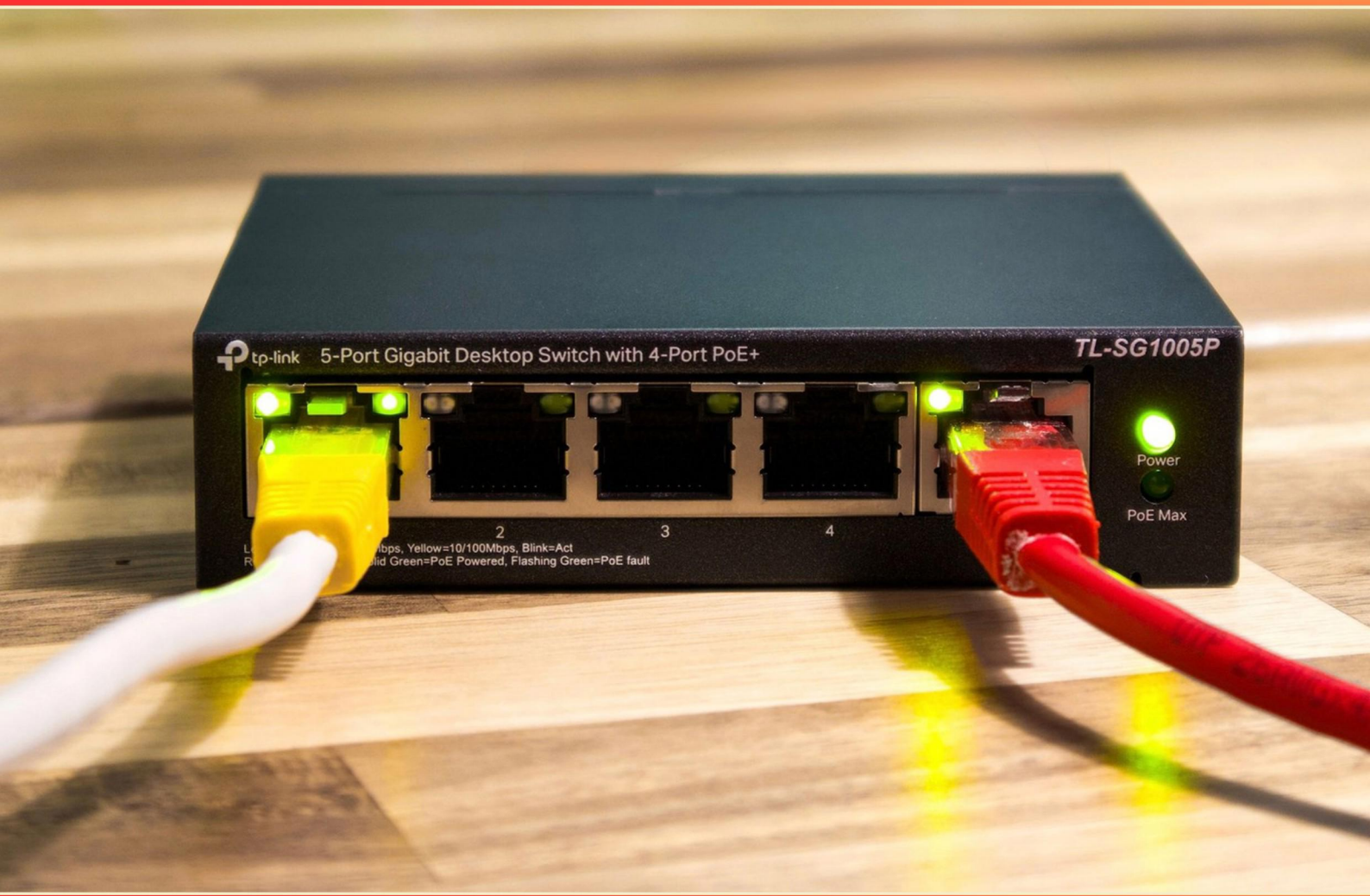
TRANSPORT LAYER PROTOCOLS AND FUNCTIONS IN NETWORKING PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://transportlayerprotocolsfunctions.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

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

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. Which protocol transfers web pages, images, and other content between web servers and clients?

