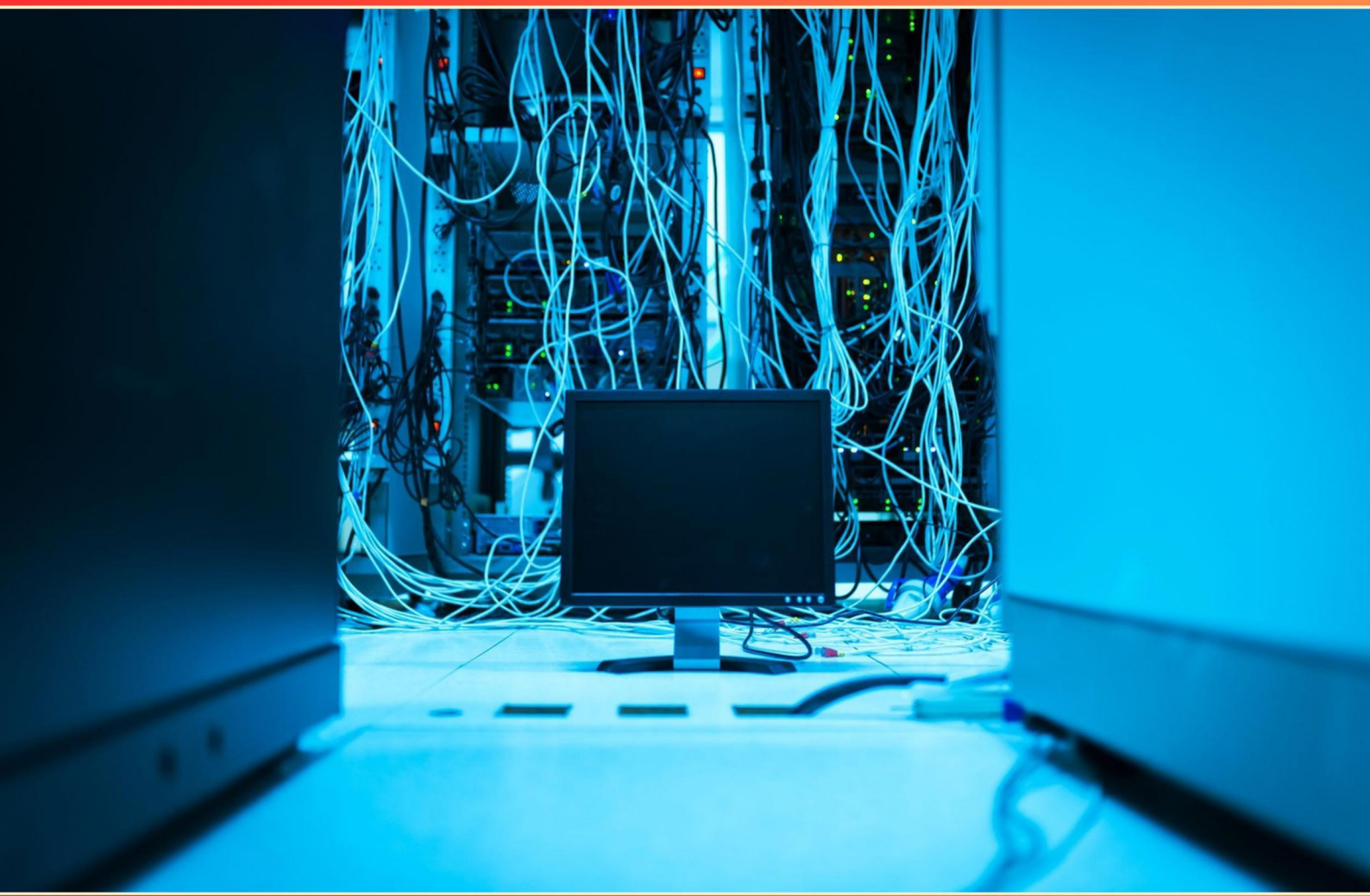
NETWORK SYSTEMS EXAM 1 PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://networksys1.examzify.com

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

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. Why is it important to rotate cryptographic keys?

A. Increases the risk of data being compromised

B. Reduces the risk of data being compromised

C. Damages encrypted data

D. Increases system complexity without security benefits

2. What best describes protocols in networking?

A. They are rules used between networked devices for communication.

B. They are electric signals used to turn devices on.

C. They are top-level domain names.

D. They are anti-virus signatures.

3. Which IPv6 address identifies multiple destinations, with packets delivered to the closest destination?

A. Global address

B. Anycast address

C. Multicast address

D. Unicast address

4. What best describes the difference between an ARP table and a MAC address table?

A. An ARP table maps IP addresses to MAC addresses.

B. A MAC address table maps IP addresses to switch ports.

C. An ARP table stores IPv6 addresses only.

D. A MAC address table maps MAC addresses to VLAN IDs.

5. Reviewing the router inventory can reveal which details?

A. The physical location of each router

B. How many routers are present

C. The firmware version of each router

D. The network password for admin access

6. If a live feed transmitted using UDP shows color glitches because packets are lost or dropped, which statement explains this behavior?

