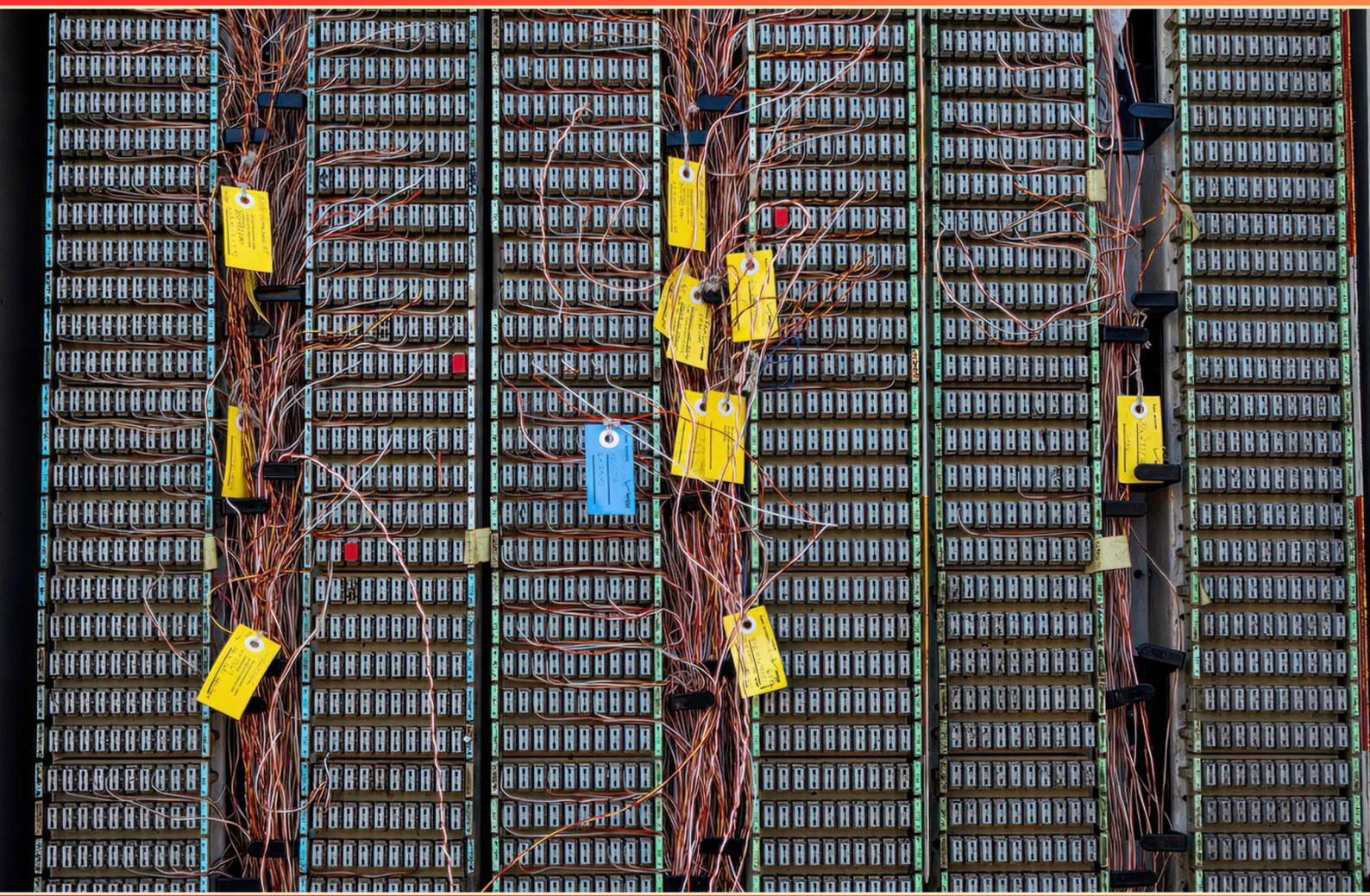
WFA LESSON 2 – NETWORKING PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://wfalesson2networking.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. Which role is least likely to be part of a NOC team?

A. Network Engineers

B. Security Analysts

C. Field Technicians

D. Marketing Staff

2. What is a key security enhancement WPA3 provides over WPA2?

A. WPA3 uses Simultaneous Authentication of Equals (SAE) and stronger encryption, providing better protection against offline password guessing.

B. WPA3 uses the same encryption as WPA2.

C. WPA3 eliminates the need for passwords.

D. WPA3 uses a weaker authentication method.

3. CIDR reduces routing table size by what mechanism?

A. Aggregating routes using variable-length prefixes

B. Using fixed-length prefixes of 32 bits

C. Increasing the number of routing table entries

D. Using classful addressing

4. Which of the following descriptions best captures a primary VLAN benefit?

A. They require multiple physical switches to segment traffic.

B. They isolate IP addresses at the data link layer.

C. They provide logical segmentation of broadcast domains within a switch to improve security and reduce broadcast traffic.

