Introduction to Networking Concepts 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 is used for networking that covers a metropolitan area?

A. LAN

B. CAN

C. MAN

D. WAN

2. Which tool is frequently used for vulnerability assessment by mapping hosts and services on a network?

A. nmap

B. ncat

C. netcat

D. wireshark

3. Which category uses four tightly woven twisted pairs (with more twists per foot) and supports 1 Gbps for up to 100 meters and 10 Gbps for up to 55 meters?

A. Cat5

B. Cat5e

C. Cat6

D. Cat6a

4. Which command shows information about active ports and their state across Windows, macOS, and Linux?

A. Arp

B. Netstat

C. Route

D. Whois

5. Which OSI layer is responsible for connection establishment, session maintenance, and authentication?

A. Layer 2 Data Link

B. Layer 5 Session

C. Layer 3 Network

D. Layer 1 Physical

6. Which network type would best be described as connecting devices across the widest geographic area among the listed types?

A. LAN

B. WLAN

C. SAN

D. WAN

7. Bare-metal hypervisors are commonly referred to as which type?

A. Type 1 Hypervisors

B. Type 2 Hypervisors

C. Hosted Hypervisors

D. Virtual Hypervisors

8. Which network type connects multiple LANs over a larger area than a campus but smaller than a country?

A. LAN

B. CAN

C. MAN

D. WAN

9. Which protocol is unencrypted and often used for remote access?

A. ssh

B. ftp

C. http

D. telnet

10. Which term describes networking across a metropolitan area?

A. LAN

B. WLAN

C. MAN

D. WAN

Answers

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

Explanations

1. Which term is used for networking that covers a metropolitan area?

A. LAN

B. CAN

C. MAN

D. WAN

A metropolitan-area network (MAN) is built to span an entire city, linking multiple local-area networks within the metro so they can share data and services at high speeds. This scale sits between a LAN, which generally serves a single building or campus, and a WAN, which covers broad geographic regions such as countries or continents. CAN refers to a campus-area network, typically connecting several buildings within a university or corporate campus, also smaller than a city-wide scope. By using fiber rings, Metro Ethernet, or wireless backbones, a MAN can efficiently connect various sites across a metropolitan area, providing faster interconnectivity than a WAN would typically offer while remaining more localized than a nationwide or global network. That's why the term used for networking that covers a metropolitan area is a metropolitan-area network.

2. Which tool is frequently used for vulnerability assessment by mapping hosts and services on a network?

A. nmap

B. ncat

C. netcat

D. wireshark

Identifying which devices exist on a network and what services they expose is a fundamental step in vulnerability assessment. Nmap is built for this purpose: it can discover hosts through various scanning techniques, determine which ports are open, and identify the services and often their versions running on those ports. This gives you a map of reachable machines and exposed software, which is essential for spotting vulnerabilities like outdated versions or misconfigurations. Nmap's power also comes from its service/version detection and the Nmap Scripting Engine, which can run automated checks to flag known vulnerabilities or risky configurations, turning discovered details into actionable risk insights. That combination—who's on the network, what's open, and what versions are running—directly supports assessing security posture. The other tools serve different roles. General-purpose connection tools are handy for manual testing and data transfer but aren't designed to scale discovery and detailed service enumeration across a network. A packet analyzer focuses on inspecting traffic to help troubleshoot or study network behavior, not on mapping every host and service to assess vulnerabilities. So, for vulnerability assessment that involves mapping hosts and services, the best choice is Nmap.

3. Which category uses four tightly woven twisted pairs (with more twists per foot) and supports 1 Gbps for up to 100 meters and 10 Gbps for up to 55 meters?

A. Cat5

B. Cat5e

C. Cat6

D. Cat6a

The concept being tested is how cable construction—specifically using four twisted pairs and how tightly those pairs are twisted—affects network speed and reach. Four twisted pairs are standard for modern Ethernet copper cables, and increasing how tightly the pairs are twisted helps reduce crosstalk and enables higher data rates over given distances. Cat5e is the enhanced version of Cat5 that tightened the twists and improved pair design to reliably carry 1 Gigabit Ethernet over the full 100-meter link. The emphasis on "four tightly woven twisted pairs" fits Cat5e's upgrade from Cat5, which is what makes it the best match for the description. While higher categories like Cat6 and Cat6a also use four pairs and can support 10 Gbps (Cat6 up to about 55 meters, Cat6a up to 100 meters), the description here centers on the improved twisting from Cat5, which is characteristic of Cat5e.

