Cisco Networking Essentials (25B) Practice Exam (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 organization is the creator of wireless standards?

A. IEEE

B. ISO

C. ANSI

D. IETF

2. What type of data is encoded using light?

A. Electrical signals

B. Radio waves

C. Fiber optic

D. Digital packets

3. What is the primary purpose of a router in a network?

A. To connect multiple devices on the same local network

B. To transmit data on the same network segment

C. To direct data packets between different networks

D. To enhance signal strength in a network

4. 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

5. What type of routing allows routers to automatically adjust to changes in the network?

A. Static routing

B. Dynamic routing

C. Manual routing

D. Policy-based routing

6. What is the function of a DNS server?

A. To assign IP addresses dynamically

B. To translate domain names into IP addresses

C. To filter internet traffic

D. To manage network load

7. What is the difference between TCP and UDP?

A. TCP is connectionless while UDP is connection-oriented

B. TCP ensures reliable delivery while UDP does not guarantee delivery

C. UDP is faster than TCP because it is more reliable

D. TCP is used for video streaming while UDP is used for emails

8. Which command prints a detailed listing of the device's interfaces including their MAC addresses?

A. show ip interface

B. show interface status

C. show running-config

D. show interfaces

9. Which command could provide information about IP addressing of all interfaces, including status and hardware addresses?

A. show ip interface brief

B. show interfaces

C. show ip route

D. show config

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

A. Random Access Memory

B. Flash memory

C. Hard drive

D. Network boot server

Answers

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

Explanations

1. What organization is the creator of wireless standards?

A. IEEE

B. ISO

C. ANSI

D. IETF

The IEEE, or the Institute of Electrical and Electronics Engineers, is the organization responsible for setting many of the standards that govern wireless communication technologies. This includes the widely recognized 802.11 standards that outline the protocols for wireless local area networks (WLANs), which encompass various Wi-Fi technologies. The IEEE develops these standards through collaboration among professionals in the field, ensuring they are comprehensive and beneficial for industry and consumers alike. Other organizations such as ISO (International Organization for Standardization) and ANSI (American National Standards Institute) focus on broader standards and do not specifically specialize in wireless standards. The IETF (Internet Engineering Task Force) primarily concentrates on internet protocols and not on the wireless communication standards set forth by the IEEE. Therefore, the IEEE stands out as the key player in the development of wireless standards, making it the correct choice for this question.

2. What type of data is encoded using light?

A. Electrical signals

B. Radio waves

C. Fiber optic

D. Digital packets

The correct choice is fiber optic, as it pertains specifically to the transmission of data using light. Fiber optic technology uses thin strands of glass or plastic fibers to guide light signals over long distances. The data is transmitted as pulses of light, which are modulated to represent information. This method of data transmission offers significant advantages, including higher bandwidth capacity and reduced signal degradation compared to traditional electrical signals. When comparing fiber optic to other options, electrical signals involve the transmission of data through electrical impulses, typically found in copper cables. Radio waves are used for wireless communication technologies and involve the modulation of radio frequency signals, not light. Digital packets refer to units of data that are transmitted across networks, most commonly associated with data packets in IP networks, and do not specify the method of transmission. Thus, the unique characteristic of fiber optic technology is its reliance on light for encoding and transmitting data.

3. What is the primary purpose of a router in a network?

A. To connect multiple devices on the same local network

B. To transmit data on the same network segment

C. To direct data packets between different networks

D. To enhance signal strength in a network

The primary purpose of a router in a network is to direct data packets between different networks. This involves determining the best path for data to travel as it moves through various interconnected networks, which can include both local area networks (LANs) and wide area networks (WANs). Routers use routing tables and protocols to analyze packet destinations and make forwarding decisions, ensuring efficient communication between diverse network segments. While some of the other options might relate to networking concepts, they don't capture the essential role of a router. For instance, connecting multiple devices on the same local network is typically handled by switches rather than routers. Transmitting data on the same network segment is a function of network switches as well, focusing on local traffic instead of inter-network communication. Enhancing signal strength refers more to repeaters or amplifiers, which do not perform routing functions. Therefore, directing data packets between different networks encapsulates the core responsibility of a router in managing and facilitating network traffic across various domains.

4. 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.