D. They improve router performance by increasing hop count.

5. What is port forwarding and when is it used?

A. Blocking all external traffic on a port.

B. Allocating a private address from DHCP.

C. Forwarding a specific external port to an internal IP/port; used to expose a service behind a NAT.

D. Proxying all ports to a single internal host.

SAMPLE

6. A network in which the computers are located within a small geographic area.

A. Wide Area Network (WAN)

B. Internet

C. Local Area Network (LAN)

D. Extranet

7. IPv6 addresses require a subnet mask.

A. Yes, they require a subnet mask

B. Yes, but a different format

C. Yes, 128-bit mask is used

D. No, no subnet mask needed

8. What is the purpose of the ARP protocol in IPv4 networks?

A. ARP maps MAC addresses to IP addresses.

B. ARP maintains DNS records for hostnames.

C. ARP assigns IP addresses to hosts automatically via DHCP.

D. ARP maps IP addresses to MAC addresses on a local network.

9. Which statement correctly describes BGP?

A. Border Gateway Protocol

B. Interior Gateway Protocol

C. Routing Information Protocol

D. Open Shortest Path First

10. Which command is used to verify reachability by sending a request from one computer to another?

A. nslookup

B. ping

C. tracert

D. netstat

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which role is least likely to be part of a NOC team?

A. Network Engineers

B. Security Analysts

C. Field Technicians

D. Marketing Staff

The essential idea is that a Network Operations Center focuses on ongoing technical operations: monitoring, troubleshooting, and maintaining the network and its security. Roles that fit this environment are those with hands-on networking knowledge and incident response skills. Network engineers bring design, configuration, and optimization expertise to keep devices and paths healthy. Security analysts specialize in watching for threats, analyzing events, and guiding responses to protect systems. Field technicians handle on-site hardware maintenance, replacements, and timely repairs to keep equipment functioning and networks up. Marketing staff, on the other hand, work on promoting products, branding, and communications. Their day-to-day tasks don't align with monitoring, diagnosing, or fixing network issues, so they're the least likely to be part of a NOC team.

2. What is a key security enhancement WPA3 provides over WPA2?

A. WPA3 uses Simultaneous Authentication of Equals (SAE) and stronger encryption, providing better protection against offline password guessing.

B. WPA3 uses the same encryption as WPA2.

C. WPA3 eliminates the need for passwords.

D. WPA3 uses a weaker authentication method.

WPA3 improves security by using a password-based authenticated key exchange called SAE, which provides strong protection against offline password guessing. SAE lets devices prove they know the password without sending it, and each authentication uses fresh, ephemeral keys. Because the handshake doesn't reveal material that can be tested offline, an attacker who captures traffic can't efficiently verify password guesses without interacting with the network in real time, making offline brute-force attempts impractical. In addition, WPA3 strengthens the encryption and overall key exchange, further safeguarding data even if the password is weak. The other options don't fit because the password is still used in WPA3, the encryption isn't the same as WPA2, and the authentication method isn't weaker—it's stronger with SAE.

3. CIDR reduces routing table size by what mechanism?

A. Aggregating routes using variable-length prefixes

B. Using fixed-length prefixes of 32 bits

C. Increasing the number of routing table entries

D. Using classful addressing

CIDR reduces routing table size by allowing multiple networks to be represented as one entry through a common, shorter prefix. This is done by using variable-length masks to aggregate adjacent networks into a single route—known as supernetting. Routers then forward traffic based on the longest prefix match, so packets destined for any of the aggregated networks follow the same next hop, instead of requiring separate entries for each /24 (or other small) network. For example, several contiguous /24 networks can be summarized as a single route like 192.168.0.0/22, which covers a larger block and cuts down the number of routes the router must store. This consolidation is what makes the routing tables more scalable. In contrast, using fixed-length prefixes (like all 32-bit addresses), relying on classful addressing, or simply increasing the number of entries would not achieve this combined efficiency.

SAMPLE

4. Which of the following descriptions best captures a primary VLAN benefit?

A. They require multiple physical switches to segment traffic.

B. They isolate IP addresses at the data link layer.

C. They provide logical segmentation of broadcast domains within a switch to improve security and reduce broadcast traffic.

D. They improve router performance by increasing hop count.

Dividing a network into VLANs creates separate broadcast domains at the data link layer. This means broadcast frames from a device in one VLAN don't reach devices in other VLANs, which cuts down on unnecessary traffic and helps security by limiting who can see what at the switch level. VLANs use unique IDs and can span across multiple switches through trunk links, so teams or departments stay logically separated even if they're in different physical locations. Communication between VLANs requires routing, so inter-VLAN traffic passes through a router or layer-3 switch, enabling centralized policy and access control. The idea that you must use multiple physical switches to segment traffic isn't necessary—one switch can host many VLANs. Isolating IP addresses at the data link layer isn't accurate since IP addressing is a network-layer concept, while VLANs focus on separating broadcast domains. And increasing hop count isn't a described benefit; VLANs aim to reduce broadcast traffic and organize traffic, with inter-VLAN routing handling communication between them.

