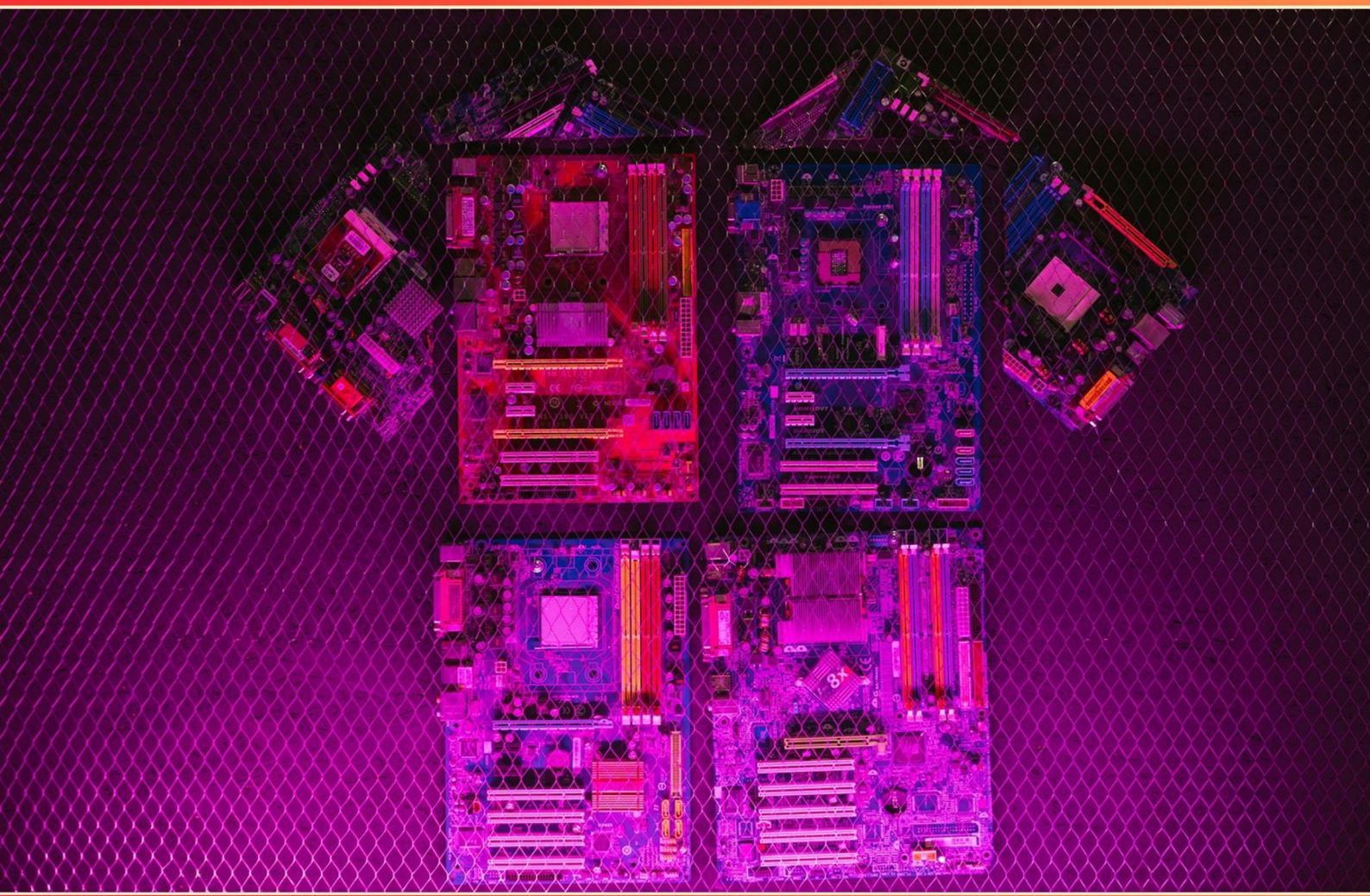
JASON DION'S NETWORK+ COURSE PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://jasondionsnetpluscourse.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 statement accurately describes TLS in data transmission?