A. Hypertext Transfer Protocol (HTTP)

B. Hypertext Transfer Protocol Secure (HTTPS)

C. Simple Mail Transfer Protocol Secure (SMTPS)

D. Server Message Block (SMB)

2. What is Precision Time Protocol (PTP)?

A. A protocol for very precise time synchronization, down to the nanosecond

B. A protocol for securing SIP signaling

C. A protocol for DNS resolution caching

D. A protocol for packet compression

3. Which set of fields constitutes the 4-tuple used by the transport layer to identify a specific connection?

A. Source IP, Destination IP, Source Port, Destination Port

B. Source IP, Destination IP, Protocol, Time To Live

C. Source Port, Destination Port, Source IP, Destination IP

D. Destination IP, Source IP, Time To Live, Protocol

4. How does time-out retransmission differ from fast retransmit?

A. Time-out retransmission triggers when no ACK is received within a timeout; fast retransmit triggers when duplicate ACKs are received.

B. Time-out retransmission uses duplicate ACKs; fast retransmit uses a timer.

C. They are the same.

D. Time-out retransmission only applies to UDP.

5. Which layer in the OSI model is responsible for providing network services to end-user applications?

A. Application Layer

B. Data Link Layer

C. Physical Layer

D. Network Layer

SAMPLE

6. Which OSI layer is responsible for translating data formats to ensure readability on the receiving end?

A. Session Layer

B. Presentation Layer

C. Transport Layer

D. Network Layer

7. What is the purpose of DNS over HTTPS (DoH)?

A. To encrypt DNS queries and responses for privacy and security.

B. To route DNS over a dedicated port for performance.

C. To speed up DNS resolution by caching results.

D. To publish DNS records as HTTP resources.

8. What happens to data as it moves through the OSI model layers?

A. It is decrypted at each layer

B. It is encapsulated with headers and processed at each layer

C. It is transmitted without changes

D. Each layer only forwards data without modification

9. What does MSS stand for in TCP, and what is its primary purpose?

A. Maximum Segment Size; it limits the payload per segment to avoid IP fragmentation and optimize transmission efficiency

B. Maximum Service Size; it defines the maximum service payload for TCP processing

C. Minimum Segment Size; it sets the smallest allowed TCP segment

D. Message Segments Size; it controls how messages are segmented for TCP

10. What is the main function of the DNS hierarchy?

A. To manage and distribute information about domain names across different servers.

B. To assign dynamic IPs to devices automatically.

C. To replace the need for any local DNS queries.

D. To map domain names to physical hardware addresses.

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which protocol transfers web pages, images, and other content between web servers and clients?

A. Hypertext Transfer Protocol (HTTP)

B. Hypertext Transfer Protocol Secure (HTTPS)

C. Simple Mail Transfer Protocol Secure (SMTPS)

D. Server Message Block (SMB)

HTTP is the protocol that defines how a web client (like a browser) requests resources and how a server responds, enabling the transfer of web pages, images, styles, scripts, and other content. The client sends a request for a resource, the server returns a status code along with the resource, and this request–response cycle is what delivers web content to your screen. HTTPS exists as a secure variant of this protocol, adding encryption and authentication, but it still uses the same mechanism to transfer content; the distinction is secure transport, not a different content-delivery protocol. The other options serve different purposes: SMTPS is for securely sending email, and SMB is for file sharing on local networks, not for retrieving web content from servers.

2. What is Precision Time Protocol (PTP)?

A. A protocol for very precise time synchronization, down to the nanosecond

B. A protocol for securing SIP signaling

C. A protocol for DNS resolution caching

D. A protocol for packet compression

Precision Time Protocol is about synchronizing clocks across a network with extremely high accuracy, often down to nanoseconds. Devices exchange timestamped messages to measure how long signals take to travel and to adjust local clocks so they all stay in tight lockstep. Achieving this precision relies on features like a master clock distributing time, slave clocks following it, and hardware timestamping to reduce measurement errors. The standard is defined by IEEE 1588 and is used in environments where coordinated timing is crucial, such as telecom networks, financial trading systems, industrial automation, and power-grid control. The other options don't fit because PTP isn't about securing SIP signaling, DNS resolution caching, or packet compression.