5. What is port forwarding and when is it used?

A. Blocking all external traffic on a port.

B. Allocating a private address from DHCP.

C. Forwarding a specific external port to an internal IP/port; used to expose a service behind a NAT.

D. Proxying all ports to a single internal host.

Port forwarding is directing traffic for a specific external port on a router to a particular internal IP address and port inside a private network. This lets someone from outside reach a service that's behind NAT, like a home server, by exposing only the chosen port while keeping internal addresses hidden. For example, you can map external port 80 to 192.168.1.10:80 so a web server running on that internal machine is reachable from the Internet. This is why port forwarding is used: it enables access to a inside-host service without changing internal addressing or making the entire network directly public. Blocking external traffic, assigning private IPs via DHCP, or forwarding all ports to one internal host don't describe this targeted external-to-internal port mapping.

6. A network in which the computers are located within a small geographic area.

A. Wide Area Network (WAN)

B. Internet

C. Local Area Network (LAN)

D. Extranet

Understanding network size and geographic scope. A local area network is designed for a small geographic area—such as a building or campus—connecting devices like computers and printers with high speed and low latency using privately owned infrastructure (Ethernet or Wi Fi). This contrasts with a wide area network, which covers large distances; the Internet, a global system of networks; and an extranet, which extends a private network to external partners. So the described scenario fits a Local Area Network.

SAMPLE

7. IPv6 addresses require a subnet mask.

A. Yes, they require a subnet mask

B. Yes, but a different format

C. Yes, 128-bit mask is used

D. No, no subnet mask needed

In IPv6, the network portion of an address is defined by a prefix length rather than a separate subnet mask. An address is 128 bits, and routing uses a slash notation like /64 to specify how many leading bits form the network. For example, 2001:db8:abcd:0012::/64 means the first 64 bits identify the network and the remaining bits identify the host. Because the mask is conveyed as this prefix length, there isn't a need to apply a traditional subnet mask to an IPv6 address. That's why the correct interpretation is that no subnet mask is needed; you use a prefix length to indicate the subnet.

8. What is the purpose of the ARP protocol in IPv4 networks?

A. ARP maps MAC addresses to IP addresses.

B. ARP maintains DNS records for hostnames.

C. ARP assigns IP addresses to hosts automatically via DHCP.

D. ARP maps IP addresses to MAC addresses on a local network.

ARP resolves IP addresses to MAC addresses on the local network so a device can actually deliver a packet at the data link layer. When a host wants to send a packet to another host on the same LAN, it needs the destination's MAC address, not just its IP. ARP broadcasts a request asking who has that IP, and the device with that IP replies with its MAC address. The requester then caches this mapping for faster use next time. This is specifically about local IP-to-MAC resolution, which is why ARP isn't about DNS (names to IPs) or DHCP (automatic IP assignment). It's also not about mapping MAC to IP (the reverse direction). In IPv4, ARP's job is the IP-to-MAC mapping on the local network.

9. Which statement correctly describes BGP?

A. Border Gateway Protocol

B. Interior Gateway Protocol

C. Routing Information Protocol

D. Open Shortest Path First

BGP is the protocol used for exchanging routing information between different networks that are under separate administrative control—the autonomous systems that make up the Internet. It's designed for interdomain routing and supports policy-based decisions, letting operators control which networks to advertise and which paths to prefer. BGP is a path-vector protocol, meaning it conveys the route as a sequence of autonomous systems rather than just a single metric. It runs over TCP (port 179) to ensure reliable transport of routing updates. This combination of interdomain scope, path-vector behavior, and policy control distinguishes it from interior gateway protocols, which operate inside one network. The other options refer to different protocols: an interior gateway protocol, RIP, and OSPF, which are used for internal routing and use different algorithms.

SAMPLE

10. Which command is used to verify reachability by sending a request from one computer to another?

A. nslookup

B. ping

C. tracert

D. netstat

Verifying reachability between two machines is about confirming that one can reach the other over the network by sending a small request and waiting for a reply. Ping does exactly that: it sends an ICMP Echo Request to the target and reports whether an Echo Reply comes back, along with the round-trip time. This quick test shows if the destination is reachable and how long the path takes. nslookup is about translating a domain name to an IP address using DNS, not testing connectivity. tracert (traceroute) reveals the path to a destination and the routers along the way, which helps diagnose where a problem might lie, but it's not a direct reachability check. netstat lists current network connections and listening ports on the local machine, not whether another host is reachable. So the command that verifies reachability by sending a request is ping.

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://wfalesson2networking.examzify.com

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

SAMPLE