

CCNA Introduction to Networks (ITN) Practice Test (Sample)

Study Guide



Everything you need from our exam experts!

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.

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

SAMPLE

- 1. What is a function of NAT in IPv4 networks?**
 - A. To verify and encrypt data during transmission**
 - B. To translate private IP addresses to public IP addresses**
 - C. To increase the speed of the network**
 - D. To provide firewall capabilities**

- 2. An organization is assigned an IPv6 address block of 2001:db8:0:ca00::/56. How many subnets can be created without using bits in the interface ID space?**
 - A. 128**
 - B. 256**
 - C. 512**
 - D. 1024**

- 3. Which tool would a technician use to trace the path that a packet takes through a network?**
 - A. ping**
 - B. nslookup**
 - C. tracert**
 - D. netstat**

- 4. What is the consequence of configuring a router with the ipv6 unicast-routing command?**
 - A. Interfaces become disabled**
 - B. Only IPv4 traffic is allowed**
 - C. ICMPv6 Router Advertisement messages are sent**
 - D. Routing tables become inaccessible**

- 5. A user sends an HTTP request to a web server on a remote network. During encapsulation for this request, what information is added to the address field of a frame to indicate the destination?**
 - A. The IP address of the web server**
 - B. The MAC address of the client**
 - C. The MAC address of the default gateway**
 - D. The hostname of the web server**

- 6. What is one primary function of the data link layer?**
- A. Routes data between networks**
 - B. Provides for the exchange of frames over a common local media**
 - C. Encrypts data for security**
 - D. Establishes a session between devices**
- 7. In the context of addressing, what does "host address" refer to?**
- A. The unique identifier for a device on a network**
 - B. The address of a network device's manufacturer**
 - C. The gateway's IP address within a local network**
 - D. The broadcast address for a subnet**
- 8. Why would a Layer 2 switch need an IP address?**
- A. To enable the switch to be managed remotely**
 - B. To improve data throughput**
 - C. To enhance physical security**
 - D. To serve as a firewall**
- 9. What is a function of a router in a network?**
- A. To store data files**
 - B. To connect different networks and route packets**
 - C. To manage network security**
 - D. To provide hardware for internet access**
- 10. Which statements accurately describe advantages or disadvantages of deploying NAT for IPv4? (Choose two.)**
- A. NAT helps slow down IPv4 address depletion**
 - B. NAT improves the speed of local connections**
 - C. NAT introduces issues for some applications requiring end-to-end connectivity**
 - D. NAT requires additional hardware to function effectively**

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is a function of NAT in IPv4 networks?

- A. To verify and encrypt data during transmission
- B. To translate private IP addresses to public IP addresses**
- C. To increase the speed of the network
- D. To provide firewall capabilities

One of the main functions of Network Address Translation (NAT) in IPv4 networks is to translate private IP addresses to public IP addresses. This is crucial because IPv4 addresses are limited, and many devices in a local network can use private IP addresses that are not routable on the internet. When a device with a private IP address wants to communicate with external networks, NAT translates its private IP address into a public IP address. This process allows multiple devices on a local network to share a single public IP address, facilitating access to the internet while preserving the limited public IP address space. Additionally, NAT provides an added layer of security by masking internal IP addresses, making it harder for external entities to directly access devices in a private network. This translation process is essential for enabling connectivity for devices that do not have their own public IP addresses. While NAT does not provide direct security features like a firewall does, its function in address translation is critical for the effective operation of modern IPv4 networks.

2. An organization is assigned an IPv6 address block of 2001:db8:0:ca00::/56. How many subnets can be created without using bits in the interface ID space?

- A. 128
- B. 256**
- C. 512
- D. 1024

To determine how many subnets can be created from the given IPv6 address block of 2001:db8:0:ca00::/56 without using bits in the interface ID space, we first need to analyze the allocation of bits within the address structure. An IPv6 address consists of 128 bits in total. In a /56 subnet, the first 56 bits of the address are designated for the network portion, leaving the remaining 72 bits for subnets and the interface ID. However, since we are tasked with creating subnets without using bits from the interface ID space, we focus solely on the bits available for subnets within the provided prefix. In the case of a /56 prefix, the first 56 bits define the network, and we have the ability to manipulate the following bits for subnetting. Specifically, we have 8 bits left for creating subnets (from the 57th to the 64th bit). To calculate the number of possible subnets, we take the number of bits available for the subnetting, which is 8 bits. Using the formula 2^n (where n is the number of bits allocated for subnetting), we find: $2^8 = 256$.

