Transport Layer Protocols and Functions in Networking 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 statement describes the main difference between TCP and UDP as addressed in the material?

A. TCP is designed for reliability, while UDP prioritizes speed and does not guarantee delivery.

B. TCP is connectionless and UDP is connection-oriented.

C. TCP uses IP whereas UDP does not.

D. TCP operates only on LAN, UDP only on WAN.

2. Which statement about DNS hierarchy is true?

A. It serves to distribute management of domain name data across multiple servers.

B. It stores all DNS records in a single centralized server.

C. It translates IP addresses into MAC addresses for local networks.

D. It requires no servers to function.

3. Which statement best describes a non-authoritative DNS server?

A. It caches information from authoritative servers.

B. It holds the original data for a domain.

C. It hosts the domain's zone file.

D. It signs DNS responses with DNSSEC.

4. Which mechanism is primarily responsible for ensuring data does not overwhelm the receiver in a TCP connection?

A. Flow control

B. Routing

C. Encryption

D. Compression

5. What is the significance of the OSI model in networking?

A. It guarantees interoperability without standards

B. It provides a framework for understanding and implementing network protocols and services

C. It describes hardware specifications

D. It dictates vendor-unique protocols

6. How does the Transport Layer recover lost data?

- **A. By reordering packets only**
- **B. By performing encryption**
- **C. By automatically requesting that the data be sent again**
- **D. By compressing data**

7. What is the purpose of TFTP?

- **A. To perform simple file transfers, particularly in booting or configuring network devices.**
- **B. To securely transfer files.**
- **C. To deliver streaming media.**
- **D. To manage network routing tables.**

8. Which of the following is a common use case for TCP?

- **A. Web browsing, where data integrity is crucial.**
- **B. Email delivery, where reliability is less critical.**
- **C. Live video streaming, where speed is critical.**
- **D. Remote terminal access to devices.**

9. What does SIP stand for?

- **A. Session Initiation Protocol**
- **B. Secure Internet Protocol**
- **C. Session Internal Protocol**
- **D. Signaling Internet Protocol**

10. What is DNS over TLS (DoT)?

- **A. A method for encrypted DNS communication using a dedicated port.**
- **B. A protocol for validating DNS records with signatures.**
- **C. A method for distributing DNS zone files via TLS.**
- **D. A standard for DNS query prioritization.**

Answers

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

Explanations

1. Which statement describes the main difference between TCP and UDP as addressed in the material?

A. TCP is designed for reliability, while UDP prioritizes speed and does not guarantee delivery.

B. TCP is connectionless and UDP is connection-oriented.

C. TCP uses IP whereas UDP does not.

D. TCP operates only on LAN, UDP only on WAN.

The main idea here is the trade-off between reliability and performance in transport protocols. TCP provides reliable, connection-oriented delivery with mechanisms for ensuring data arrives correctly and in order, including acknowledgments, retransmission, and flow/congestion control. UDP, on the other hand, is a lightweight, connectionless protocol that sends datagrams with minimal overhead and no built-in guarantees of delivery, order, or duplication protection. This is why the statement that TCP is designed for reliability while UDP prioritizes speed and does not guarantee delivery is the best description. The other options don't fit because TCP is not connectionless (it's connection-oriented) and UDP is not connection-oriented. Both TCP and UDP run over IP, so one does not "use IP" while the other does not. And neither protocol is limited to LAN or WAN; both can operate across local networks and wide areas depending on the routing.

2. Which statement about DNS hierarchy is true?

A. It serves to distribute management of domain name data across multiple servers.

B. It stores all DNS records in a single centralized server.

C. It translates IP addresses into MAC addresses for local networks.

D. It requires no servers to function.

DNS uses a hierarchical structure to distribute management of domain name data across multiple servers. This design places root servers at the top, directing queries to the appropriate top-level domain (TLD) servers, which then delegate to authoritative servers for individual domains. By spreading responsibility across many servers, the system scales to the entire Internet, balances load, and provides redundancy—so no single server holds every record. Recursive resolvers can cache responses to speed up repeated lookups, but the data itself is stored across a network of delegated zones. In contrast, translating IP addresses to MAC addresses is handled by ARP for local networks, and DNS inherently relies on servers (root, TLD, and authoritative) to function.

3. Which statement best describes a non-authoritative DNS server?

A. It caches information from authoritative servers.

B. It holds the original data for a domain.

C. It hosts the domain's zone file.

D. It signs DNS responses with DNSSEC.

Non-authoritative DNS servers act as caches and resolvers rather than as the source of truth for domain data. They store responses learned from authoritative servers and answer queries using that cached information, until the records' TTL expires or new data is needed. They don't hold the original domain data or the zone file itself—that role belongs to authoritative servers. They also don't sign DNS responses; signing DNS data is done by the authoritative zone (and, if enabled, validated by resolvers), not by the non-authoritative server.

4. Which mechanism is primarily responsible for ensuring data does not overwhelm the receiver in a TCP connection?

A. Flow control

B. Routing

C. Encryption

D. Compression

Flow control is the mechanism that prevents a sender from overwhelming the receiver in a TCP connection. In TCP, the receiver advertises a receive window (the rwnd) in its acknowledgments, which tells the sender how much data it can buffer. The sender must keep the amount of data in flight (unacknowledged data) within that window. If the receiver's buffer fills up, the advertised window shrinks or becomes zero, causing the sender to pause until more space is available. This keeps the receiver from being flooded with data it can't handle. Routing, encryption, and compression don't manage the pacing of data delivery to the receiver.

