GCIA Fundamentals of Traffic Analysis 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 IPv6 prefix denotes a link-local address?

A. ::1/128

B. fe80::/10

C. 2000::/3

D. ff00::/8

2. Which statement describes SEND's security feature?

A. A cryptographic security for sender address verification

B. Increased speed of address resolution

C. Requires no key management

D. Eliminates all overhead

3. Fragment offset values are always multiples of which number?

A. 4

B. 16

C. 8

D. 2

4. What is the purpose of a Teredo Bubble Packet?

A. Initial tunnel negotiation

B. Data transfer initiation

C. Error reporting

D. Keep-alive signaling

5. Which statement correctly describes how to derive the header length from the IHL value?

A. IHL is expressed in bytes; header length in bytes equals IHL times 4.

B. IHL is expressed in 32-bit words; header length is equal to IHL.

C. IHL is expressed in 16-bit words; header length equals IHL times 2.

D. IHL is unrelated to header length.

6. Cyclic Redundancy Check (CRC) in Ethernet frames is how many bytes?

A. 2 bytes

B. 8 bytes

C. 4 bytes

D. 6 bytes

7. DHCPv6 uses which UDP ports?

A. 547 548

B. 546 548

C. 546 547

D. 67 68

8. What is Gratuitous ARP?

A. Send ARP requests to broadcast with sender and target address the same (sender's address)

B. Respond to ARP requests with its own address

C. Broadcast its IP/MAC pairing to segment

D. Request broadcast to refresh ARP table periodically

9. What does the ECN value 01/10 signify?

A. Not Protocol aware or negotiating

B. 01/10: Both endpoints are protocol aware

C. Congestion experienced and marked by router

D. Reserved for future use

10. Which IPv4 address block is reserved for documentation and examples?

A. 198.51.100.0/24

B. 203.0.113.0/24

C. 198.18.0.0/15

D. 192.0.2.0/24

Answers

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

Explanations

1. Which IPv6 prefix denotes a link-local address?

A. ::1/128

B. fe80::/10

C. 2000::/3

D. ff00::/8

Link-local addresses are valid only on the local link and aren't routed beyond that single network segment. The prefix that designates this scope is fe80::/10, which covers addresses from fe80 to febf. Interfaces automatically generate a link-local address for local communication and neighbor discovery. Other prefixes correspond to different scopes or purposes—::1/128 is the loopback address for a single host, 2000::/3 is global unicast space for internet-facing addresses, and ff00::/8 is used for multicast. So fe80::/10 is the link-local prefix.

2. Which statement describes SEND's security feature?

A. A cryptographic security for sender address verification

B. Increased speed of address resolution

C. Requires no key management

D. Eliminates all overhead

Secure Neighbor Discovery (SEND) adds cryptographic proof to IPv6 neighbor discovery messages, so receivers can trust that the sender really owns the advertised address. The core feature is cryptographic verification of the sender's address, achieved through mechanisms like Cryptographically Generated Addresses (CGA) and digital signatures on neighbor solicitation and neighbor advertisement messages. This binding of an address to a public key lets other nodes verify the origin of NDP messages and prevents spoofing of both the address and the message. Because of this cryptographic layer, SEND focuses on ensuring that a host cannot impersonate another by simply sending fraudulent NDP traffic. These choices don't fit SEND's purpose: increasing speed of address resolution would conflict with the extra cryptographic processing SEND requires, and saying no key management is needed ignores the cryptographic keys involved in CGA verification. Likewise, eliminating all overhead is inaccurate because the security features add processing and message size overhead.

3. Fragment offset values are always multiples of which number?

A. 4

B. 16

C. 8

D. 2

Fragment offset is defined in units of eight bytes. When a datagram is fragmented, every fragment must start at an 8-byte boundary in the original payload, so the actual byte position where a fragment begins is a multiple of eight. The value stored in the header tells how many 8-byte blocks into the datagram this fragment starts, and you multiply by eight to get the byte offset. For example, an offset value of 3 means the fragment starts at byte 24. This 8-byte alignment is why the correct choice is eight.

4. What is the purpose of a Teredo Bubble Packet?

A. Initial tunnel negotiation

B. Data transfer initiation

C. Error reporting

D. Keep-alive signaling

Keep-alive signaling. In Teredo, NAT devices and firewalls can drop mappings if there's no traffic for a while. A Teredo Bubble Packet is a tiny UDP packet sent periodically to refresh the NAT translation and verify the path to the Teredo relay, ensuring the IPv6 tunnel stays usable even when no actual data is being transferred. It's not about starting a tunnel, carrying data, or reporting errors—its role is to keep the tunnel alive.