3. Which tool would a technician use to trace the path that a packet takes through a network?

- A. ping**
- B. nslookup**
- C. tracert**
- D. netstat**

The correct answer involves the use of a specific tool known for its ability to track the journey of packets through different routers and network devices in a given network. This tool sends out packets from a source and records the intermediate hops, allowing users to see each router's IP address along the way, as well as the round-trip time for packets to reach those routers. This capability is vital for diagnosing network issues, such as where delays or failures may be occurring within the path to a destination. Users can interpret the resulting output to identify specific problems in the network path, including potential misconfigurations or connectivity issues. The "ping" tool, while useful for checking the reachability of a host, simply measures round-trip time to a specified destination and does not provide details about the intermediary hops taken by the packets. Similarly, "nslookup" is focused solely on querying domain name system (DNS) to obtain information about hostnames or IP addresses, and does not perform any tracing of packet routes across a network. "Netstat" serves a different purpose, providing information about active connections, routing tables, interface statistics, and more on the local device, but does not trace packet paths like the tool in question does. Thus, the tool used to effectively trace

4. What is the consequence of configuring a router with the ipv6 unicast-routing command?

- A. Interfaces become disabled**
- B. Only IPv4 traffic is allowed**
- C. ICMPv6 Router Advertisement messages are sent**
- D. Routing tables become inaccessible**

Configuring a router with the ipv6 unicast-routing command enables IPv6 routing on the device. This command specifically activates the capability for the router to forward IPv6 packets and is essential for establishing IPv6 connectivity. Once activated, the router can begin to send and receive IPv6 traffic, including handling ICMPv6 Router Advertisement messages. ICMPv6 messages play a crucial role in IPv6 networks, particularly for Neighbor Discovery. Router Advertisement messages are sent from routers to inform nearby devices of their presence and to provide them with the necessary information to configure their IPv6 addresses and discover other parameters like the default gateway. Thus, with the invocation of the ipv6 unicast-routing command, the router starts participating in IPv6 networking, facilitating communication and facilitating address configuration processes in the network. This capability becomes vital in ensuring that devices on the network can communicate with each other using IPv6, which is increasingly important as the industry transitions from IPv4.

5. A user sends an HTTP request to a web server on a remote network. During encapsulation for this request, what information is added to the address field of a frame to indicate the destination?

- A. The IP address of the web server**
- B. The MAC address of the client**
- C. The MAC address of the default gateway**
- D. The hostname of the web server**

In this scenario, when a user sends an HTTP request, the encapsulation process involves several layers of communication. At the data link layer, frames are created to transport packets across a local area network (LAN). Within each frame, the destination address needs to be specified for the data to reach its intended endpoint. The information added to the address field of the frame corresponds to the MAC address of the device that will receive the frame over the local network segment. In typical network configurations, if the destination is outside the local network, the frame will be sent to the default gateway. The default gateway acts as an intermediary to forward traffic to other networks. Thus, the frame's destination address will contain the MAC address of the default gateway, allowing the original device's frame to be directed appropriately. The other options do not pertain directly to the addressing required for the encapsulation of the frame in this context. The IP address of the web server is relevant at the network layer but is not used at the data link layer for framing purposes. The MAC address of the client references the source device and is not what needs to be added for the destination. Finally, the hostname is a human-readable label and does not serve a role in the hardware addressing needed for the

6. What is one primary function of the data link layer?

- A. Routes data between networks**
- B. Provides for the exchange of frames over a common local media**
- C. Encrypts data for security**
- D. Establishes a session between devices**

One primary function of the data link layer is to provide for the exchange of frames over a common local media. The data link layer is responsible for the encapsulation of network layer packets into frames and controlling how these frames are placed on the physical media. It facilitates communication between devices on the same local area network (LAN) by managing the access to the physical medium and ensuring that data is transmitted without errors. This layer ensures that the data is correctly framed for transmission and that the receiving device knows how to interpret it. Additionally, the data link layer handles physical addressing through MAC (Media Access Control) addresses, allowing devices to identify and communicate with each other within the same network segment. It also implements error detection and, in some cases, correction methods to ensure data integrity during transfer. This focus on local communication and frame management is what distinguishes the data link layer's primary function in the networking model.

