (RAM) are crucial for temporary data storage while the system is running but are not involved in the initial phase of startup before the operating system is loaded. Similarly, looking for a network boot server is a method for booting but is generally only used in specific scenarios where network booting is configured as a priority over local drives. Thus, the first step in this boot

6. What does DHCP stand for?

A. Dynamic Host Control Protocol

B. Dynamic Host Configuration Protocol

C. Dynamic Hypertext Control Protocol

D. Distributed Host Control Protocol

The correct answer is Dynamic Host Configuration Protocol. DHCP is a network management protocol used to automate the process of configuring devices on IP networks. This includes assigning IP addresses, subnet masks, default gateways, and other communication parameters to devices, which enables them to connect to the network and communicate effectively. This process greatly simplifies network administration, especially in environments where devices frequently join and leave the network, as it eliminates the need for a network administrator to manually assign IP addresses. By dynamically configuring these settings, DHCP ensures that each device can communicate over the network without conflict and with minimized human intervention. The other options do not accurately characterize the function of DHCP. Dynamic Host Control Protocol, Dynamic Hypertext Control Protocol, and Distributed Host Control Protocol do not reflect the intended purpose of the protocol, which is to manage the allocation of IP addresses and other configuration settings in a streamlined manner.

SAMPLE

7. What type of attack is characterized by overwhelming a system with pings?

A. Phishing

B. Denial of Service - DOS

C. Man-in-the-middle

D. Trojan Horse

The scenario described, where a system is overwhelmed with pings, is characteristic of a Denial of Service (DoS) attack. In this type of attack, the attacker sends a flood of requests (in this case, ping requests) to the target system, consuming its resources and rendering it unable to respond to legitimate requests. The primary goal of a DoS attack is to make a machine or network resource unavailable to its intended users, thus disrupting normal operations. In a typical DoS attack, the excessive volume of traffic leads to network congestion, service degradation, or complete unavailability, effectively preventing legitimate users from accessing the system. By flooding the target with pings, the attacker exploits the system's resources, demonstrating how vulnerable systems can be to such simple yet effective strategies. Other options like phishing, man-in-the-middle, and Trojan Horse attacks involve different methodologies and objectives. Phishing usually aims at deceiving individuals into revealing sensitive information, while man-in-the-middle attacks focus on intercepting and manipulating communication between two parties. A Trojan Horse is a type of malware disguised as legitimate software. These methods do not share the same fundamental mechanism of overwhelming a target with traffic, which is why they do not apply in this context.

8. Which of the following is a method to enhance the security of a wireless network?

A. SSID Visibility

B. Change default passwords

C. MAC Filtering

D. Using public IP addresses

Enhancing the security of a wireless network is critical, and the chosen method—MAC filtering—plays a significant role in controlling device access. MAC filtering works by allowing only specified devices to connect to the network based on their unique Media Access Control (MAC) address. This creates a significant barrier against unauthorized access because, even if an attacker is aware of the wireless network's SSID and password, their device must be specifically allowed to connect. While other methods might contribute to overall security, the approach of limiting access through MAC addresses directly targets unauthorized users' ability to connect, thereby enhancing the security posture of the network. However, it's important to recognize that while MAC filtering can deter casual attempts to join the network, it is not a foolproof method. Attackers can spoof MAC addresses, making it necessary to utilize it in conjunction with other security measures for more robust protection. SSID visibility may improve awareness of network presence but does not inherently increase security. Changing default passwords is a good security practice for network devices but does not directly impact the wireless network security itself. Using public IP addresses is related to addressing and routing but offers no enhancement to the security of the wireless network.

SAMPLE

9. What technology allows both IPv6 and IPv4 to be utilized at the same time?

A. Subnetting

B. Dual stack

C. VPN tunneling

D. Gateway translations

The technology that allows both IPv6 and IPv4 to be utilized simultaneously is dual stack. This approach enables devices to configure and maintain both IP versions, allowing them to communicate over IPv4 networks while also being able to interact with IPv6 networks. The dual stack method is significant because it facilitates a smooth transition to IPv6, which is necessary due to the depletion of IPv4 addresses. By implementing dual stack, network devices can send and receive packets using either IPv4 or IPv6, depending on the network they are interacting with. This flexibility is crucial for organizations that are in the process of migrating their services and applications to support IPv6 while not completely phasing out IPv4, which is still prevalent in many established networks. Other options do not provide the capability to use both protocols at the same time effectively. Subnetting refers to dividing a larger network into smaller, manageable segments, but it does not inherently relate to the simultaneous operation of IPv4 and IPv6. VPN tunneling is a method of securing private data over public networks, and while it can be used in conjunction with both IP versions, it does not enable their concurrent use. Gateway translations involve converting traffic from one IP version to another but do not allow for simultaneous operation; they are

10. What type of IP address is routable on the internet?

A. Private IP address

B. Static IP address

C. Public IP address

D. Dynamic IP address

Public IP addresses are those that are routable on the internet. These addresses are assigned to devices that need to communicate over the internet, allowing them to send and receive data from any other device connected to the internet. Public IP addresses are unique across the entire internet and are governed by the Internet Assigned Numbers Authority (IANA). In comparison, private IP addresses are designated for use within local networks and cannot be routed on the internet. They are typically used for devices within a home or office, allowing them to communicate internally without being directly exposed to the internet. Although static IP addresses (which do not change and are manually assigned) and dynamic IP addresses (which can change and are assigned automatically) can both be public or private, the key distinction here is that only public IP addresses are routable on the internet. Thus, the nature of public IP addresses being directly addressable across the global internet space is what makes the correct answer valid.

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://cisconetessentials25b.examzify.com

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

SAMPLE