AP Networking 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. Which term describes hardware or software implemented to manage and provide protection?

A. Technical Controls

B. Detective controls

C. Preventative Controls

D. Physical control

2. Which control is designed to protect facilities, systems, and resources and separate people physically from systems?

A. Detective controls

B. Administrative controls

C. Physical control

D. CAM

3. What is the PDU of the physical layer?

A. bytes

B. frames

C. bits

D. packets

4. Which statement describes a Wide Area Network (WAN)?

A. Wide Area Network a network that spans a large geographical area.

B. Local Area Network inside a room.

C. Wireless Local Area Network for campus.

D. Virtual Private Network across insecure channels.

5. Disaster recovery planning is typically part of which category of security controls?

A. Physical controls

B. Administrative controls

C. Detective controls

D. Technical Controls

6. data path

- **A. The software protocol used to route data**
- **B. The aggregated data rate across a network**
- **C. The encryption path used for secure communications**
- **D. The specific sequence of devices and physical links that a packet follows from a source to a destination**

7. Which topology combines characteristics of more than one simple physical topology?

- **A. Hybrid Topology**
- **B. Star Topology**
- **C. Bus Topology**
- **D. Mesh Topology**

8. Which topology has one central node that all devices connect to, with data first going into the central node?

- **A. Hybrid Topology**
- **B. Star Topology**
- **C. Mesh Topology**
- **D. Bus Topology**

9. Which statement correctly characterizes fiber optic cabling?

- **A. Twisted pair uses copper and is low cost.**
- **B. Coaxial cable uses copper and shielding.**
- **C. Fiber optic uses light (glass or plastic) and is not interfered by electrical signals; high cost.**
- **D. Wireless networks use radio waves.**

10. What does HTTPS stand for?

- **A. Hyper Text Transfer Protocol Secure**
- **B. Hyper Text Transfer Protocol**
- **C. Secure Hyper Text Transfer Protocol**
- **D. Hyper Transfer Protocol Secure**

Answers

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

Explanations

1. Which term describes hardware or software implemented to manage and provide protection?

A. Technical Controls

B. Detective controls

C. Preventative Controls

D. Physical control

Technical controls are safeguards implemented with hardware or software to protect information systems and manage access to resources. They include firewalls, encryption, antivirus programs, intrusion prevention or detection systems, and access control mechanisms. These are distinct from physical controls like locks or cameras, and from detective controls that monitor for breaches after they happen. While many technical controls also help prevent incidents, what sets them apart is that they are technology-based protections that actively enforce security policies and protect data.

2. Which control is designed to protect facilities, systems, and resources and separate people physically from systems?

A. Detective controls

B. Administrative controls

C. Physical control

D. CAM

Physical control focuses on physically preventing access to facilities, systems, and resources. It creates tangible barriers—locked doors, fences, security guards, turnstiles, secure rooms, and access-controlled entry—that separate people from the assets they're trying to reach. By placing a physical barrier between individuals and the systems, it reduces the chance of unauthorized interaction before anything happens. Detective controls and administrative controls deal with monitoring events after they occur or governing behavior through policies and procedures, respectively, while CAM doesn't address physical separation.

3. What is the PDU of the physical layer?

A. bytes

B. frames

C. bits

D. packets

The important idea is that each layer defines its own unit of data to pass to the layer below. At the physical layer, the data being transmitted is the raw bitstream. The hardware and signals on the medium carry individual bits (0s and 1s) as electrical, optical, or radio signals, and the physical layer's job is to turn the higher-layer data into that continuous stream of bits and back again. Because of that, the PDU for the physical layer is bits. Frames belong to the data link layer, which adds headers and trailers to create a complete frame for transmission. Packets belong to the network layer, where data is wrapped with network addressing and routing information. Bytes are a storage or representation unit, not the PDU at the physical layer, since the physical layer deals with continuing bit sequences rather than structured packets or frames.

4. Which statement describes a Wide Area Network (WAN)?

A. Wide Area Network a network that spans a large geographical area.

B. Local Area Network inside a room.

C. Wireless Local Area Network for campus.

D. Virtual Private Network across insecure channels.

A Wide Area Network is defined by spanning a large geographical area and linking multiple smaller networks, such as several LANs, over long distances. It uses various transmission methods (leased lines, fiber, satellite, or the public Internet) and is often provided or managed by service providers to connect cities, regions, or countries. This breadth sets it apart from a Local Area Network, which is confined to a building or a single location; a Wireless Local Area Network describes wireless coverage within a campus or facility, and a Virtual Private Network is a secure method for connecting across insecure networks rather than describing the WAN itself. So the statement that describes a WAN is that it spans a large geographical area.

