Cisco Certified Network Associate (CCNA) 1 v7.0 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. 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 mechanism do routers use to prevent IPv4 packets from circulating endlessly in a network?**

   A. It discards packets based on their size

   B. It increments the TTL field by 1

   C. It decrements the value of the TTL field and discards packets if TTL reaches zero

   D. It reroutes packets back to the source

2. **How many bits are contained in an IPv6 address?**

   A. 64 bits

   B. 128 bits

   C. 32 bits

   D. 256 bits

3. **What is one primary use of a default static route in a router?**

   A. To filter traffic through a specified protocol.

   B. To forward packets to a specific destination when no other routes are known.

   C. To establish a manual connection to a firewall.

   D. To improve the speed of routing table lookups.

4. **How does a firewall contribute to network security?**

   A. By limiting user access to the network

   B. By controlling network traffic with security rules

   C. By encrypting network data

   D. By blocking all incoming traffic

5. **Which activity is a function of the transport layer in networking?**

   A. Routing packets between network devices

   B. Ensuring correct delivery of packets to the application

   C. Managing connections between different networks

   D. Ensuring web pages reach the correct browser window

6. Identify the subnet ID for the IPv6 address 2001:DA48:FC5:A4:3D1B::1/64.

A. 2001:DA48:FC5:A4:3D1B::/64

B. 2001:DA48:FC5:A4::/64

C. 2001:DA48:FC5:A4::1/64

D. 2001:DA48:FC5:A4:3D1B::/128

7. In which layer of the OSI model would you find the MAC address?

A. Application layer

B. Transport layer

C. Data Link layer

D. Network layer

8. What device is typically used to connect multiple computers within the same network segment?

A. Router

B. Hub

C. Switch

D. Modem

9. What occurs when a host does not have the MAC address but has the IP address of a destination device?

A. The host generates an ARP broadcast

B. The host sends a request to the server

C. The host ignores the packet

D. The host contacts the DHCP server

10. What is the primary purpose of Spanning Tree Protocol (STP) in networking?

A. Increase data transfer speed

B. Prevent network congestion

C. Manage active paths to prevent loops in Ethernet networks

D. Enhance wireless connectivity

Answers

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

Explanations

1. What mechanism do routers use to prevent IPv4 packets from circulating endlessly in a network?

A. It discards packets based on their size

B. It increments the TTL field by 1

C. It decrements the value of the TTL field and discards packets if TTL reaches zero

D. It reroutes packets back to the source

Routers utilize the Time to Live (TTL) field in an IPv4 packet to prevent packets from circulating endlessly within a network. Each IPv4 packet includes a TTL value that is set when the packet is created. As the packet traverses through routers, each router decrements this TTL value by one. When the TTL value reaches zero, the router recognizes that the packet has exceeded its allowed lifespan in the network and subsequently discards it. This mechanism serves as a safeguard against routing loops, where packets could otherwise be endlessly forwarded among routers without reaching their destination. By discarding packets that have become too old, the network is protected from unnecessary traffic and potential congestion, maintaining overall network performance and efficiency.

2. How many bits are contained in an IPv6 address?

A. 64 bits

B. 128 bits

C. 32 bits

D. 256 bits

An IPv6 address consists of 128 bits, which allows for a vastly larger number of unique addresses compared to its predecessor, IPv4. This extended length is crucial for accommodating the growing number of devices connecting to the internet and helps ensure a sufficient address space for the foreseeable future. IPv6 is structured in such a way that its 128 bits are typically represented as eight groups of four hexadecimal digits, each group separated by colons. This format not only simplifies the representation of the address but also facilitates easier configuration and management of devices within networks. The adoption of IPv6 is primarily driven by the exhaustion of IPv4 addresses, emphasizing the importance of its extended bit length to support a more expansive internet landscape.