3. Which set of fields constitutes the 4-tuple used by the transport layer to identify a specific connection?

A. Source IP, Destination IP, Source Port, Destination Port

B. Source IP, Destination IP, Protocol, Time To Live

C. Source Port, Destination Port, Source IP, Destination IP

D. Destination IP, Source IP, Time To Live, Protocol

The transport layer identifies a specific connection by the combination of who is communicating and which applications are involved on each end. That means the four fields are the source and destination IP addresses (which host is talking to which host) plus the source and destination ports (which application on each host is using the connection). This four-field identifier uniquely distinguishes one transport connection from another between the same pair of hosts, even if they are exchanging data on the same port numbers. Fields like Time To Live or Protocol belong to routing and higher-layer signaling, not to the per-connection identity at the transport layer. TTL can change as packets traverse networks, and Protocol only indicates which upper-layer protocol is being used (TCP or UDP), not which specific connection it represents. So the correct set is Source IP, Destination IP, Source Port, Destination Port.

SAMPLE

4. How does time-out retransmission differ from fast retransmit?

A. Time-out retransmission triggers when no ACK is received within a timeout; fast retransmit triggers when duplicate ACKs are received.

B. Time-out retransmission uses duplicate ACKs; fast retransmit uses a timer.

C. They are the same.

D. Time-out retransmission only applies to UDP.

The main idea tested is how TCP detects and handles lost data through two different retransmission mechanisms. Time-out retransmission happens when the sender's retransmission timer expires without seeing an acknowledgment for the segment. That timeout signals a likely loss, so the sender retransmits the unacknowledged data and typically enters a more cautious congestion window adjustment. Fast retransmit, on the other hand, is triggered earlier by the reception of duplicate acknowledgments. When the receiver keeps acknowledging the last in-order byte and repeats the same acknowledgment, the sender infers that a segment within the window was lost behind what has already been received. After detecting a certain number of duplicate ACKs (commonly three), the sender quickly retransmits the presumed missing segment without waiting for the timer, often followed by a more limited adjustment of the congestion window (fast recovery). So the correct statement captures that time-out retransmission relies on a timer, while fast retransmit relies on duplicate ACKs to detect loss earlier. The other options misstate who uses the timer, claim they are the same, or wrongly tie time-out retransmission to UDP.

5. Which layer in the OSI model is responsible for providing network services to end-user applications?

A. Application Layer

B. Data Link Layer

C. Physical Layer

D. Network Layer

The key idea is which layer directly offers the network-facing services that end-user applications use. The Application Layer sits at the top of the OSI model and provides protocols and services that applications rely on to communicate over a network—think HTTP for web pages, SMTP for email, FTP for file transfer, DNS for name resolution, and similar interfaces. It translates user requests into network data and presents received data to applications in a usable form, handling things like data representation and user-facing services. The other layers handle the mechanics of transmission rather than providing services to applications. The Data Link Layer takes care of framing, error detection, and access to the local link. The Physical Layer deals with the actual electrical, optical, or radio signals and hardware. The Network Layer handles routing and addressing to move packets between networks. Because they don't offer direct services to end-user applications, they aren't the layer described in the question.

SAMPLE

6. Which OSI layer is responsible for translating data formats to ensure readability on the receiving end?

A. Session Layer

B. Presentation Layer

C. Transport Layer

D. Network Layer

Translating data formats so the receiving end can read the information is the job of the Presentation layer. This layer handles syntax and data representation, performing tasks like character encoding conversions, data encoding schemes, and, when needed, compression or encryption so that the data arrives in a form the application can understand. It sits between the Session layer, which manages dialogue and connections, and the Application layer, which uses the data directly. By converting and formatting data for the other end, the presentation layer ensures consistent interpretation regardless of how the data was originally encoded or compressed. The other layers don't perform this translation: the Session layer manages connections, the Transport layer ensures delivery, and the Network layer handles routing. So, the Presentation layer is the one responsible for translating data formats for readability.

