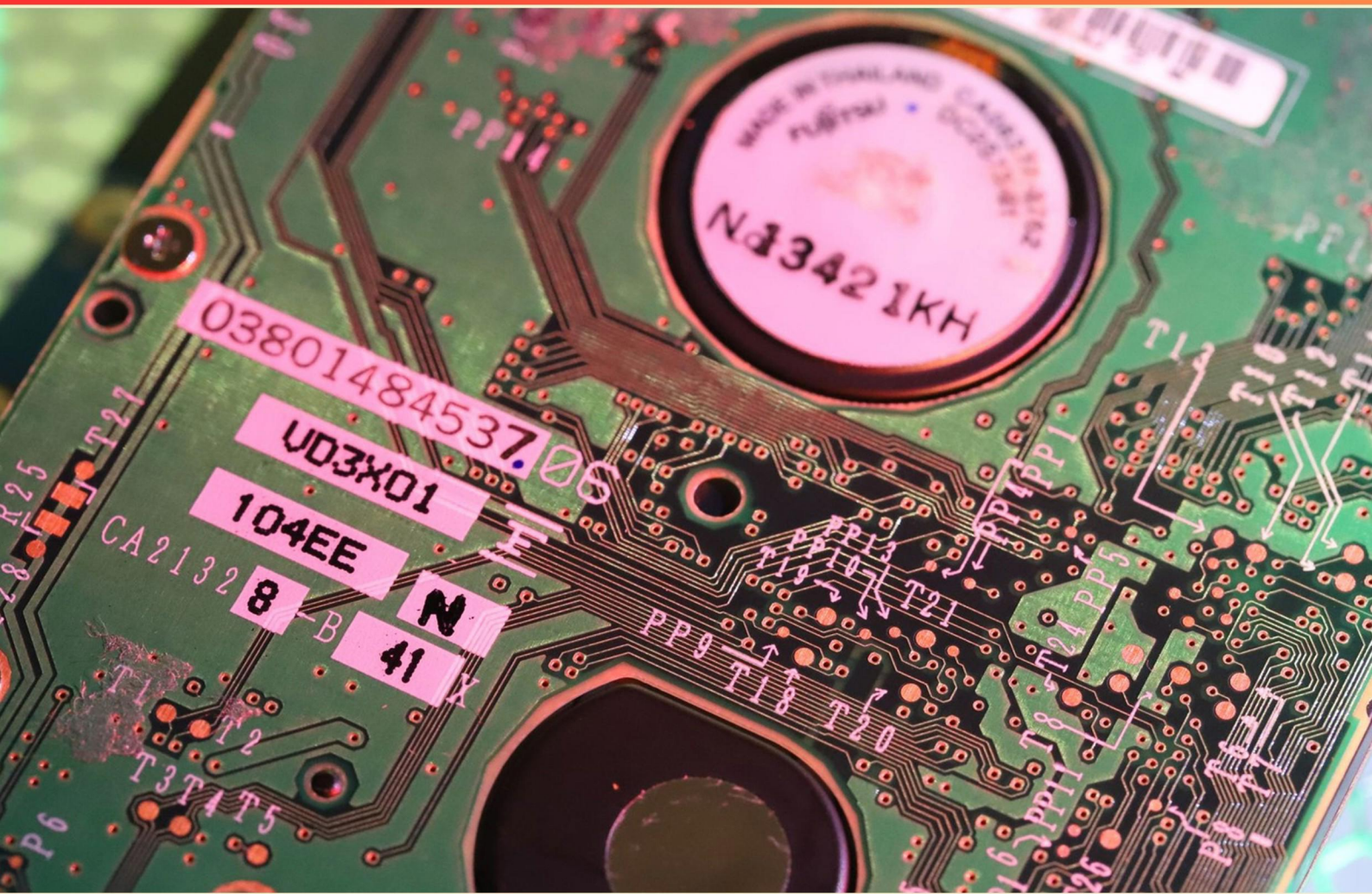


COMPTIA A+ CORE 1 (220-1201) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR
THE FULL VERSION STUDY GUIDE

<https://comptiaapluscore12201201.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	16

