AP NETWORKING PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://apnetworking.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 15

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. DRM stands for which of the following?

A. Digital Rights Management

B. Information Rights Management

C. Content Addressable Memory

D. Administrative controls

2. What is the fixed length of an IPv6 header?

A. 60 bytes

B. 40 bytes

C. 20 bytes

D. 128 bytes

3. Recovery Controls

A. They block all access to the network during an incident

B. Recovery controls work with corrective to bring back to normal state

C. They encrypt data to prevent theft

D. They provide user authentication for logins

4. Which description correctly contrasts stateful and stateless firewalls?

A. Stateful firewalls track connection state and context; stateless firewalls apply rules per packet without maintaining connection state.

B. Stateful firewalls apply rules per packet; stateless firewalls track connection state.

C. Both types track connection state equally; the difference is only vendor terminology.

D. Stateless firewalls provide stronger security by default and track all connections.

5. What is the PDU of the Application Layer?

A. segments

B. data

C. frames

D. packets

SAMPLE

6. Which layer controls the way messages are sent on the physical media and manages framing, error control, and media access?

A. Physical Layer

B. Data Link Layer

C. Network Layer

D. Transport Layer

7. What is the primary function of a router?

A. Encrypts data at the application layer

B. Directs traffic between networks

C. Provides wireless access

D. Translates domain names

8. Which statement correctly compares IPv4 and IPv6 headers in terms of address length and header structure?

A. IPv4 headers typically 20 bytes minimum with 32-bit addresses; IPv6 headers are fixed at 40 bytes with 128-bit addresses; IPv6 uses extension headers to carry options.

B. IPv4 uses 128-bit addresses and a 40-byte header.

C. IPv6 headers are variable length and do not have extension headers.

D. IPv4 headers are 60 bytes minimum and use 64-bit addresses.

9. What problem does Spanning Tree Protocol (STP) address in a LAN?

A. STP prevents Layer 2 loops by creating a loop-free tree topology and blocking redundant paths.

B. STP encrypts data across the local network to prevent eavesdropping.

C. STP assigns IP addresses automatically to devices on the network.

D. STP manages VLAN tagging across switches.

10. In a router, where are the routes to network destinations stored?

A. DNS cache of domain name mappings

B. MAC address table

C. routing table

D. ARP cache

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. DRM stands for which of the following?

A. Digital Rights Management

B. Information Rights Management

C. Content Addressable Memory

D. Administrative controls

DRM stands for Digital Rights Management. This term refers to a set of technologies and policies that control how digital content can be accessed, used, copied, and distributed, helping copyright holders enforce licensing terms and prevent unauthorized sharing across devices and platforms. The other options point to different concepts—Information Rights Management is a related but distinct term often used in enterprise document security, Content Addressable Memory is a hardware memory concept, and Administrative controls are general security measures not specific to protecting digital content. In practical use, DRM mechanisms enforce usage rights, such as restricting playback to authorized devices or limiting the number of copies, which is why Digital Rights Management is the correct expansion.

2. What is the fixed length of an IPv6 header?

A. 60 bytes

B. 40 bytes

C. 20 bytes

D. 128 bytes

IPv6 uses a fixed-size base header of 40 bytes. This comes from how the header is laid out: the first 4 bytes carry Version, Traffic Class, and Flow Label; then 2 bytes for Payload Length; 1 byte for Next Header; 1 byte for Hop Limit; and 16 bytes each for the Source and Destination addresses. Since there is no header-length field like in IPv4, the base header does not vary in size. If extra information is needed, it's carried in extension headers that follow after this 40-byte header. So the fixed length of the IPv6 header is 40 bytes.

3. Recovery Controls

A. They block all access to the network during an incident

B. Recovery controls work with corrective to bring back to normal state

C. They encrypt data to prevent theft

D. They provide user authentication for logins

Recovery controls are actions used to restore normal operations after an incident. They focus on getting systems and services back online, restoring data, and returning the business to a functioning state as quickly as possible. They work with corrective controls, which address the root cause and prevent recurrence, so together they not only fix what happened but also bring the environment back to normal. The other options describe steps taken during an incident (blocking access) or protective measures (encryption, authentication) rather than the process of returning to normal operations.

SAMPLE

4. Which description correctly contrasts stateful and stateless firewalls?

A. Stateful firewalls track connection state and context; stateless firewalls apply rules per packet without maintaining connection state.

B. Stateful firewalls apply rules per packet; stateless firewalls track connection state.

C. Both types track connection state equally; the difference is only vendor terminology.

D. Stateless firewalls provide stronger security by default and track all connections.

The key idea here is the difference in how each firewall handles traffic. A stateful firewall keeps track of active connections and the context of those connections (the state). It builds a state table that monitors how a conversation starts, progresses, and ends, so decisions can be made with knowledge of the session as a whole. A stateless firewall, on the other hand, makes decisions based on each individual packet without remembering any past packets or the larger connection context. This description is the best because it directly captures that distinction: stateful firewalls monitor connection state and context, while stateless firewalls evaluate packets in isolation without maintaining a connection state. For example, with a stateful firewall, the return packets for an outbound request are allowed because the firewall already knows there's an active connection. A stateless firewall wouldn't rely on that context and would require explicit rules for each packet, making it less capable of handling legitimate ongoing connections with minimal rule sets. The other options misstate the relationship. Saying both track connection state equally ignores the fundamental difference in how each one handles traffic. Claiming it's just vendor terminology isn't accurate because the behavior of maintaining state versus not maintaining state is a real architectural distinction. Saying stateless provides stronger security by default and tracks all connections is not correct because stateless firewalls don't track connections at all; their security model is based on per-packet decisions rather than session context.

