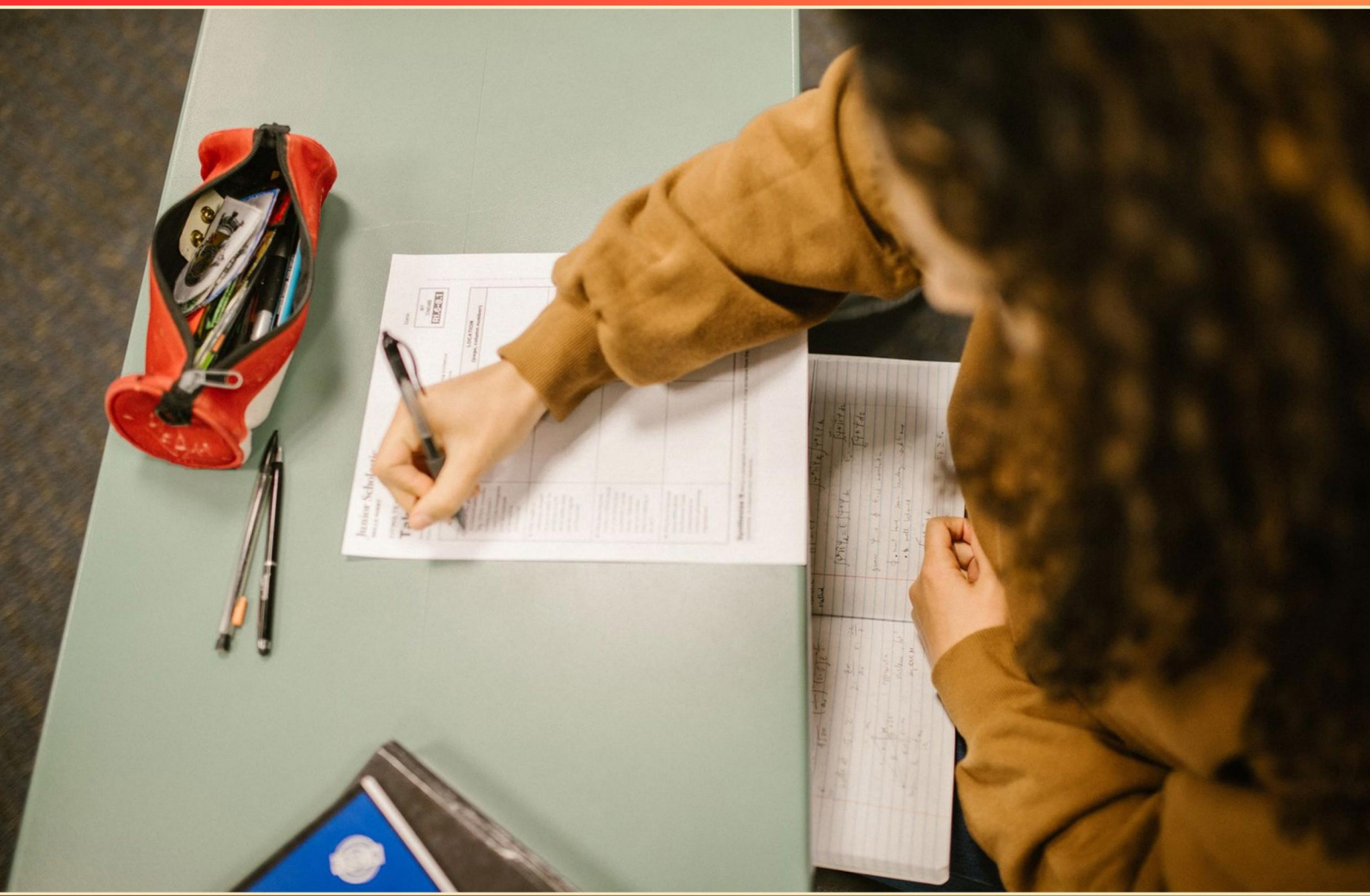
FSNA READINESS PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://fsnareadiness.examzify.com

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 type of cable must be used when cabling in areas where there are forced air returns?**

   A. PVC

   B. Plenum Rated

   C. Riser

   D. Shielded

2. **The traditional mode for wireless access where devices communicate through a wireless AP to access the LAN is called:**

   A. Infrastructure Mode

   B. Ad-hoc Mode

   C. Mesh Mode

   D. Enterprise Mode

3. **This interior gateway routing protocol uses hierarchical areas with Area 0 as the backbone area.**

   A. BGP

   B. RIP

   C. OSPF

   D. EIGRP

4. **Which Ethernet naming defines 10 Gigabit Ethernet over single-mode up to 40 kilometers?**

   A. 10GBASE-SR

   B. 10GBASE-T

   C. 10GBASE-ER

   D. 10GBASE-LX

5. **The main goal of First Hop Redundancy is that if even one gateway router fails the hosts on the network will never lose connectivity to _____.**

   A. Their Default Gateway

   B. The Internet

   C. The Local Network

   D. The DNS Server

6. Which term specifically refers to a single decoy system designed to attract attackers, in contrast to a network of decoys?