A. TLS is used for email only.

B. SSL is stronger than TLS.

C. TLS provides encryption for data at rest.

D. TLS provides encryption and authentication for data in transit.

2. Which statement best describes multi-factor authentication?

A. Multi-Factor Authentication uses a single verification method.

B. Multi-Factor Authentication uses multiple verification methods to increase security.

C. MFA stands for Managed File Access.

D. Multi-Factor Authentication is only used in high-security environments.

3. Which items are the key components of disaster recovery planning?

A. RTO (recovery time objective), RPO (recovery point objective), backups, failover plans, and testing.

B. SLA, maintenance window, change management, runbooks.

C. Asset tags, inventory, lifecycle, maintenance.

D. SNMP, monitoring, performance.

4. Why is change control important?

A. It ensures the fastest possible changes.

B. It documents network topology.

C. It ensures only security updates.

D. It prevents unapproved or risky changes that could cause outages or security issues.

5. Which DNS record maps a domain name to an IPv4 address?

A. A

B. AAAA

C. CNAME

D. MX

6. In IPv4 networks, what does ARP do?

A. Translates IPv4 addresses to MAC addresses by broadcasting a request and receiving a reply with the MAC

B. Verifies route paths between networks

C. Encrypts data over VPN

D. Maps IP addresses to DNS names

7. Which transport protocol is typically used for streaming audio/video, and why?

A. UDP – lower overhead, no guaranteed delivery, tolerates some loss

B. SCTP

C. ICMP

D. TCP – reliable but overhead

8. What is the purpose of a subnet mask in IPv4 addressing?

A. It assigns the default gateway for the network.

B. It translates hostnames to IP addresses.

C. It determines the broadcast address for an entire network.

D. It defines which bits are network versus host, enabling subnetting and address separation.

9. Which protocol is used to translate domain names to IP addresses?

A. FTP

B. SMTP

C. SSH

D. DNS

10. Which statement best describes the primary function of a router in a network?

A. Provides end-user storage for files

B. Allows network segments and broadcast domains to communicate with each other

C. Converts analog signals to digital

D. Only filters traffic at the network edge

Answers

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

Explanations

1. Which statement accurately describes TLS in data transmission?

A. TLS is used for email only.

B. SSL is stronger than TLS.

C. TLS provides encryption for data at rest.

D. TLS provides encryption and authentication for data in transit.

TLS protects data as it travels across a network by providing both encryption and authentication. During the handshake, each end authenticates the other (often with certificates) and they agree on a session key. That key encrypts the transmitted data, keeping it confidential, and the protocol also includes integrity checks so you can detect any tampering. This is why TLS is used to secure many kinds of traffic, not just email—HTTPS for web pages, secure email transmissions (via StartTLS or SMTPS), and other protocols all rely on TLS to keep data in transit private and trustworthy. Data at rest, such as files stored on a disk, isn't protected by TLS. That would require encryption at rest. SSL is the older protocol family that TLS superseded, and TLS is the current standard for secure transmission.

2. Which statement best describes multi-factor authentication?

A. Multi-Factor Authentication uses a single verification method.

B. Multi-Factor Authentication uses multiple verification methods to increase security.

C. MFA stands for Managed File Access.

D. Multi-Factor Authentication is only used in high-security environments.

Multi-factor authentication requires more than one way to verify who you are, which makes it much harder for someone to pose as you. It uses at least two independent factors, typically something you know (like a password), something you have (a code from a device or an app), or something you are (a fingerprint or other biometric). By needing multiple proofs, even if one factor is compromised, access isn't granted without the other factors. That's why the statement that best describes MFA is that it uses multiple verification methods to increase security. The other ideas fall short because a single verification method is just single-factor authentication, the acronym reference is incorrect, and MFA isn't limited to only high-security environments; it's common in everyday security practices.

3. Which items are the key components of disaster recovery planning?

A. RTO (recovery time objective), RPO (recovery point objective), backups, failover plans, and testing.

B. SLA, maintenance window, change management, runbooks.

C. Asset tags, inventory, lifecycle, maintenance.

D. SNMP, monitoring, performance.

Disaster recovery planning focuses on how to resume operations after a disruption, balancing data protection with timing. The best answer includes defining the Recovery Time Objective and Recovery Point Objective, which set the maximum allowable downtime and data loss, guiding how you design backups and replication. Backups provide the actual data copies you restore from, while failover plans describe how to switch to an alternate system or site to keep services running. Testing is crucial to verify that the plan works, that backups are usable, and that failover procedures will execute smoothly during an incident. Together, these elements establish the targets for recovery and the concrete steps to meet them. The other options cover general IT operations rather than the specific components needed to recover from a disaster. Service-level agreements, maintenance windows, change management, and runbooks relate to service expectations and process control. Asset tags, inventory, lifecycle, and maintenance focus on asset management. SNMP, monitoring, and performance deal with detecting and measuring system health, not the actual recovery strategy.

4. Why is change control important?

A. It ensures the fastest possible changes.

B. It documents network topology.

C. It ensures only security updates.

D. It prevents unapproved or risky changes that could cause outages or security issues.

Change control is about governing changes to IT systems so that every modification goes through a formal, reviewed process. This means proposed changes are evaluated for risk, tested in a safe environment, approved by responsible stakeholders, scheduled to minimize impact, and backed up with a plan to roll back if something goes wrong. By inserting checks and oversight, change control reduces the chance that a risky or unapproved modification will cause outages, performance problems, or security gaps. That's why this option is the best. It captures the core purpose: preventing unapproved or risky changes that could jeopardize availability or security. The other ideas miss the broader role of change control: it isn't solely about speed, it isn't just about documenting topology, and it isn't limited to security updates. Change control applies to all meaningful changes, with governance, testing, and rollback planning to protect the environment.