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

SAMPLE

- 1. What is the advantage of using Orthogonal Frequency Division Multiplexing (OFDM)?**
 - A. Greater susceptibility to EMI
 - B. Higher data rates and reduced interference
 - C. Simpler implementation
 - D. Lower frequency usage
- 2. Which wireless technology is commonly used for point-to-point connections?**
 - A. Wi-Fi/802.11
 - B. Bluetooth
 - C. Near Field Communication (NFC)
 - D. Zigbee
- 3. What component typically handles the processing function of a computer?**
 - A. Power Supply
 - B. Central Processing Unit (CPU)
 - C. Graphics Card
 - D. Hard Drive
- 4. What are the frequency bands used in wireless networking?**
 - A. 2.4 GHz, 5 GHz, 6 GHz
 - B. 1.2 GHz, 3.2 GHz, 6.2 GHz
 - C. 2.5 GHz, 5.5 GHz, 7 GHz
 - D. 2.1 GHz, 4 GHz, 8 GHz
- 5. What is the term for an authentication method that requires two different factors to verify a user's identity?**
 - A. Single Factor Authentication
 - B. Two-Factor Authentication
 - C. Multi-factor Authentication
 - D. Single Sign-On

- 6. Which security protocol is considered highly vulnerable to attack due to its short initialization vector?**
- A. Wi-Fi Protected Access 2
 - B. Wired Equivalent Privacy
 - C. Wi-Fi Protected Access
 - D. Pre-Shared Key
- 7. What type of cabling is needed for PoE support?**
- A. Cat 5 or above
 - B. Cat 6 or above
 - C. Cat 4 or above
 - D. Fiber optic cabling only
- 8. How much RAM is typically suitable for an office workstation?**
- A. 8 GB
 - B. 16 GB
 - C. 32 GB
 - D. 64 GB
- 9. What is the primary purpose of the Tag Protocol Identifier (TPI)?**
- A. To authenticate users
 - B. To specify VLAN membership
 - C. To encrypt data
 - D. To establish user permissions
- 10. Which cable is proprietary to Apple devices and is used for charging and data transfer?**
- A. USB-C Cable
 - B. Lightning Cable
 - C. USB 2.0 Micro B Cable
 - D. USB 2.0 Mini B Cable

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the advantage of using Orthogonal Frequency Division Multiplexing (OFDM)?

- A. Greater susceptibility to EMI
- B. Higher data rates and reduced interference**
- C. Simpler implementation
- D. Lower frequency usage

Orthogonal Frequency Division Multiplexing (OFDM) offers significant advantages in wireless communications, particularly in achieving higher data rates and minimizing interference. This modulation technique divides a single data stream into multiple smaller sub-streams that are transmitted simultaneously over different frequencies. By doing so, OFDM effectively uses the available bandwidth, enabling faster data transmission rates. Additionally, OFDM enhances resistance to interference and multipath fading—a common issue in wireless environments where signals may reflect off surfaces and combine in unpredictable ways. The orthogonality of the frequencies allows them to overlap without causing interference to one another, leading to more reliable communication. This characteristic is especially beneficial in crowded frequency environments where multiple signals are present. In contrast, other concepts like greater susceptibility to electromagnetic interference, simpler implementation, and lower frequency usage may not accurately capture the core benefits of OFDM in networking contexts. These factors could lead to decreased performance or complexity in deployment, making higher data rates and reduced interference the most notable advantages of utilizing OFDM technology.

2. Which wireless technology is commonly used for point-to-point connections?

- A. Wi-Fi/802.11**
- B. Bluetooth
- C. Near Field Communication (NFC)
- D. Zigbee

The correct choice for wireless technology commonly used for point-to-point connections is Wi-Fi/802.11. Wi-Fi technology is designed for both personal and enterprise networking and allows devices to connect directly to each other over a wireless network, which facilitates point-to-point connections in a variety of environments. This capability enables devices such as laptops, smartphones, and printers to communicate directly without the need for physical cables, making it suitable for applications where reliable and high-speed data transfer is required. Wi-Fi technology supports a range of standards under the 802.11 family, which offer varying speeds and distances, and it is commonly utilized in home, office, and outdoor connectivity solutions. This versatility and robustness make Wi-Fi the go-to technology for establishing connections between two distinct devices or a device and an access point in point-to-point scenarios. In contrast, other technologies like Bluetooth are primarily designed for short-range communication between devices, such as connecting peripherals like headsets or mice to computers but are not typically optimized for point-to-point networking on a larger scale. Near Field Communication (NFC) operates over very short distances, usually within a few centimeters, making it unsuitable for broader point-to-point connections. Zigbee focuses on low-power, short-range communication commonly used in lo

