Transport Layer Protocols and Functions in Networking Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Table of Contents

SAMPLE

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. **How does the Transport Layer interact with the Network Layer?**
   A. The Transport Layer passes data down to the Network Layer for routing to the destination.
   B. The Network Layer passes data up to the Transport Layer for processing by the application.
   C. They operate independently with no interaction.
   D. The Transport Layer handles IP addressing directly.

2. **What is the main characteristic of TCP?**
   A. It is connection-oriented and ensures reliable data transmission.
   B. It is connectionless and fastest.
   C. It does not guarantee delivery.
   D. It uses datagrams and no segmentation.

3. **What is the primary purpose of MX records?**
   A. They specify mail servers responsible for receiving email for the domain.
   B. They map domain names to IP addresses.
   C. They indicate reverse DNS mappings for the domain.
   D. They designate the authoritative DNS server for the domain.

4. **Which statement best describes UDP in relation to reliability?**
   A. It does not guarantee reliability and may deliver packets out of order.
   B. It always ensures in-order delivery.
   C. It uses acknowledgment to guarantee delivery.
   D. It enforces flow control.

5. **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

6. **What is the purpose of SNMP?**

   A. To manage and monitor network devices

   B. To encrypt directory services

   C. To initialize voice sessions

   D. To assign IP addresses

7. **Which statement best describes how a hosts file compares to DNS in a network?**

   A. It is a local manual mapping on a device, whereas DNS is a distributed resolution system.

   B. It automatically updates domain mappings from the internet.

   C. It caches DNS responses for all devices on a network.

   D. It monitors DNS query traffic to optimize resolution.

8. **What is the secure version of HTTP?**

   A. Hypertext Transfer Protocol (HTTP)

   B. Hypertext Transfer Protocol Secure (HTTPS)

   C. Simple Network Management Protocol (SNMP)

   D. Network Time Protocol (NTP)

9. **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.

10. **Which DNS server caches information from authoritative servers?**

    A. Non-Authoritative DNS Server.

    B. Authoritative DNS Server.

    C. Primary DNS Server.

    D. Secondary DNS Server.

Answers

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

Explanations

1. **How does the Transport Layer interact with the Network Layer?**

   A. The Transport Layer passes data down to the Network Layer for routing to the destination.

   B. The Network Layer passes data up to the Transport Layer for processing by the application.

   C. They operate independently with no interaction.

   D. The Transport Layer handles IP addressing directly.

The Transport Layer interacts with the Network Layer by passing the data it receives from the application down to the Network Layer for routing to the destination. The transport layer prepares segments (with port numbers) and hands them to the Network Layer, which adds IP addressing and handles routing. On the receiving side, the Network Layer passes the packet up to the Transport Layer, which uses the port information to deliver the data to the correct application. IP addressing is a responsibility of the Network Layer, not the Transport Layer, so that layer does the routing work while the Transport Layer focuses on end-to-end delivery and port multiplexing.

2. **What is the main characteristic of TCP?**

   A. It is connection-oriented and ensures reliable data transmission.

   B. It is connectionless and fastest.

   C. It does not guarantee delivery.

   D. It uses datagrams and no segmentation.

TCP's defining trait is that it is connection-oriented and provides reliable data transmission. Before any data moves, TCP sets up a dedicated session between the endpoints using a three-way handshake, establishing an end-to-end connection. Once the connection is in place, data is sent as a stream and is divided into segments with sequence numbers. The receiver acknowledges received data, and if an acknowledgment is missing or a timeout occurs, the sender retransmits the relevant segment, ensuring the data arrives correctly and in order. Flow control (the sliding window) and congestion control modulate the sending rate to prevent overwhelming the network or the receiver, reinforcing reliable delivery. Because TCP prioritizes accuracy and order over raw speed, it is typically slower than connectionless protocols. It also differs from datagram-based approaches by delivering a continuous byte stream rather than discrete, independent messages.

3. What is the primary purpose of MX records?

A. They specify mail servers responsible for receiving email for the domain.

B. They map domain names to IP addresses.

C. They indicate reverse DNS mappings for the domain.

D. They designate the authoritative DNS server for the domain.

MX records specify the mail servers that receive email for a domain. They list the hostnames of the mail exchangers and include a priority value to indicate which server should be tried first. When an email is sent to an address at that domain, the sending mail transfer agent looks up the domain's MX records to find the destination mail server and then delivers the message via SMTP. The lower priority number means higher preference, so if the primary server can't be reached, delivery can be attempted to the next one in order. This is distinct from other DNS records: A or AAAA records map domain names to IP addresses, PTR records provide reverse DNS mappings from IP addresses back to domain names, and NS records designate the authoritative DNS servers for the domain. An MX record must point to a host name that has its own reachable A or AAAA record so the mail server can actually be reached.