3. What is one primary use of a default static route in a router?

A. To filter traffic through a specified protocol.

B. To forward packets to a specific destination when no other routes are known.

C. To establish a manual connection to a firewall.

D. To improve the speed of routing table lookups.

A default static route is primarily used to forward packets to a specific destination when no other routes are known. This type of route acts as a catch-all pathway for traffic that doesn't match any specific routes in the routing table. When a router receives a packet destined for an address not explicitly listed in its routing table, it can use the default static route to send that packet to a predetermined next hop or interface. This ensures that packets can still be routed even if there are no specific entries for them, thus providing a pathway for traffic to reach destinations outside of the local network or to unknown remote networks. The other choices do not accurately represent the function of a default static route. Filtering traffic through a specified protocol is more related to access control lists (ACLs) rather than routing itself. Establishing a manual connection to a firewall doesn't align with the default route's purpose, as it pertains more to network security configurations. Improving the speed of routing table lookups involves different optimization techniques but isn't directly relevant to the role of a default static route. Therefore, the function of forwarding packets without known routes is what makes the default static route essential in network design.

4. How does a firewall contribute to network security?

A. By limiting user access to the network

B. By controlling network traffic with security rules

C. By encrypting network data

D. By blocking all incoming traffic

A firewall plays a critical role in network security primarily by controlling network traffic with security rules. These rules define which types of traffic are allowed to enter or exit the network, providing a protective barrier against unauthorized access, threats, and attacks. The secure management of traffic is fundamental because it enables organizations to permit legitimate communications while blocking potentially harmful data packets based on specific criteria such as source and destination IP addresses, protocol types, and port numbers. This level of control allows for tailored security strategies that can adapt to the organization's needs and threat landscape. In contrast to controlling traffic, other functions mentioned in the options do not entirely capture the comprehensive role of a firewall in security. While limiting user access might suggest managing permissions, the firewall's primary function is not about user authentication or access rights but rather about monitoring and filtering traffic at the network boundary. Encryption of network data relates to securing the information being transmitted, which is not a direct function of firewall systems, while blocking all incoming traffic would be overly restrictive and detrimental to normal business operations, as it would impede all legitimate external communications. Therefore, controlling network traffic with security rules is the key way in which a firewall enhances overall network security.

5. Which activity is a function of the transport layer in networking?

A. Routing packets between network devices

B. Ensuring correct delivery of packets to the application

C. Managing connections between different networks

D. Ensuring web pages reach the correct browser window

The function of the transport layer in networking primarily focuses on providing end-to-end communication services for applications. This includes ensuring that data is delivered reliably and in the correct order, as well as managing the flow of data to prevent congestion. Among the options provided, ensuring web pages reach the correct browser window aligns with the transport layer's responsibility of delivering the data to the appropriate application. The transport layer uses protocols like TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) to facilitate this process. TCP, for instance, establishes a connection between the client and server, ensuring that the web page data transferred is accurately delivered to the web browser application on the client side. The other options mainly pertain to different layers of the networking model. For example, routing packets between network devices is a function of the network layer, while managing connections between different networks and ensuring correct delivery of packets to the application also involve different layers in the OSI model. Thus, the correct answer highlights the transport layer's role in communicating with the application directly, ensuring that the information requested by the web browser is precisely transmitted.

6. Identify the subnet ID for the IPv6 address 2001:DA48:FC5:A4:3D1B::1/64.

A. 2001:DA48:FC5:A4:3D1B::/64

B. 2001:DA48:FC5:A4::/64

C. 2001:DA48:FC5:A4::1/64

D. 2001:DA48:FC5:A4:3D1B::/128

In this scenario, the task is to determine the subnet ID from the given IPv6 address, 2001:DA48:FC5:A4:3D1B::1/64. The key element to understand here is how IPv6 subnetting works, specifically in relation to the prefix length indicated by the "/64". The prefix length "/64" means that the first 64 bits of the address are used to define the network portion or the subnet ID. In the address 2001:DA48:FC5:A4:3D1B::1, the subnet part consists of the first four blocks, which are represented as 2001:DA48:FC5:A4. The '3D1B' and the rest of the address (the '::1' part) represents the host portion. Thus, when truncated to just the network part with the /64 prefix, the subnet ID is indeed 2001:DA48:FC5:A4::/64. This representation indicates that all addresses in this subnet will share these first four blocks, while the latter parts can be varied to specify different hosts within the same network. In contrast, the other options deviate in ways that misunderstand the structure