3. What component typically handles the processing function of a computer?

- A. Power Supply
- B. Central Processing Unit (CPU)**
- C. Graphics Card
- D. Hard Drive

The Central Processing Unit (CPU) is recognized as the primary component responsible for the processing function in a computer. It acts as the brain of the computer, performing calculations, executing instructions, and managing the flow of information throughout the system. The CPU interprets and carries out program commands, which is essential for all computer operations. The power supply, while vital for providing the necessary electrical energy to all components, does not handle any data processing or execution of tasks. The graphics card, on the other hand, specializes in rendering images and video, offloading graphical tasks from the CPU but is not the primary processor for general computing tasks. Lastly, the hard drive is used for data storage but does not play a role in processing data; it merely retains information needed for the CPU to function effectively. Thus, the CPU is the correct answer, as it is the core component that executes and manages operations within the computer.

4. What are the frequency bands used in wireless networking?

- A. 2.4 GHz, 5 GHz, 6 GHz**
- B. 1.2 GHz, 3.2 GHz, 6.2 GHz
- C. 2.5 GHz, 5.5 GHz, 7 GHz
- D. 2.1 GHz, 4 GHz, 8 GHz

The frequency bands commonly used in wireless networking are 2.4 GHz, 5 GHz, and 6 GHz. These frequency bands are part of the IEEE 802.11 wireless standards, which are widely used for Wi-Fi networks. The 2.4 GHz band has been traditionally used for Wi-Fi since the early days of wireless networking. It offers a longer range and better penetration through walls compared to higher frequencies, but it is also more susceptible to interference from other devices, such as microwaves and Bluetooth devices. The 5 GHz band was introduced to alleviate congestion in the 2.4 GHz band, offering higher data rates and less interference as it has more non-overlapping channels available. This band is especially useful in environments with many devices, such as homes and offices. The introduction of the 6 GHz band marks a significant step in wireless networking, as it allows for even wider channels and more capacity, thus improving performance in environments with high demand for bandwidth. The other frequency options listed do not align with the standard frequency bands used for wireless networking, which is why they do not apply to the context of the question.

5. What is the term for an authentication method that requires two different factors to verify a user's identity?

- A. Single Factor Authentication
- B. Two-Factor Authentication**
- C. Multi-factor Authentication
- D. Single Sign-On

The term for an authentication method that requires two different factors to verify a user's identity is Two-Factor Authentication. This method enhances security by combining two distinct forms of verification, typically something you know (like a password) and something you have (like a mobile device or a token). By requiring these two different factors, Two-Factor Authentication reduces the likelihood of unauthorized access because even if one factor (such as the password) is compromised, the second factor still provides a layer of security. This dual requirement makes it harder for attackers to gain access to accounts and sensitive information. While Multi-Factor Authentication is a broader term that encompasses any use of two or more verification factors (which could include more than just two factors), Two-Factor Authentication specifically refers to the use of exactly two factors. Single Factor Authentication employs just one method of verification, and Single Sign-On allows users to access multiple applications with one set of credentials, which does not inherently involve multiple factors for authentication.

6. Which security protocol is considered highly vulnerable to attack due to its short initialization vector?

- A. Wi-Fi Protected Access 2
- B. Wired Equivalent Privacy**
- C. Wi-Fi Protected Access
- D. Pre-Shared Key

Wired Equivalent Privacy (WEP) is highly vulnerable to attack primarily because of its weak encryption mechanisms, particularly its use of a short initialization vector (IV). The IV, which is a key component in the encryption process, is only 24 bits long in WEP. This limited size makes it susceptible to various types of attacks, such as IV collisions and brute-force attacks. When attackers can observe enough traffic and capture enough IVs, they can exploit the weaknesses inherent in how WEP generates and uses these initialization vectors to break the encryption and gain access to sensitive data on the network. As a result, WEP is considered insecure and has largely been replaced by more robust security protocols, such as Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2), which implement stronger encryption methods and longer key sizes to mitigate these vulnerabilities.