A. Honeynet

B. Sandbox

C. Decoy Farm

D. Honeypot

7. The Toner and Probe are used for locating specific cable runs.

A. Cable Tester

B. Toner and Probe

C. TDR

D. Multimeter

8. Which tool is used to determine the physical distance to a fault along a cable by sending a signal and analyzing reflections?

A. Cable Tester

B. Toner and Probe

C. TDR

D. Multimeter

9. The TCP/IP Network Interface Layer is also known as the

A. Internet Layer

B. Application Layer

C. Link Layer

D. Transport Layer

10. Which WLAN encryption standard is the most secure?

A. WEP

B. WPA

C. WPA2

D. TKIP

Answers

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

Explanations

1. Which type of cable must be used when cabling in areas where there are forced air returns?

A. PVC

B. Plenum Rated

C. Riser

D. Shielded

The key idea is that cable in spaces where air is circulated must meet strict fire and smoke safety requirements. In a forced air return area, the cable can become part of the air path, so it needs to minimize how much smoke and toxic fumes it releases if a fire occurs. Plenum-rated cables are designed for these spaces; they use materials that produce very low smoke and limited toxic gases, helping to keep air ducts and returns safer and less contaminated during a fire. Other options don't address this specific safety need. PVC jackets are common for general use but can emit more smoke and harmful gases in a fire, making them unsuitable for plenum spaces. Riser-rated cables are intended for vertical runs between floors, not specifically for air-handling plenums. Shielded cables focus on protecting against electromagnetic interference and don't tackle the fire-smoke requirements of air-return pathways.

2. The traditional mode for wireless access where devices communicate through a wireless AP to access the LAN is called:

A. Infrastructure Mode

B. Ad-hoc Mode

C. Mesh Mode

D. Enterprise Mode

In wireless networking, there are two main ways devices can connect to the LAN: through an access point or directly to each other. The setup described—devices communicating via a wireless AP to reach the LAN—fits infrastructure mode, where the access point acts as the central hub that bridges wireless clients to the wired network and provides centralized services like authentication and IP addressing. Ad-hoc mode would have devices talk directly to each other without an AP, so there's no single point bridging to the LAN. Mesh mode involves multiple APs working together to extend coverage and route traffic, which is a more complex topology than the traditional single AP bridging to the LAN. Enterprise mode isn't a mode of operation for the wireless link itself; it typically refers to security and management approaches rather than the basic topology.

3. This interior gateway routing protocol uses hierarchical areas with Area 0 as the backbone area.

A. BGP

B. RIP

C. OSPF

D. EIGRP

Hierarchical routing with a central backbone is a hallmark of this protocol. In this design, the network is divided into areas, and a special backbone area serves as the core that all other areas must connect to. Each area builds its own link-state database and runs its own SPF calculation, which keeps routing decisions localized and scalable. Inter-area routing can only happen through the backbone, with Area Border Routers bridging non-backbone areas to it. This structure allows the protocol to scale to large networks while preserving fast convergence and efficient routing. Other protocols don't follow this backbone-area model. The first focuses on routing between different autonomous systems and isn't designed around a central backbone of areas. The second is a basic distance-vector protocol without area segmentation, offering limited scalability. The last is a Cisco-proprietary protocol that uses its own routing philosophy and doesn't employ the Area 0 backbone concept.

4. Which Ethernet naming defines 10 Gigabit Ethernet over single-mode up to 40 kilometers?

A. 10GBASE-SR

B. 10GBASE-T

C. 10GBASE-ER

D. 10GBASE-LX

Understanding Ethernet naming and reach: the suffix in 10GBASE-ER stands for Extended Reach, indicating 10 Gigabit Ethernet over single-mode fiber with the ability to span up to about 40 kilometers. This makes it the option that fits "single-mode up to 40 kilometers." Other designs use different media and distances: SR is short-range over multimode fiber (short distance), LX uses long-wavelength single-mode fiber with moderate reach, and T runs over copper twisted pair (not fiber).

5. The main goal of First Hop Redundancy is that if even one gateway router fails the hosts on the network will never lose connectivity to _____.