A. UDP provides error checking or correction.

B. UDP uses sequence numbers to ensure order.

C. UDP does not guarantee delivery.

D. UDP does not provide error checking or retransmission.

7. Which term describes the process of designing, implementing, and maintaining a broad set of IT systems, including hardware, software, and processes?

A. System development lifecycle

B. IT governance

C. Software development lifecycle

D. System life cycle

8. Which OSI layer is responsible for physical addressing using MAC addresses?

A. Network Layer (Layer 3)

B. Data Link Layer (Layer 2)

C. Physical Layer (Layer 1)

D. Transport Layer (Layer 4)

9. What action should Allan take for the 10 laptops that encountered issues with a firmware update?

A. Shut off BIOS updates for the affected laptops and continue to update for the rest.

B. Disable BIOS updates for all laptops

C. Proceed with updates on all laptops

D. Ignore OEM notifications

10. Which statement about stream ciphers is true?

A. A stream cipher encrypts one bit or byte at a time.

B. A stream cipher encrypts data in fixed-size blocks.

C. A stream cipher uses no keys.

D. A stream cipher is always faster than a block cipher.

Answers

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

Explanations

1. Why is it important to rotate cryptographic keys?

A. Increases the risk of data being compromised

B. Reduces the risk of data being compromised

C. Damages encrypted data

D. Increases system complexity without security benefits

Rotating cryptographic keys means periodically replacing the keys used to protect data. This keeps the impact of any single compromised key small: if a key is stolen, only the data encrypted with that specific key is at risk, and once you rotate to a new key, past data can be retired from usability with the old key. It also enables quick revocation and rekeying if a key is suspected or proven compromised, giving post-compromise security and forward secrecy for future data. The actual data remains protected overall because new data is encrypted with fresh keys, and the transition is handled through proper key management. So, the main benefit is reducing the risk of data being compromised.

2. What best describes protocols in networking?

A. They are rules used between networked devices for communication.

B. They are electric signals used to turn devices on.

C. They are top-level domain names.

D. They are anti-virus signatures.

Protocols govern how devices communicate on a network. They are the agreed rules that specify how data is formatted, transmitted, detected, and acknowledged, and how sessions start and end. With these rules, devices can exchange messages reliably, understand each other's syntax, and handle issues like errors and ordering. For example, TCP handles reliable transport, IP handles addressing and routing, HTTP defines how web requests and responses are structured, and DNS maps domain names to IP addresses. The other descriptions don't fit networking communication rules: electric signals for turning devices on refer to power, not data exchange; top-level domain names relate to naming rather than how communication happens; antivirus signatures pertain to security software patterns, not the protocols that govern data transfer.

3. Which IPv6 address identifies multiple destinations, with packets delivered to the closest destination?

A. Global address

B. Anycast address

C. Multicast address

D. Unicast address

Anycast addresses identify multiple destinations, with packets delivered to the nearest member. In IPv6, several devices can share the same anycast address, and when a packet is sent to that address, routers route it to the closest instance based on current routing metrics like cost or latency. This lets services be accessed from the nearest location without the sender needing to know which specific device will answer, which is ideal for things like regional DNS servers or nearby edge routers. This behavior is different from a multicast address, which delivers to all members of a group, and from a unicast address, which targets a single device. A global address is simply a routable unicast address type and does not imply multiple destinations.

4. What best describes the difference between an ARP table and a MAC address table?

A. An ARP table maps IP addresses to MAC addresses.

B. A MAC address table maps IP addresses to switch ports.

C. An ARP table stores IPv6 addresses only.

D. A MAC address table maps MAC addresses to VLAN IDs.

The main idea is that ARP tables and MAC address tables serve different functions in how devices locate each other on a local network. An ARP table is about resolving addresses: it stores mappings from IP addresses to MAC addresses so a host can encapsulate an IPv4 packet in an Ethernet frame with the correct destination hardware address. These mappings are learned dynamically through ARP requests and replies and are used when a host needs to send data to another IPv4 device on the same subnet. A MAC address table, on the other hand, lives in switches and tells the switch which physical port to forward a frame to based on the destination MAC address. The switch learns these mappings by observing the source MAC of frames it sees, building a MAC-to-port map (often within the context of a VLAN). This speeds up forwarding and avoids broadcasting to all ports. So the statement that ARP tables map IP addresses to MAC addresses is the best description because it captures the purpose of ARP: translating an IP address to the hardware address needed to actually deliver the frame. The other ideas mix up the roles: a MAC address table maps MAC addresses to switch ports (not IPs), ARP tables are not limited to IPv6, and MAC tables aren't defined by VLAN IDs themselves.