5. Disaster recovery planning is typically part of which category of security controls?

A. Physical controls

B. Administrative controls

C. Detective controls

D. Technical Controls

Disaster recovery planning is a management activity that establishes policies, plans, roles, and procedures to restore operations after a disruption. This fits administrative controls because these controls govern how the organization is managed—covering governance, risk management, incident response planning, and business continuity efforts. It's not about securing the physical environment, detecting incidents, or implementing a technology-based safeguard, which are the realms of physical, detective, and technical controls respectively.

6. data path

A. The software protocol used to route data

B. The aggregated data rate across a network

C. The encryption path used for secure communications

D. The specific sequence of devices and physical links that a packet follows from a source to a destination

Data path is the specific sequence of devices and physical links that a packet follows from a source to a destination. It's the actual route the data takes through the network—each hop through switches and routers and the links connecting them. Routing decisions determine which path is chosen, and the data path is the realized path that packets traverse, which is why it directly affects latency and reliability. In practice, you can observe the data path with tools like traceroute, which reveals the hop-by-hop route from sender to receiver. The other descriptions describe related ideas but not the route itself: a routing protocol is about how paths are calculated and advertised, not the exact sequence a particular packet takes; aggregate data rate concerns how much data can pass through a network over time (throughput), not the path; an encryption path isn't a standard term for the route data travels.

7. Which topology combines characteristics of more than one simple physical topology?

A. Hybrid Topology

B. Star Topology

C. Bus Topology

D. Mesh Topology

A network topology that combines characteristics of more than one simple physical topology is designed to fit different parts of a network by mixing layouts. A hybrid topology is defined by merging two or more simple topologies into one overall network, such as having star segments connected by a bus backbone or mixing star with mesh in different sections. This flexibility lets you leverage the strengths and mitigate the weaknesses of each approach in different areas of the network. The other options describe single, uniform layouts: a star connects every device to a central hub, a bus uses a single shared cable, and a mesh focuses on multiple direct connections between devices. None of these inherently blends different topologies within the same network, which is why the hybrid topology best fits the description.

8. Which topology has one central node that all devices connect to, with data first going into the central node?

A. Hybrid Topology

B. Star Topology

C. Mesh Topology

D. Bus Topology

In this setup, every device connects to a single central node, and all data must pass through that central point first. That describes a star topology. Each device runs its own link to the central hub or switch, so when one device sends data, it goes to the central node, which then forwards it to the intended recipient. This central node acts as the traffic manager, making it easy to add new devices and isolate issues to individual links, but it also creates a single point of failure if the central device fails. The other topologies don't fit because a mesh has multiple interconnections between devices, a bus uses a single shared communication medium along a backbone without a central switch to route traffic, and a hybrid combines elements of different layouts and doesn't inherently require every device to connect to one central point.

9. Which statement correctly characterizes fiber optic cabling?

A. Twisted pair uses copper and is low cost.

B. Coaxial cable uses copper and shielding.

C. Fiber optic uses light (glass or plastic) and is not interfered by electrical signals; high cost.

D. Wireless networks use radio waves.

Fiber optic cabling transmits data by sending light through glass or plastic fibers. This light-based signaling makes the medium immune to electrical interference from nearby signals, so data integrity remains high even in electrically noisy environments. It also supports very high bandwidth and can carry signals over long distances with relatively low attenuation. The trade-off is higher upfront cost due to materials, precision manufacturing, and more complex installation and splicing. That combination—uses light (glass or plastic), is not affected by electrical signals, and is typically more expensive—is what makes this description the best fit for fiber. Other statements describe copper-based media or wireless, which are valid for those technologies but not for fiber.

10. What does HTTPS stand for?

A. Hyper Text Transfer Protocol Secure

B. Hyper Text Transfer Protocol

C. Secure Hyper Text Transfer Protocol

D. Hyper Transfer Protocol Secure

HTTPS stands for Hyper Text Transfer Protocol Secure. It's the secure version of HTTP, using TLS to encrypt the data between your browser and the server. This encryption protects confidentiality (nobody can read the data in transit), integrity (it's hard for someone to alter the data without detection), and authenticity (you can verify you're talking to the legitimate server). That's why you'll often see URLs begin with https:// and a padlock icon. The other forms don't fit because they either omit the word Text, place Secure in the wrong spot, or drop a word entirely, which changes the meaning away from the standard secure protocol.

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!