7. What is the purpose of DNS over HTTPS (DoH)?

A. To encrypt DNS queries and responses for privacy and security.

B. To route DNS over a dedicated port for performance.

C. To speed up DNS resolution by caching results.

D. To publish DNS records as HTTP resources.

DNS over HTTPS aims to protect the privacy and integrity of DNS queries by carrying them inside HTTPS with TLS encryption. Because the DNS messages are encrypted, onlookers can't easily see which domains you're asking about or tamper with the responses as they travel across networks. That privacy and security benefit is the core reason for DoH. It isn't primarily about using a special port, speeding up lookups, or publishing DNS records as HTTP resources. DoH uses HTTPS (usually over standard ports like 443), so the traffic looks like regular web traffic rather than traditional DNS traffic. Caching and speed depend more on the resolver and network conditions than on the DoH transport itself, and publishing records as HTTP resources is not what DoH does.

8. What happens to data as it moves through the OSI model layers?

A. It is decrypted at each layer

B. It is encapsulated with headers and processed at each layer

C. It is transmitted without changes

D. Each layer only forwards data without modification

As data moves through the OSI layers, each layer wraps the data with its own header (and sometimes a trailer) and performs its designated processing. This encapsulation adds control information needed for functions like routing, error detection, sequencing, and port addressing as the data descends from the application toward the physical layer. When the data reaches the destination, the process is reversed: each layer decapsulates by removing its header and passes the remaining data up to the next layer, until the original data is delivered to the application. This behavior—encapsulation at each layer with headers and layered processing—best describes what happens.

SAMPLE

9. What does MSS stand for in TCP, and what is its primary purpose?

A. Maximum Segment Size; it limits the payload per segment to avoid IP fragmentation and optimize transmission efficiency

B. Maximum Service Size; it defines the maximum service payload for TCP processing

C. Minimum Segment Size; it sets the smallest allowed TCP segment

D. Message Segments Size; it controls how messages are segmented for TCP

The main idea tested here is understanding what MSS means in TCP and why it matters. MSS stands for Maximum Segment Size, and its primary purpose is to cap how much TCP data can be carried in a single segment. This value represents just the payload size of the TCP segment, meaning it does not include the IP or TCP headers. During the TCP handshake, the two ends negotiate an MSS using the MSS option in the SYN packets. The chosen MSS is typically derived from the path MTU (maximum transmission unit) minus the header overhead, so segments stay within what the network path can carry without fragmentation. For example, on a common Ethernet network with a 1500-byte MTU, the typical MSS is about 1460 bytes. Keeping segments within this limit helps avoid IP fragmentation, which can degrade performance and reliability because fragmented packets are more likely to be dropped or reordered. Keep in mind that MSS is not the same as MTU. MTU is the maximum size of an entire IP packet on a link, including headers, whereas MSS is specifically the maximum TCP data payload that a segment can carry. The other options don't match TCP terminology: there isn't a service size, minimum segment size, or message segment size in standard TCP usage.

10. What is the main function of the DNS hierarchy?

A. To manage and distribute information about domain names across different servers.

B. To assign dynamic IPs to devices automatically.

C. To replace the need for any local DNS queries.

D. To map domain names to physical hardware addresses.

The main function of the DNS hierarchy is to manage and distribute information about domain names across a network of servers so lookups can be resolved efficiently and reliably. By organizing authority into root servers, top-level domain servers, and delegated zones, DNS spreads responsibility, prevents any single server from becoming a bottleneck, and enables caching for faster responses. When you resolve a name, your local resolver may check its cache, then ask root servers to direct you to the right TLD server, which points to the authoritative server for the domain; that server returns the IP address, and the answer can be cached for future requests. This structure also provides redundancy: many root and DNS servers exist so queries can still complete if some servers fail. Other options describe functions not performed by DNS. Dynamic IP assignment is handled by DHCP. DNS does not eliminate local queries; it complements them and relies on caching and local configurations. Domain names are mapped to IP addresses, not to hardware addresses; mapping to physical hardware addresses is done by ARP on the local network.

SAMPLE

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!

SAMPLE