5. Which statement correctly describes how to derive the header length from the IHL value?

A. IHL is expressed in bytes; header length in bytes equals IHL times 4.

B. IHL is expressed in 32-bit words; header length is equal to IHL.

C. IHL is expressed in 16-bit words; header length equals IHL times 2.

D. IHL is unrelated to header length.

The value in the IHL field represents the header length in 32-bit words, not in bytes. To get the header length in bytes, multiply IHL by 4 (since each 32-bit word is 4 bytes). For example, an IHL of 5 means a 20-byte header (5 × 4). If options are present, IHL increases accordingly, up to a maximum of 15 (60 bytes). This conversion—IHL × 4—is what you use to derive the actual header length from the IHL value.

6. Cyclic Redundancy Check (CRC) in Ethernet frames is how many bytes?

A. 2 bytes

B. 8 bytes

C. 4 bytes

D. 6 bytes

Ethernet frames carry a trailer called the Frame Check Sequence that holds a 32-bit CRC, i.e., four bytes. This CRC is computed over the frame's header and payload, and the receiver recalculates it on arrival to verify integrity by comparing it to the FCS. If they match, the frame is considered intact; if not, it's discarded as corrupted. A 16-bit CRC would offer less protection, an 8-byte field is larger than standard for Ethernet, and six bytes is the length of a MAC address, not the CRC.

7. DHCPv6 uses which UDP ports?

A. 547 548

B. 546 548

C. 546 547

D. 67 68

DHCPv6 runs over UDP and uses two specific ports to separate client and server messages. The client sends its request from UDP port 546 to the server's UDP port 547, and the server replies from 547 back to the client's 546. This handshake-style port usage keeps IPv6 address assignment traffic properly directed between the two ends. In contrast, DHCP for IPv4 uses ports 67 and 68, which is not how DHCPv6 operates. So the correct ports are 546 and 547.

8. What is Gratuitous ARP?

A. Send ARP requests to broadcast with sender and target address the same (sender's address)

B. Respond to ARP requests with its own address

C. Broadcast its IP/MAC pairing to segment

D. Request broadcast to refresh ARP table periodically

Gratuitous ARP is an ARP request sent to all devices on the local network to announce the sender's own IP-to-MAC mapping. The key is that the request uses the sender's IP as both the source and the target, and it's broadcast so every host on the segment hears it. This unsolicited broadcast updates neighbors' ARP caches with the new mapping and helps detect IP address conflicts, since another device using the same IP would respond and reveal the clash. That's why the best description is the one that says it sends ARP requests to broadcast with the sender's address as both the sender and the target. The other options describe ARP replies or general broadcasting of a mapping or periodic refresh—behaviors that don't capture the specific unsolicited, self-addressed ARP announcement meant by gratuitous ARP.

9. What does the ECN value 01/10 signify?

A. Not Protocol aware or negotiating

B. 01/10: Both endpoints are protocol aware

C. Congestion experienced and marked by router

D. Reserved for future use

ECN uses two bits in the IP header to indicate whether endpoints support ECN and to signal congestion. The two-bit field has defined codepoints: 00 means not ECN-capable, 01 and 10 indicate ECN-capable (ECT) endpoints, and 11 means congestion has been experienced (CE). When you see 01 or 10, it shows that both ends of the communication are ECN-capable, so ECN can be used for congestion signaling (routers may mark CE without dropping packets). That's why this option—the indication that both endpoints are protocol aware—best fits the meaning of 01/10. The other codepoints correspond to different states: 00 is not ECN-capable, 11 is congestion experienced, and "reserved for future use" does not apply here.

10. Which IPv4 address block is reserved for documentation and examples?

A. 198.51.100.0/24

B. 203.0.113.0/24

C. 198.18.0.0/15

D. 192.0.2.0/24

Documentation and example blocks are set aside so you can show network addresses without risking real routes or allocations. This is defined in RFC 5737, which designates three IPv4 blocks for documentation and examples: 192.0.2.0/24, 198.51.100.0/24, and 203.0.113.0/24. These ranges are reserved and not assigned for actual use on the public Internet. The block 198.18.0.0/15, by contrast, is reserved for benchmarking inter-network interconnect tests, not for documentation. So, among the options, the blocks suitable for documentation examples are the ones in the 192.0.2.0/24, 198.51.100.0/24, and 203.0.113.0/24 ranges (with 192.0.2.0/24 often cited as the canonical example).

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://gciafundoftrafficanalysis.examzify.com

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