5. Reviewing the router inventory can reveal which details?

A. The physical location of each router

B. How many routers are present

C. The firmware version of each router

D. The network password for admin access

An inventory is a catalog of devices you have in the network, focusing on listing assets and how many of each exist. When you review it, the most reliable takeaway is the total count of routers deployed, because the primary purpose of an inventory is to track quantity for management, planning, and audits. While some records may include additional details like location or firmware, those fields aren't guaranteed to be present or up to date in every inventory, and sensitive information such as admin passwords is not stored there for security reasons. So the number of routers you have is the detail you can definitively determine from reviewing the inventory.

6. If a live feed transmitted using UDP shows color glitches because packets are lost or dropped, which statement explains this behavior?

A. UDP provides error checking or correction.

B. UDP uses sequence numbers to ensure order.

C. UDP does not guarantee delivery.

D. UDP does not provide error checking or retransmission.

The main idea is that UDP is a best-effort, connectionless protocol that does not guarantee delivery or perform automatic retransmission. In a live video feed, if some UDP packets are lost, the data for those portions of the stream never arrives again unless the application itself handles recovery. Because there's no built-in mechanism to resend lost packets, the viewer ends up seeing missing data within frames, which shows up as color glitches or artifacts. Streaming systems often rely on error concealment or higher-level recovery methods for smoother playback, or choose protocols that provide reliability when needed. It's true that UDP has a checksum for detecting corruption, but it doesn't offer built-in error correction or retransmission, which is why the lack of guaranteed delivery explains the glitches.

7. Which term describes the process of designing, implementing, and maintaining a broad set of IT systems, including hardware, software, and processes?

A. System development lifecycle

B. IT governance

C. Software development lifecycle

D. System life cycle

The process described is the full lifecycle of an information system as an integrated entity—from initial concept through design, deployment, ongoing operation, maintenance, and eventual retirement. This broad view includes hardware, software, and the processes that run and govern how the system is used, updated, and finally decommissioned. That scope is captured by the term that refers to the system's life from start to finish, not just the development or software aspects. The other terms are narrower or focus on governance. System development lifecycle centers on creating and deploying a system, often with emphasis on the development phases and not necessarily the ongoing life of the entire system. Software development lifecycle targeted at software products misses the hardware and organizational processes. IT governance is about policy, oversight, and decision-making rather than the end-to-end lifecycle of a system.

8. Which OSI layer is responsible for physical addressing using MAC addresses?

A. Network Layer (Layer 3)

B. Data Link Layer (Layer 2)

C. Physical Layer (Layer 1)

D. Transport Layer (Layer 4)

In networking, identifying devices on the local network uses physical addresses assigned to network interface cards, and this is a function of the Data Link layer. This layer encapsulates data into frames and attaches source and destination MAC addresses, which allow switches to deliver the frame to the correct device on the same local segment. MAC addresses are hardware identifiers tied to NICs and operate within the local broadcast domain. The other layers don't handle this kind of addressing: the Physical layer deals with sending raw bits over the medium, not addresses; the Network layer uses logical addresses like IPs for routing across networks; the Transport layer focuses on end-to-end delivery and uses ports rather than hardware addresses.

9. What action should Allan take for the 10 laptops that encountered issues with a firmware update?

A. Shut off BIOS updates for the affected laptops and continue to update for the rest.

B. Disable BIOS updates for all laptops

C. Proceed with updates on all laptops

D. Ignore OEM notifications

When a firmware update causes issues on a subset of devices, the best approach is to isolate those affected devices from the update while continuing updates for the rest. This minimizes risk: the 10 laptops won't be subjected to another failing or potentially bricking update, while the other machines still receive important firmware and security fixes. It also gives you time to collect error logs, determine the cause, and consult the OEM for a fix or workaround before attempting a broader rollout. Shutting off BIOS updates for everyone or proceeding to update all machines ignores the specific failure on the affected group and can propagate problems or leave healthy devices without essential updates. Ignoring OEM notifications misses important guidance and fixes that could address the issue.

10. Which statement about stream ciphers is true?

A. A stream cipher encrypts one bit or byte at a time.

B. A stream cipher encrypts data in fixed-size blocks.

C. A stream cipher uses no keys.

D. A stream cipher is always faster than a block cipher.

Stream ciphers work by generating a keystream from a secret key (often with an IV) and combining it with the plaintext bit by bit or byte by byte, typically using XOR. That continuous, bit- or byte-level processing is what makes them different from block ciphers, which operate on fixed-size blocks of data at a time. So the statement is true because a defining feature of stream ciphers is precisely encrypting data one bit or one byte at a time as it flows through the system. Keep in mind that stream ciphers do use a key to drive the keystream, and they can be highly efficient for real-time or variable-length data. They are not always faster than block ciphers, though—their performance depends on the specific algorithm and the hardware or software implementation. Also, a keystream must never be reused with different messages, or security is severely compromised.

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://networksys1.examzify.com

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