5. What type of routing allows routers to automatically adjust to changes in the network?

A. Static routing

B. Dynamic routing

C. Manual routing

D. Policy-based routing

Dynamic routing is the type of routing that allows routers to automatically adjust to changes in the network. This adaptability is achieved through routing protocols that enable routers to communicate with each other, share routing information, and update their routing tables based on real-time network conditions. Dynamic routing protocols, such as OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol), detect changes in the network topology, such as a failed link or the addition of new routers, and respond accordingly. This capability ensures that data packets follow the most efficient path to their destination, which is essential for maintaining network reliability and performance as conditions change. In contrast, static routing requires manual configuration of routing tables, meaning any changes in the network must be addressed by manually updating those tables. Manual routing, similarly, suggests a hands-on approach with no automated adjustments, while policy-based routing focuses on traffic management based on predetermined policies rather than adapting to real-time changes.

6. What is the function of a DNS server?

A. To assign IP addresses dynamically

B. To translate domain names into IP addresses

C. To filter internet traffic

D. To manage network load

The primary function of a DNS (Domain Name System) server is to translate human-readable domain names, like www.example.com, into their corresponding numerical IP addresses, such as 192.0.2.1. This process is crucial because computers and networking equipment communicate using IP addresses, while users typically find it easier to remember domain names. By resolving domain names into IP addresses, DNS servers facilitate seamless access to websites and other online services without requiring users to remember specific numerical addresses. The ability of DNS servers to provide this translation is foundational to the functioning of the internet and various applications that depend on domain names. When a user enters a web address in their browser, the DNS server quickly translates that name into an IP address and directs the user to the appropriate resource on the internet. This process is essential for routing internet traffic efficiently and effectively. In contrast, other functionalities mentioned in the question serve different roles within a network. For instance, assigning IP addresses dynamically pertains to DHCP (Dynamic Host Configuration Protocol) rather than DNS. Filtering internet traffic is typically undertaken by firewalls or intrusion detection systems which manage security policies. Load management often falls to load balancers, which distribute incoming network traffic across multiple servers to ensure optimal performance and reliability. Thus, the role

7. What is the difference between TCP and UDP?

A. TCP is connectionless while UDP is connection-oriented

B. TCP ensures reliable delivery while UDP does not guarantee delivery

C. UDP is faster than TCP because it is more reliable

D. TCP is used for video streaming while UDP is used for emails

The distinction between TCP and UDP primarily revolves around reliability and connection characteristics. TCP, or Transmission Control Protocol, is known for its reliability features. It establishes a connection-oriented session between the sender and receiver, ensuring that data packets are delivered in the correct order and that lost packets are retransmitted. This makes it suitable for applications where data integrity and order are critical, such as file transfers and web browsing. In contrast, UDP, or User Datagram Protocol, operates as a connectionless protocol. It does not establish a connection prior to data transmission and does not ensure that packets are delivered reliably or in order. While this may lead to potential data loss during transmission, it allows for faster delivery of packets, making UDP a preferred choice for applications that can tolerate some data loss, such as streaming and online gaming. Understanding this fundamental difference helps in determining the appropriate protocol to use based on the requirements of the application being implemented. The focus on reliability in TCP versus the speed and efficiency of UDP is crucial in networking scenarios.

8. Which command prints a detailed listing of the device's interfaces including their MAC addresses?

A. show ip interface

B. show interface status

C. show running-config

D. show interfaces

The command that provides a detailed listing of a device's interfaces, including their MAC addresses, is "show interfaces." This command displays comprehensive information about each interface on the device, such as the interface's status (up or down), protocol status, hardware type, and MAC address, along with other metrics like bandwidth and error statistics. In contrast, other commands do not provide the same level of detail or specific information regarding MAC addresses. For example, the command for "show ip interface" focuses on IP-related information of the interfaces and does not include MAC addresses. "Show interface status" primarily gives a brief overview of the interfaces' operational status and capacities but lacks detailed MAC address information. Meanwhile, "show running-config" reveals the current configuration of the device but does not specifically focus on interface details or MAC addresses. Thus, "show interfaces" is the most comprehensive choice for this specific need.

9. Which command could provide information about IP addressing of all interfaces, including status and hardware addresses?

A. show ip interface brief

B. show interfaces

C. show ip route

D. show config

The command that provides information about IP addressing for all interfaces, including their statuses and hardware addresses, is indeed the one that starts with "show ip interface brief." This command summarizes the interface status and address information in a concise format. It displays details such as the IP address assigned to each interface, whether the interface is up or down, and the corresponding MAC (hardware) addresses. This command is especially valuable for network administrators who need a quick overview of the current state of the network interfaces without the overwhelming details that might come from other commands. It allows easy troubleshooting and monitoring of a device's interface configurations at a glance. In contrast, the other options serve different purposes. While "show interfaces" provides detailed information about each interface, including statistics and configurations, it does not summarize in the same straightforward manner. "Show ip route" focuses on the routing table rather than interface details, and "show config" displays the entire device configuration, which is much broader than just interface information.

10. 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

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!