A. Their Default Gateway

B. The Internet

C. The Local Network

D. The DNS Server

First Hop Redundancy is all about keeping the path to the next hop out of the local network up even if a gateway router fails. In practice, hosts use a shared virtual gateway IP as their default gateway. A group of routers runs a redundancy protocol so one is active and the others are ready to take over. If the active gateway dies, a standby becomes active, and traffic continues to reach the default route without manual reconfiguration. This ensures hosts never lose connectivity to their default gateway—the entry point for all traffic leaving the local network. External factors like an upstream Internet link or DNS service may still affect actual Internet or name resolution, but the immediate gateway path remains available.

6. Which term specifically refers to a single decoy system designed to attract attackers, in contrast to a network of decoys?

A. Honeynet

B. Sandbox

C. Decoy Farm

D. Honeypot

This item centers on the distinction between a single decoy setup and a broader decoy network. A honeypot is a single decoy system—one host or service intentionally made attractive to attackers—used to lure intruders, monitor their actions, and gather detailed data about attack techniques in a controlled way. It acts as a trap to study attacker behavior without exposing real assets. A honeynet, by contrast, is a network of multiple decoy systems that together attract and capture a wider range of attacker activity across several hosts. Sandboxes are isolated environments for safely executing potentially dangerous code, not primarily designed to lure attackers. Decoy Farm is not a standard term used in this context. So the correct term for a single decoy meant to attract attackers is honeypot.

7. The Toner and Probe are used for locating specific cable runs.

A. Cable Tester

B. Toner and Probe

C. TDR

D. Multimeter

When you need to locate a specific cable run, a toner and probe is the right tool because it is designed to trace the path of a conductor without having to disconnect or visually follow it. The tone generator is connected to the target cable end and injects a detectable signal (tone) onto that conductor. The probe or wand picks up that tone along the cable's route, letting you follow the wire through walls, behind panels, or inside a bundle to identify which cable is in use and where it runs. This method is especially useful for identifying lines in a crowded patch panel or locating a particular pair inside a bundle. A cable tester, while valuable for checking continuity and verifying pinouts and basic integrity, doesn't reveal the physical route of cables. A Time Domain Reflectometer (TDR) is great for pinpointing faults and locating breaks by sending a pulse and reading reflections, but it's not intended for tracing where a cable runs. A multimeter measures electrical properties like voltage, current, and resistance, which isn't helpful for mapping cable paths. So, for locating specific cable runs, using a toner and probe directly addresses the task by enabling you to trace the route of the target conductor.

8. Which tool is used to determine the physical distance to a fault along a cable by sending a signal and analyzing reflections?

A. Cable Tester

B. Toner and Probe

C. TDR

D. Multimeter

Time Domain Reflectometry (TDR) is used to locate faults along a cable by sending a fast electrical pulse into the line and analyzing reflections that occur when the signal meets impedance changes. The time between sending the pulse and seeing a reflection, together with the cable's propagation velocity, lets you calculate how far away the fault is. Since the pulse travels to the fault and back, you use half the round-trip time to get the one-way distance (distance = round-trip time × velocity / 2). This is like a sonar test for cables, revealing opens, shorts, or bad connections wherever the impedance changes along the run. The reflection shows up as a spike on a TDR trace, with its position indicating where the fault lies. Other tools don't provide this distance-to-fault capability: a cable tester checks continuity and mapping but not fault location, toner and probe helps trace physical paths rather than electrical faults, and a multimeter measures voltage, resistance, or current without locating reflections along a line.

9. The TCP/IP Network Interface Layer is also known as the

A. Internet Layer

B. Application Layer

C. Link Layer

D. Transport Layer

In the TCP/IP model, the Network Interface Layer covers how data actually travels over the local network and how devices on that network are addressed. It combines the responsibilities of the OSI Data Link and Physical layers and is commonly called the Link Layer in TCP/IP. This layer includes hardware addressing (MAC addresses), framing, and the methods used to access the local network medium (like Ethernet or Wi Fi). It also handles how the local network maps IP addresses to hardware addresses (ARP is a part of how this works on the local segment). The other layers have different roles: the Internet Layer handles routing between networks with IP, the Transport Layer handles end-to-end communication with TCP/UDP, and the Application Layer deals with software protocols used by applications. So, the TCP/IP Network Interface Layer is known as the Link Layer.

10. Which WLAN encryption standard is the most secure?

A. WEP

B. WPA

C. WPA2

D. TKIP

Strong WLAN security depends on using a robust encryption method with solid integrity protection. WEP relies on an old, broken RC4-based system with a short initialization vector, so it's easily cracked and not safe. TKIP, used with early WPA, fixed some WEP flaws but still relies on weaker techniques and has known vulnerabilities, so it isn't as secure as newer standards. WPA can offer improvements over WEP, but the most secure option among these is WPA2, which uses AES-based CCMP encryption to provide strong confidentiality and integrity. Therefore, WPA2 is the best choice for secure wireless protection.

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://fsnareadiness.examzify.com

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