7. In which layer of the OSI model would you find the MAC address?

A. Application layer

B. Transport layer

C. Data Link layer

D. Network layer

The MAC address is located in the Data Link layer of the OSI model. This layer is responsible for node-to-node data transfer and handles the physical addressing of devices on a local network. Each device on a network interface has a unique MAC address, which allows for the identification of devices at the data link level. The Data Link layer is crucial for establishing communication between devices on the same local area network (LAN). It ensures that data frames are transferred effectively over the physical medium while managing access to that medium. By using MAC addresses, the Data Link layer facilitates the delivery of frames to the correct devices within the local network. In contrast, the Application layer is focused on providing network services directly to end-user applications, while the Transport layer is concerned with ensuring complete data transfer and error recovery between hosts. The Network layer is responsible for path determination and logical addressing, such as IP addresses, but it does not handle the physical or MAC addresses associated with devices in a LAN.

8. What device is typically used to connect multiple computers within the same network segment?

A. Router

B. Hub

C. Switch

D. Modem

The device typically used to connect multiple computers within the same network segment is a switch. Switches operate at the data link layer (Layer 2) of the OSI model and are designed to forward data packets between devices on the same local area network (LAN). When a switch receives a data packet, it examines the MAC (Media Access Control) addresses contained within the packet to determine its destination. It then forwards the packet only to the specific device that needs it, rather than sending it to all connected devices. This efficient method of communication reduces network congestion and improves overall performance compared to older devices like hubs, which broadcast incoming data packets to all ports regardless of the intended recipient. In a typical LAN setup, switches facilitate direct communication between computers, printers, and servers, enabling them to share resources with minimal delay. This functionality is crucial in modern networking environments to ensure that devices can communicate quickly and effectively within the same network segment.

9. What occurs when a host does not have the MAC address but has the IP address of a destination device?

A. The host generates an ARP broadcast

B. The host sends a request to the server

C. The host ignores the packet

D. The host contacts the DHCP server

When a host has an IP address for a destination device but does not have the corresponding MAC address, the host must determine that MAC address in order to send frames at the data link layer. This process is managed through the Address Resolution Protocol (ARP). To resolve the MAC address, the host generates an ARP broadcast. This broadcast is sent to all devices on the network segment, asking "Who has IP address X.X.X.X? Tell me your MAC address." The device that owns that IP address replies with its MAC address, allowing the originating host to build the necessary Ethernet frame for communication. This method is essential because the Internet Protocol operates at the network layer, where it uses IP addresses, while MAC addresses are used at the data link layer for actual frame delivery. Therefore, an ARP broadcast is a standard mechanism that facilitates the mapping of IP addresses to MAC addresses crucial for communication on a local network.

10. What is the primary purpose of Spanning Tree Protocol (STP) in networking?

A. Increase data transfer speed

B. Prevent network congestion

C. Manage active paths to prevent loops in Ethernet networks

D. Enhance wireless connectivity

The primary purpose of Spanning Tree Protocol (STP) in networking is to manage active paths to prevent loops in Ethernet networks. In a network that implements multiple switches with redundant links, there is a risk of creating loops, which can cause broadcast storms, multiple frame copies, and ultimately lead to network congestion and downtime. STP functions by identifying the redundant paths in the network and placing some of them in a blocking state, ensuring that there is a single active path between any two network devices. This protocol works by using a tree structure to determine the optimal paths, and it actively monitors network changes. When a primary link fails, STP can activate a previously blocked link, thereby maintaining network connectivity without creating loops. The strength of STP lies in its ability to dynamically adapt and maintain a loop-free network topology, promoting stability in Ethernet-based networks. In contrast, increasing data transfer speed, preventing network congestion, and enhancing wireless connectivity do not directly pertain to the core function of STP, as its main role is specifically focused on loop prevention and path management within switched Ethernet networks.

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://ccna1v7.examzify.com

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