Network Security Instructional Terminology Practice Test (Sample)

Study Guide

BY EXAMZIFY

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 category is associated with a 600 MHz bandwidth?**

   A. Ethernet (Cat 6a)

   B. Ethernet (Cat 6)

   C. Ethernet (Cat 5e)

   D. Ethernet (Cat 7)

2. **Which term describes the loss of signal strength from one end of a link to the other?**

   A. Attenuation

   B. Asset

   C. Authentication

   D. Backup

3. **IP addresses that use a default subnet mask per class are described by which addressing method?**

   A. Classful

   B. Classless Inter-Domain Routing (CIDR)

   C. Dynamic Host Configuration Protocol

   D. Private Internet Protocol (Private IP)

4. **Which type of fiber cable carries data via multiple light paths and typically has a core diameter of 50–100 microns?**

   A. Multi-mode Fiber

   B. Single-mode Fiber

   C. Fiber (Generic)

   D. Plastic Fiber

5. **An identifier for the network an IP address belongs to (32-bit in IPv4).**

   A. Network ID

   B. Network Topology

   C. NIC

   D. NetBIOS

6. **Which device provides centralized file storage accessible over the network?**

    A. Network Attached Storage

    B. Storage Area Network

    C. Direct Attached Storage

    D. Tape Library

7. **Which Ethernet category is designed to reduce cross-talk or noise by twisting the pairs without shielding?**

    A. Ethernet (RJ11)

    B. Ethernet (RJ45)

    C. Ethernet (Shielded Twisted Pair)

    D. Ethernet (Unshielded Twisted Pair)

8. **What term describes a network segment where devices can reach each other through broadcast messages?**

    A. Broadcast Domain

    B. Collision Domain

    C. VLAN

    D. Subnet

9. **A system of consistent monitoring of a network and informing network administrators of any issues.**

    A. Network Monitor

    B. Network Topology

    C. Nonrepudiation

    D. Numbering System (Binary)

10. **What TCP/IP attack redirects users by changing the DNS of a legit site?**

    A. DNS Poisoning

    B. DNS

    C. Dig

    D. Direct

Answers

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

Explanations

1. Which category is associated with a 600 MHz bandwidth?

A. Ethernet (Cat 6a)

B. Ethernet (Cat 6)

C. Ethernet (Cat 5e)

D. Ethernet (Cat 7)

Bandwidth ratings show the highest frequency a cable can carry while keeping signal quality. The higher the category, the higher the allowed frequency, enabling better performance. In this set of materials, 600 MHz is associated with Cat 6a. Cat 6a is the enhanced version of Cat 6, designed with improved shielding to reduce interference, which allows operation at higher frequencies than older categories. That's why 600 MHz is linked to Cat 6a in this context. Lower categories like Cat 5e and Cat 6 have smaller frequency ceilings, and Cat 7 is typically tied to even higher or differently defined specs, so the pairing here aligns with Cat 6a.

2. Which term describes the loss of signal strength from one end of a link to the other?

A. Attenuation

B. Asset

C. Authentication

D. Backup

Attenuation is the gradual loss of signal strength as it travels from one end of a link to the other. This weakening happens because the signal spreads out and interacts with the transmission medium, and it can worsen with longer distances or poorer cable quality. Engineers measure how much signal is lost in decibels over the length of the link and often use repeaters or amplifiers to keep the signal usable at the far end. The other terms describe different ideas—an asset is something valuable you own, authentication is proving who you are, and backup is creating a copy of data for recovery—so they don't describe how signal strength degrades along a medium.

3. IP addresses that use a default subnet mask per class are described by which addressing method?

A. Classful

B. Classless Inter-Domain Routing (CIDR)

C. Dynamic Host Configuration Protocol

D. Private Internet Protocol (Private IP)

Classful addressing uses fixed default subnet masks that are tied to the IP address class. In this approach, the first octet of the address determines whether it's Class A, B, or C, and the default masks are /8, /16, and /24 respectively. So, when an address is described using its default mask for its class, it's being described by classful addressing. CIDR is the modern, classless alternative that allows arbitrary prefix lengths (like /19 or /22) and isn't bound to the class-based defaults. DHCP is just the protocol for dynamically assigning addresses, and Private IP refers to reserved address ranges, not the addressing method itself.

4. Which type of fiber cable carries data via multiple light paths and typically has a core diameter of 50–100 microns?

A. Multi-mode Fiber

B. Single-mode Fiber

C. Fiber (Generic)

D. Plastic Fiber

Understanding fiber optic cable types and how core size affects light propagation. Data traveling via multiple light paths describes modal transmission, which happens when the fiber has a relatively large core that can support several propagation modes. Core diameters around 50 to 100 microns are characteristic of multimode fiber (such as 50/125 or 62.5/125). In multimode fiber, light can take many paths through the core, which makes it more susceptible to modal dispersion but is adequate for shorter-distance links and commonly uses cheaper light sources like LEDs. Single-mode fiber, by contrast, has a much smaller core (about 8–10 microns) designed to carry light along a single path, suitable for long-distance, high-bandwidth links, and does not match the 50–100 micron core size. Plastic fiber is a different material and isn't described by this core-size range in standard contexts. Therefore, the description fits multimode fiber best.