7. What type of cabling is needed for PoE support?

- A. Cat 5 or above
- B. Cat 6 or above**
- C. Cat 4 or above
- D. Fiber optic cabling only

Power over Ethernet (PoE) allows electrical power and data to be transmitted over the same Ethernet cabling. For PoE support, the cabling needs to be capable of carrying the required power levels as well as high-speed data. Cabling rated at Cat 5 and above is actually sufficient for most PoE applications, but using Cat 6 or higher is often recommended because it supports greater bandwidth (up to 10 Gbps at shorter distances) and enhanced performance, particularly over longer runs. Cat 6 cables have better shielding and reduced crosstalk compared to lower categories, which can contribute to more stable connections in environments where PoE is utilized. While Cat 4 cabling is not commonly used today due to its limitations in terms of bandwidth and distance, fiber optic cabling can be thought of for longer distances and higher data rates, but it does not directly support PoE as it is not an electrical medium. Therefore, the best practice is to utilize at least Cat 6 cabling to ensure optimal performance and compatibility within PoE networks. This makes selecting Cat 6 or above the more prudent choice when setting up a system that utilizes Power over Ethernet.

8. How much RAM is typically suitable for an office workstation?

- A. 8 GB
- B. 16 GB**
- C. 32 GB
- D. 64 GB

A workstation in an office setting generally requires a balance between performance and cost-effectiveness, especially when handling common tasks such as word processing, spreadsheet management, and web browsing. While 8 GB of RAM is the minimum for basic tasks and may suffice for very light usage, it can lead to performance bottlenecks when multitasking or using more demanding applications. Choosing 16 GB of RAM provides a more comfortable buffer for simultaneous applications and enhances overall responsiveness. This amount of memory allows users to run productivity software, virtual machines, and other applications smoothly without significant slowdowns. Moreover, it accounts for future software updates and multitasking needs, making it a practical choice. On the other hand, 32 GB and 64 GB of RAM are generally more suited for high-performance tasks such as video editing, large-scale data analysis, or software development, which exceed typical office configurations. Therefore, while they offer additional capacity, most standard office tasks do not require such extensive RAM, making 16 GB the optimal option for a workstation in this context.

9. What is the primary purpose of the Tag Protocol Identifier (TPI)?

- A. To authenticate users
- B. To specify VLAN membership**
- C. To encrypt data
- D. To establish user permissions

The primary purpose of the Tag Protocol Identifier (TPI), commonly used in VLAN tagging protocols such as IEEE 802.1Q, is to specify VLAN membership. The TPI serves as a unique identifier that designates the VLAN to which a particular data frame belongs. By including this identifier in the frame header, network devices can properly route and segregate data traffic between different VLANs, ensuring that network traffic remains organized and secure. VLANs allow network administrators to create separate broadcast domains within a single physical network, improving performance and security by isolating traffic. The TPI makes it possible to distinguish between these segments, allowing switches to understand where to forward the traffic while maintaining the integrity of the VLAN configuration. The other choices refer to separate functionalities. User authentication, data encryption, and establishing user permissions do not relate to VLAN tagging or the role of the TPI in network traffic management. Therefore, specifying VLAN membership is the correct function of the Tag Protocol Identifier.

10. Which cable is proprietary to Apple devices and is used for charging and data transfer?

- A. USB-C Cable
- B. Lightning Cable**
- C. USB 2.0 Micro B Cable
- D. USB 2.0 Mini B Cable

The Lightning Cable is a proprietary connector developed by Apple, specifically designed for its devices such as iPhones, iPads, and iPods. This cable was first introduced in 2012 as a replacement for Apple's 30-pin dock connector. Its compact design allows for reversible use, making it easy for users to plug it in without worrying about the orientation. The Lightning Cable facilitates both charging and data transfer, enabling seamless connectivity with various Apple accessories and peripherals. Its integration with Apple's ecosystem of devices ensures compatibility and enhances user experience through features like fast charging and data synchronization. This specific functionality and design distinguish it from other common USB cables, ensuring that only Apple devices utilize this particular connection type.

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://comptiaapluscore12201201.examzify.com>

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

SAMPLE