4. Which command shows information about active ports and their state across Windows, macOS, and Linux?

A. Arp

B. Netstat

C. Route

D. Whois

Netstat is the command that reveals information about active ports and their state across Windows, macOS, and Linux. It lists open sockets, showing local and remote addresses and port numbers, along with the connection state such as LISTENING for ports waiting for connections or ESTABLISHED for active connections. This lets you quickly see which services are listening on which ports and which connections are currently in use, regardless of the operating system. Other commands have different purposes: Arp maps IP addresses to MAC addresses, Route displays the routing table, and Whois looks up domain ownership information, so they don't provide the port-and-state view that Netstat does.

5. Which OSI layer is responsible for connection establishment, session maintenance, and authentication?

A. Layer 2 Data Link

B. Layer 5 Session

C. Layer 3 Network

D. Layer 1 Physical

The main idea is that the session layer coordinates conversations between two endpoints. It establishes the connection, keeps the interaction alive as long as the session lasts, handles dialog control (who talks when), and terminates the session when done. It can also incorporate authentication as part of starting a session, ensuring both sides are trusted before communication continues, and it provides mechanisms to recover or resume a session if something goes wrong. The data link layer is about delivering frames on a local link, the network layer is about routing across networks, and the physical layer handles the actual signals over the medium; none of these manage the ongoing state of a multi-step dialogue the way the session layer does.

6. Which network type would best be described as connecting devices across the widest geographic area among the listed types?

A. LAN

B. WLAN

C. SAN

D. WAN

The key idea here is the geographic scope of the network type. A LAN stays within a small, local area—think a single building or campus—using wired or wireless connections to link computers, printers, and other devices at high speeds. A WLAN is similar in scope but uses wireless technology, so it can roam a bit within that same small region, still not spanning large distances. A SAN, on the other hand, is a specialized network concentrated in a data center to connect servers with storage devices, prioritizing extremely fast data transfer over short distances, not wide-area reach. A WAN is designed to connect many local networks over large geographic distances, potentially across cities, countries, or continents. It relies on routers and wide-area links provided by telecom and service providers, and Internet-based connections to link geographically dispersed sites. This broad reach is what sets WAN apart from the others. So the network type that connects devices across the widest geographic area is the WAN.

7. Bare-metal hypervisors are commonly referred to as which type?

A. Type 1 Hypervisors

B. Type 2 Hypervisors

C. Hosted Hypervisors

D. Virtual Hypervisors

Bare-metal hypervisors are installed directly on the physical hardware, with no underlying host operating system. This direct-to-hardware placement is what defines the Type 1 category. Because they run right on the hardware, they can manage resources and guest virtual machines with minimal overhead and take full advantage of hardware virtualization features in the CPU, giving better performance and stronger isolation. The other terms describe different setups: a hypervisor that runs on top of a host OS is Type 2 (hosted). Hosted hypervisor is another way some refer to that same concept. "Virtual hypervisor" isn't the standard classification. So the correct type for bare-metal deployment is Type 1 Hypervisors.

8. Which network type connects multiple LANs over a larger area than a campus but smaller than a country?

A. LAN

B. CAN

C. MAN

D. WAN

Connecting several LANs across a city is the job of a Metropolitan Area Network. It sits between a campus-scale network and a country-scale WAN in terms of geographic scope: larger than a single campus or building, but not spanning an entire country. A LAN stays within one location, a CAN links multiple buildings within a campus, and a WAN covers broad distances that can cross countries or continents. So when the goal is to interconnect multiple LANs over an area larger than a campus but smaller than a country, a Metropolitan Area Network is the right fit.

9. Which protocol is unencrypted and often used for remote access?

A. ssh

B. ftp

C. http

D. telnet

The central idea here is how encryption affects remote management sessions. Telnet is designed to provide a remote command-line interface, but it sends every character, including usernames and passwords, in plaintext. That means anyone sniffing the network could read the session as it happens, making it unencrypted and insecure for remote access. In contrast, SSH encrypts the entire session, protecting credentials and commands from eavesdroppers, so it's the secure choice for remote access. FTP and HTTP aren't primarily used for interactive remote login; FTP is for file transfer (and can be encrypted with FTPS/SFTP), while HTTP is web traffic and not intended for secure remote shell access (HTTPS would be the secure variant for web-based admin interfaces). So, the unencrypted protocol commonly associated with remote access is Telnet.

10. Which term describes networking across a metropolitan area?

A. LAN

B. WLAN

C. MAN

D. WAN

Networking across a metropolitan area is described by a metropolitan area network. A local area network covers a small area, like a building or campus. A wireless LAN is simply a LAN that uses wireless links. A metropolitan area network spans a city, linking multiple LANs over tens of kilometers with high-speed connections, often using fiber and metro Ethernet. A wide area network covers much larger distances, potentially countrywide or intercontinental. So for city-scale networking, the term that fits best is metropolitan area network, which sits between LANs and WANs in geographic reach and is commonly used to interconnect several sites within a city.

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://introtonetworkingconcepts.examzify.com

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