4. Which statement best describes UDP in relation to reliability?

A. It does not guarantee reliability and may deliver packets out of order.

B. It always ensures in-order delivery.

C. It uses acknowledgment to guarantee delivery.

D. It enforces flow control.

UDP is a connectionless, best-effort transport protocol that does not provide reliability. There is no acknowledgment, no retransmission, and no sequencing guarantees, so datagrams can arrive out of order or be lost. Because of this, UDP does not enforce flow control and leaves reliability and ordering to the application or higher-layer protocols. That's why the statement describing UDP in relation to reliability is that it does not guarantee reliability and may deliver packets out of order. If reliability is required, the application must implement it itself or use a protocol like TCP.

5. 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.

6. What is the purpose of SNMP?

A. To manage and monitor network devices

B. To encrypt directory services

C. To initialize voice sessions

D. To assign IP addresses

SNMP is used to manage and monitor network devices from a central system. It lets a manager query devices (via agents on the devices) to read status, performance, and configuration data stored in MIBs, and it can receive alerts (traps) when something needs attention. This combination—collecting metrics, monitoring health, and enabling alerts from a centralized point—is exactly what SNMP is designed for. The other options describe functions from different areas: encrypting directory services isn't what SNMP does, initializing voice sessions is the role of signaling protocols for voice, and assigning IP addresses is handled by DHCP.

7. Which statement best describes how a hosts file compares to DNS in a network?

A. It is a local manual mapping on a device, whereas DNS is a distributed resolution system.

B. It automatically updates domain mappings from the internet.

C. It caches DNS responses for all devices on a network.

D. It monitors DNS query traffic to optimize resolution.

The main idea here is that a hosts file is a local, manual mapping of names to IP addresses on a single device, while DNS is a distributed system that resolves names across many servers. A hosts file sits on the device and is read directly by the operating system. You or an admin explicitly add entries there, so the mapping is immediate for that machine and does not rely on any network service. DNS, in contrast, uses a hierarchy of servers to translate names into addresses for the entire network or internet, with resolvers and caches helping to scale the process. That's why the description that fits best is: the hosts file is a local manual mapping on a device, whereas DNS is a distributed resolution system. The other statements don't fit: the hosts file doesn't automatically update mappings from the internet; it requires manual edits. It isn't a shared cache for all devices, so it doesn't cache DNS responses. It also doesn't monitor DNS query traffic to optimize resolution; that would be a separate monitoring or analytics activity.

8. What is the secure version of HTTP?

A. Hypertext Transfer Protocol (HTTP)

B. Hypertext Transfer Protocol Secure (HTTPS)

C. Simple Network Management Protocol (SNMP)

D. Network Time Protocol (NTP)

HTTPS is the secure version of HTTP, because it runs HTTP over TLS/SSL to provide encryption, authentication, and data integrity for data in transit. This means the data between your browser and the web server is encrypted, so eavesdroppers can't read it, and tampering or impersonation is detected. The server's certificate helps verify you're talking to the legitimate site. In contrast, plain HTTP sends data in plaintext and offers no built-in protection. The other options are different protocols: SNMP is for managing network devices, and NTP is for clock synchronization, neither of which secures web traffic.

9. 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.

10. Which DNS server caches information from authoritative servers?

A. Non-Authoritative DNS Server.

B. Authoritative DNS Server.

C. Primary DNS Server.

D. Secondary DNS Server.

Caching of DNS responses is done by non-authoritative (recursive) resolvers. When a client asks for a domain, the recursive resolver fetches the answer by querying the root, then the appropriate top-level domain servers, and finally the authoritative server for that domain. It then stores the returned data in its cache for the time-to-live (TTL) specified by the authoritative source. This means subsequent requests for the same domain can be answered quickly from the cache without re-contacting the authoritative servers, until the TTL expires. Authoritative servers hold and serve the definitive zone data and are not primarily about caching for general client queries. Primary and secondary servers describe the master/slave setup for a zone on authoritative servers, not the caching layer used to accelerate client lookups.

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!