5. What is the PDU of the Application Layer?

A. segments

B. data

C. frames

D. packets

The thing being carried at the Application Layer is the actual user data—the message produced by the application, such as an HTTP request, email body, or file content. That data is handed down to the Transport Layer, which adds its own header and creates a segment (for TCP) or a datagram (for UDP). As it moves downward, each layer adds headers, turning the data into a packet at the Network Layer, a frame at the Data Link Layer, and finally bits at the Physical Layer. So the PDU at the Application Layer is data—the payload from the application. The other terms describe PDUs created by lower layers (segments by Transport, frames by Data Link, packets by Network).

SAMPLE

6. Which layer controls the way messages are sent on the physical media and manages framing, error control, and media access?

A. Physical Layer

B. Data Link Layer

C. Network Layer

D. Transport Layer

The Data Link Layer is in charge of moving data across a single link between two directly connected nodes. It handles framing, which means it packages network-layer data into frames with addresses and control information. It provides error detection within those frames (using a frame check sequence) to notice if something went wrong on the link. It also governs how devices access the shared medium, using MAC protocols to decide who can transmit and when. This layer sits between the Physical Layer, which actually sends the raw bits, and the Network Layer, which handles routing across networks. While the Physical Layer focuses on signaling and hardware, and the Network and Transport Layers handle end-to-end delivery and routing, the Data Link Layer ties it together on a local link with framing, error detection, and access control.

7. What is the primary function of a router?

A. Encrypts data at the application layer

B. Directs traffic between networks

C. Provides wireless access

D. Translates domain names

The key idea here is routing traffic between networks. A router looks at the destination IP address on each packet, uses its routing table to decide the next hop, and forwards the packet toward its destination. This is the network layer function that lets devices on separate networks—such as different LANs or a LAN and the internet—communicate with each other. Routers determine the best paths using routing protocols like OSPF, RIP, or BGP, and they adapt as network conditions change. While a router can also perform additional tasks like NAT or firewalling, those are supplementary; the primary role is directing traffic between networks. Encryption at the application layer happens with protocols like TLS, wireless access is provided by an access point or wireless router, and translating domain names is the job of DNS.

8. Which statement correctly compares IPv4 and IPv6 headers in terms of address length and header structure?

A. IPv4 headers typically 20 bytes minimum with 32-bit addresses; IPv6 headers are fixed at 40 bytes with 128-bit addresses; IPv6 uses extension headers to carry options.

B. IPv4 uses 128-bit addresses and a 40-byte header.

C. IPv6 headers are variable length and do not have extension headers.

D. IPv4 headers are 60 bytes minimum and use 64-bit addresses.

The key idea is how address length and header structure differ between IPv4 and IPv6. IPv4 uses 32-bit addresses, and its header can be as small as 20 bytes. The IPv4 header length can grow up to 60 bytes to accommodate options, but the minimum is 20. IPv6, on the other hand, uses 128-bit addresses to support a vastly larger address space, and its base header is fixed at 40 bytes. If additional information is needed, IPv6 doesn't pack options into the main header; instead, it uses separate extension headers to carry options or additional features. This combination—short, fixed-size base header with a large address space and extension headers for options—matches the stated description. The other choices misstate the address sizes, header sizes, or how options are carried.

SAMPLE

9. What problem does Spanning Tree Protocol (STP) address in a LAN?

A. STP prevents Layer 2 loops by creating a loop-free tree topology and blocking redundant paths.

B. STP encrypts data across the local network to prevent eavesdropping.

C. STP assigns IP addresses automatically to devices on the network.

D. STP manages VLAN tagging across switches.

STP addresses the problem of Layer 2 loops in a LAN. When multiple switches are interconnected, redundant paths can create situations where frames loop endlessly, causing broadcast storms, MAC table instability, and overall network disruption. STP prevents this by electing a root bridge and then building a loop-free tree topology: for each network segment, only one forwarding path is active, while other potential paths are placed in a blocking state. This stops loops while still allowing redundancy to be used if a link fails—blocked ports can re-enable to maintain connectivity. It's important to note that STP is not about encryption, automatic IP addressing, or VLAN tagging; those are separate functions.

10. In a router, where are the routes to network destinations stored?

A. DNS cache of domain name mappings

B. MAC address table

C. routing table

D. ARP cache

Routing decisions in a router are made using the routing table. The routing table contains destination network prefixes, the next-hop or exit interface to reach those networks, and metrics that help choose among multiple paths. When a packet arrives, the router finds the most specific match for the destination IP (the longest-prefix match) and forwards the packet toward the indicated next hop or out the specified interface. This table is built from static routes you configure or from dynamic routing protocols that learn routes from neighbors. The other caches and tables serve different purposes: the ARP cache maps IP addresses to MAC addresses on the local network to deliver frames locally; the MAC address table on a switch associates MAC addresses with switch ports for layer-2 forwarding; the DNS cache stores domain name to IP mappings for name resolution, not for routing decisions.

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://apnetworking.examzify.com

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

SAMPLE