5. An identifier for the network an IP address belongs to (32-bit in IPv4).

A. Network ID

B. Network Topology

C. NIC

D. NetBIOS

Network ID is the identifier for the network the IP address belongs to. In IPv4, an address is 32 bits and is divided into a network portion and a host portion according to the subnet mask (or CIDR prefix). The network ID is the part that identifies which network the address is on, while the remaining bits identify a specific device on that network. Routers use this network portion to decide where to forward packets. For example, with 192.168.1.10 and a /24 mask, the network ID is 192.168.1.0. The other terms refer to different concepts: network topology is the layout of devices, NIC is hardware, and NetBIOS is a legacy name service.

6. Which device provides centralized file storage accessible over the network?

A. Network Attached Storage

B. Storage Area Network

C. Direct Attached Storage

D. Tape Library

The concept being tested is centralized file storage that can be accessed over the network. A Network Attached Storage device is built to provide shared file access to many clients across the network. It runs its own dedicated file-serving software and offers shares or directories that users and applications can mount or map, often using common protocols like SMB/CIFS for Windows or NFS for Unix/Linux. This setup makes it easy to manage permissions, quotas, and backups from one central location, while any networked client can reach the stored files. Storage Area Networks, while networked, deliver block-level storage to servers rather than shared files, meaning servers manage their own file systems on top of the presented blocks. Direct Attached Storage is stored directly inside a single computer and isn't readily shared across the network by default. A Tape Library is primarily for backup and archival storage with typically sequential access, not general-purpose file sharing. So the device that provides centralized, network-accessible file storage is the Network Attached Storage.

7. Which Ethernet category is designed to reduce cross-talk or noise by twisting the pairs without shielding?

A. Ethernet (RJ11)

B. Ethernet (RJ45)

C. Ethernet (Shielded Twisted Pair)

D. Ethernet (Unshielded Twisted Pair)

Twisting the conductors in a cable without any shielding reduces cross-talk and noise by canceling interference through the twists. The regular twists cause any unwanted signals that couple into the cable to average out along its length, lowering crosstalk between pairs and making the signal more resilient without needing a shield. This is the hallmark of Unshielded Twisted Pair, which is why it's widely used for Ethernet under Cat5e and Cat6 standards with RJ45 connectors. Shielded Twisted Pair would add a shielding layer to fight external interference, which isn't part of the described design, and the other option references the connector type rather than the cable's shielding characteristics.

8. What term describes a network segment where devices can reach each other through broadcast messages?

A. Broadcast Domain

B. Collision Domain

C. VLAN

D. Subnet

Broadcast domains describe the portion of the network where a broadcast frame is delivered to every device. In Ethernet, switches forward broadcast frames to all ports within the same Layer 2 domain, while routers do not forward broadcasts, creating boundaries. So the network segment where all devices can reach each other via broadcast messages is one broadcast domain. The other concepts operate differently: a collision domain is about shared access and possible collisions, VLANs define logical boundaries that separate broadcast domains, and subnets are IP-layer boundaries defined by addressing and routing rather than how broadcasts propagate at Layer 2.

9. A system of consistent monitoring of a network and informing network administrators of any issues.

A. Network Monitor

B. Network Topology

C. Nonrepudiation

D. Numbering System (Binary)

This item tests the idea of continuous oversight of a network and alerting administrators when problems occur. A network monitor is designed to continuously check device health, uptime, performance metrics (like latency and packet loss), and service availability, then generate alerts or notifications when something goes outside expected ranges. It often collects data, provides dashboards, and logs incidents to support quick remediation, making it ideal for proactive network management. The other terms describe different concepts. Network topology is about how devices are connected and arranged in a network, not about ongoing monitoring or alerts. Nonrepudiation refers to a security property that prevents a sender from denying a transmitted message, which is about accountability in communications rather than monitoring. Numbering system (binary) is simply a way of representing data, unrelated to monitoring and alerting.

10. What TCP/IP attack redirects users by changing the DNS of a legit site?

A. DNS Poisoning

B. DNS

C. Dig

D. Direct

The attack being tested is about corrupting DNS responses so a legitimate site resolves to the wrong IP, guiding users to a fraudulent host. This is DNS poisoning (also known as DNS spoofing). By tampering with DNS data—either in a cache, on an authoritative server, or along the lookup path—the attacker makes a user's browser think the legitimate domain points to the attacker-controlled address. As a result, even when the user enters the correct URL, they're redirected to a malicious site, enabling phishing, credential theft, or malware delivery. The other options don't describe this redirection technique. DNS is the system that translates names to addresses, not an attack itself. Dig is a tool used to query DNS records, not to perform redirection. Direct isn't a standard term for a DNS-based attack.

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://netsecinstructionalterms.examzify.com

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