7. In the context of addressing, what does "host address" refer to?

- A. The unique identifier for a device on a network**
- B. The address of a network device's manufacturer**
- C. The gateway's IP address within a local network**
- D. The broadcast address for a subnet**

The term "host address" refers specifically to the unique identifier assigned to a device on a network. Each device that connects to a network requires a distinct address to facilitate communication with other devices. This unique identifier is essential for routing packets of data to and from devices, ensuring that information reaches the correct destination. In IP networking, a host address is part of the larger IPv4 or IPv6 address and allows for the identification and differentiation of devices within the same network or across interconnected networks. In contrast, the other options do not accurately represent what a host address is. The address of a network device's manufacturer pertains to the hardware and is often referenced as the MAC (Media Access Control) address, which serves a different purpose. The gateway's IP address is crucial for routing traffic outside a local network, but it is not the address of an individual host. Lastly, the broadcast address of a subnet is used to communicate with all devices on that subnet simultaneously, rather than identifying a specific host. Thus, the concept of a host address is fundamentally about distinguishing each device on a network, making it essential for effective networking.

8. Why would a Layer 2 switch need an IP address?

- A. To enable the switch to be managed remotely**
- B. To improve data throughput**
- C. To enhance physical security**
- D. To serve as a firewall**

A Layer 2 switch requires an IP address primarily to enable remote management. When a switch is configured with an IP address, network administrators can access its management interface, usually through SSH or HTTP/S protocols. This remote access facilitates monitoring, configuring settings, and troubleshooting without needing to be physically present at the switch's location. In many network setups, if a switch needs to be managed, especially in larger or more complex environments, having an IP address is essential to facilitate this level of interaction. This capability supports features such as SNMP (Simple Network Management Protocol), which provides management information for monitoring network devices. Improving data throughput, enhancing physical security, and serving as a firewall do not directly relate to the IP functionality of a Layer 2 switch. The primary role of a Layer 2 switch is to forward frames within the same local area network based on MAC addresses, not to perform higher-level functions like routing or packet filtering that require an IP address. Thus, the main reason that a Layer 2 switch would need an IP address is for remote management purposes.

9. What is a function of a router in a network?

- A. To store data files
- B. To connect different networks and route packets**
- C. To manage network security
- D. To provide hardware for internet access

A router serves a crucial role in networking by connecting different networks and routing packets of data between them. This function allows devices on separate networks (for example, two different local area networks) to communicate with each other effectively. When a router receives data packets, it evaluates the destination IP address and determines the best path for the packet to take through the network, ensuring that it reaches its intended destination efficiently. The router uses routing protocols and algorithms to make decisions on how to forward packets, which might involve passing through multiple routers before reaching the final destination. This capability is essential for the functioning of the internet, where diverse networks with different configurations need to interconnect smoothly. While other options mention important network functions, they do not accurately describe the primary role of a router. For instance, the task of storing data files is typically associated with servers or storage devices, managing network security is often the responsibility of firewalls or security appliances, and providing hardware for internet access is typically the role of a modem or a gateway rather than a router itself. Hence, the specific function of packets routing between different networks distinctly highlights why the router is essential in a network environment.

10. Which statements accurately describe advantages or disadvantages of deploying NAT for IPv4? (Choose two.)

- A. NAT helps slow down IPv4 address depletion**
- B. NAT improves the speed of local connections
- C. NAT introduces issues for some applications requiring end-to-end connectivity
- D. NAT requires additional hardware to function effectively

The statement that NAT helps slow down IPv4 address depletion is indeed correct. Network Address Translation (NAT) allows multiple devices on a local network to share a single public IP address. By enabling several devices to connect to the internet using one address, NAT effectively extends the lifespan of the IPv4 address space. This is particularly valuable in a time when the number of available IPv4 addresses is limited, as it reduces the demand for multiple public IP addresses for every device in a local network, thereby alleviating some of the pressure on the overall pool of available IPv4 addresses. While other choices touch on the potential impacts of NAT, they do not demonstrate the same fundamental benefit that deploying NAT provides against address depletion.

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://ccnaintrotonetworks.examzify.com>

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

SAMPLE