5. What is the significance of the OSI model in networking?

A. It guarantees interoperability without standards

B. It provides a framework for understanding and implementing network protocols and services

C. It describes hardware specifications

D. It dictates vendor-unique protocols

Understanding the OSI model provides a layered framework to see how network functions relate and interact. It splits communication into seven layers with distinct responsibilities and interfaces, so designers can modularize tasks from data creation and presentation to reliable transport, routing, and physical transmission. This structure makes it easier to understand, implement, and troubleshoot network protocols and services because you can map functionality to a specific layer and reason about where issues happen or how changes propagate. It's a reference model that guides standards and interoperability, even though many real networks use the TCP/IP stack instead; OSI remains a valuable teaching and design tool. The other statements miss its purpose: it doesn't guarantee interoperability by itself, it isn't about hardware specifications, and it doesn't enforce vendor-unique protocols.

6. How does the Transport Layer recover lost data?

A. By reordering packets only

B. By performing encryption

C. By automatically requesting that the data be sent again

D. By compressing data

The transport layer recovers lost data through automatic retransmission. In protocols like TCP, each data segment carries a sequence number and the receiver sends back acknowledgments when data is received. If an acknowledgment doesn't arrive in time, or if multiple duplicate acknowledgments indicate a missing piece, the sender automatically resends the unacknowledged data. This retransmission mechanism is what restores lost information and ensures reliable delivery. Encryption or compression don't fix lost data, and reordering alone doesn't recover missing packets; only retransmission guarantees the data eventually gets through.

7. What is the purpose of TFTP?

A. To perform simple file transfers, particularly in booting or configuring network devices.

B. To securely transfer files.

C. To deliver streaming media.

D. To manage network routing tables.

The main concept here is that TFTP is built for simple, quick file transfers used during booting or initial configuration of network devices. It's a lightweight protocol that operates over UDP and intentionally keeps features to a minimum, without built-in authentication or encryption. Because of its simplicity, it's ideal for tasks like loading a bootloader or operating system image, and fetching configuration files during startup or during network device setup (for example, PXE boot scenarios). This is why it's the best fit: in environments where a device needs to obtain essential files quickly and with minimal overhead, TFTP provides that straightforward transfer mechanism. It's not designed for secure transfers, since there's no encryption or authentication. It's also not used for streaming media, which requires protocols designed for continuous data delivery and timing, nor for managing routing tables, which relies on routing protocols and administrative tools.

8. Which of the following is a common use case for TCP?

A. Web browsing, where data integrity is crucial.

B. Email delivery, where reliability is less critical.

C. Live video streaming, where speed is critical.

D. Remote terminal access to devices.

TCP is designed for applications that need reliable, in-order delivery with error checking. Web browsing fits this perfectly because a page is made up of multiple resources (HTML, CSS, images, scripts) that must arrive intact and in the correct sequence for the browser to render properly. TCP provides a three-way handshake to establish a connection, sequence numbers and acknowledgments to track data, retransmission of any lost segments, and checksums to detect corruption. It also uses flow control to prevent overwhelming the client and congestion control to adjust the sending rate based on network conditions. All of these features ensure pages load correctly and completely, making web browsing a classic TCP use case. Live video streaming prioritizes low latency and can tolerate some data loss, so it often favors faster, best-effort delivery (like UDP) rather than TCP's strict reliability. Email delivery does rely on reliability, contrary to the idea that reliability is less critical, and remote terminal access also benefits from TCP's reliability, but the ubiquitous and everyday nature of web page loading makes it the most representative example of TCP's common use.

9. What does SIP stand for?

A. Session Initiation Protocol

B. Secure Internet Protocol

C. Session Internal Protocol

D. Signaling Internet Protocol

SIP stands for Session Initiation Protocol, a signaling protocol used to start, modify, and terminate multimedia sessions such as voice and video calls over IP networks. It operates at the application layer and handles tasks like locating users, establishing who is in a session, negotiating media capabilities, and signaling call setup and teardown. The actual media (voice or video) is typically carried separately, often using RTP, once SIP has established the session. SIP messages are text-based and include requests like INVITE, ACK, and BYE to manage the session lifecycle. This makes it the correct meaning for SIP. The other options refer to different concepts (for example, IPsec for securing IP traffic or a nonstandard "Session Internal Protocol"), which don't describe SIP's role in initiating and managing multimedia sessions.

10. What is DNS over TLS (DoT)?

A. A method for encrypted DNS communication using a dedicated port.

B. A protocol for validating DNS records with signatures.

C. A method for distributing DNS zone files via TLS.

D. A standard for DNS query prioritization.

DNS over TLS is about wrapping DNS queries in a TLS session so the communication between a client and resolver is encrypted and protected from eavesdropping or tampering. It uses a dedicated TLS port, typically 853, to keep DNS traffic separate from ordinary web traffic. This is what makes DoT different from plain DNS (which is unencrypted) and from DNS over HTTPS, which runs DNS queries over HTTPS on port 443. It's not about signing DNS records (that's DNSSEC), transferring zone data, or prioritizing queries.

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://transportlayerprotocolsfunctions.examzify.com

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