5. Which DNS record maps a domain name to an IPv4 address?

A. A

B. AAAA

C. CNAME

D. MX

A records are used to map a domain name to an IPv4 address. This is the standard way a hostname is resolved for IPv4 networks, linking something like a domain to a 32-bit address such as 198.51.100.5. The other record types serve different purposes: AAAA records map a domain to an IPv6 address, CNAME records create an alias from one name to another domain name, and MX records specify which mail server handles email for the domain. So when the goal is to find the IPv4 address associated with a domain, the A record is the one that provides that mapping.

6. In IPv4 networks, what does ARP do?

A. Translates IPv4 addresses to MAC addresses by broadcasting a request and receiving a reply with the MAC

B. Verifies route paths between networks

C. Encrypts data over VPN

D. Maps IP addresses to DNS names

ARP's job is to translate IPv4 addresses into MAC addresses on a local network. When a device wants to send a packet to another host on the same LAN, it first checks its ARP cache for the destination IP. If there's no entry, it broadcasts an ARP request asking who has that IP, and the device that owns it replies with its MAC address. With that MAC, the sender can place the frame on the wire and reach the destination. That mapping is stored temporarily in the ARP table to speed up subsequent traffic. The other options describe different technologies: routing verifies paths between networks, VPNs encrypt data, and DNS maps domain names to IP addresses—not MACs. ARP is specifically about resolving IP addresses to MAC addresses on the local network.

7. Which transport protocol is typically used for streaming audio/video, and why?

A. UDP – lower overhead, no guaranteed delivery, tolerates some loss

B. SCTP

C. ICMP

D. TCP – reliable but overhead

For streaming audio and video, keeping latency low matters more than ensuring every packet arrives. UDP provides a lightweight, connectionless transport with minimal overhead and no retransmission delays. It doesn't guarantee delivery, and packets can be lost or arrive out of order, but the application—and often the media protocol on top of it—handles this with buffering, error concealment, or forward error correction. That quick, steady flow keeps playback smooth, especially for live or real-time streams. In contrast, TCP guarantees delivery of every byte by using acknowledgments and retransmissions, which introduces latency and jitter that can disrupt real-time playback. ICMP is a diagnostic protocol, not used to transport media. SCTP adds reliability and multi-streaming features, but it's not as widely adopted for streaming media and typically incurs more overhead than UDP in this context. Therefore UDP is the typical choice for streaming audio/video due to its lower overhead and tolerance for some data loss.

8. What is the purpose of a subnet mask in IPv4 addressing?

A. It assigns the default gateway for the network.

B. It translates hostnames to IP addresses.

C. It determines the broadcast address for an entire network.

D. It defines which bits are network versus host, enabling subnetting and address separation.

Subnet masks define which bits in an IPv4 address belong to the network portion and which belong to the host portion. They are written as 32-bit values with 1s indicating network bits and 0s indicating host bits. This separation lets you subdivide an address space into subnets (subnetting) and determine where to route traffic within a network. When you apply the mask to an IP address, you can derive the network address, which identifies the specific subnet, and you can infer the range of usable host addresses in that subnet. The broadcast address can be derived by setting all host bits to 1, but the essential purpose of the mask is to distinguish network versus host bits for proper addressing and subnetting. The other options describe different network functions (gateway assignment, name resolution) that are not what the mask determines.

9. Which protocol is used to translate domain names to IP addresses?

A. FTP

B. SMTP

C. SSH

D. DNS

DNS, the Domain Name System, is what translates human-friendly domain names into IP addresses. Computers need IPs to reach services, but people remember names like example.com, not numeric addresses. When you look up a domain, your device asks a DNS resolver. If the answer isn't cached, the resolver queries a hierarchy: root servers, then the appropriate top-level domain servers, and finally the domain's authoritative servers until it gets the IP. That IP is returned to your device so it can establish the connection. DNS primarily uses UDP on port 53 for queries, with TCP used for reliable transfers or large responses. Other protocols serve different purposes: FTP is for transferring files, SMTP handles email transport, and SSH provides secure remote login. They don't translate domain names to IP addresses like DNS does.

10. Which statement best describes the primary function of a router in a network?

A. Provides end-user storage for files

B. Allows network segments and broadcast domains to communicate with each other

C. Converts analog signals to digital

D. Only filters traffic at the network edge

Routers operate at the network layer to connect different IP networks and determine the best path for data to travel between them. Their primary role is to forward packets between network segments, enabling devices on separate subnets to communicate with one another. Because each interface on a router sits in its own network, routers inherently create separate broadcast domains; they don't forward broadcasts from one subnet to another by default, but they do enable communication across those networks by routing unicast traffic to the correct destination. That's why this statement best captures the router's main function: it links network segments and allows communication across different broadcast domains. The other options describe functions that aren't the router's core purpose—storage is for file sharing, converting analog to digital is a job for a modem, and while routers can filter traffic, filtering isn't their primary role.

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://jasondionsnetpluscourse.examzify.com

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