

# BCM Information Technology Specialist (25B) Practice Exam (Sample)

## Study Guide



**Everything you need from our exam experts!**

**This is a sample study guide. To access the full version with hundreds of questions,**

**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 from reliable sources accurate, complete, and timely information about this product.**

**SAMPLE**

# Table of Contents

<b>Copyright</b> .....	<b>1</b>
<b>Table of Contents</b> .....	<b>2</b>
<b>Introduction</b> .....	<b>3</b>
<b>How to Use This Guide</b> .....	<b>4</b>
<b>Questions</b> .....	<b>6</b>
<b>Answers</b> .....	<b>9</b>
<b>Explanations</b> .....	<b>11</b>
<b>Next Steps</b> .....	<b>17</b>

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. Don't worry about getting everything right, 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, and take breaks to retain information better.**

## 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.**

## 7. Use Other Tools

**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. How do you check for open ports on a network?**
  - A. By resetting the router**
  - B. By using a port scanning tool like Nmap**
  - C. By disabling the firewall**
  - D. By checking system logs manually**
- 2. What aspect does the Physical Layer of the OSI model focus on?**
  - A. Data formatting and representation**
  - B. Logical addressing and routing**
  - C. Connectors and cabling**
  - D. Connection management**
- 3. Which wiring standard uses White/Orange as its first color code?**
  - A. T568A**
  - B. T568B**
  - C. ISO/IEC 11801**
  - D. ANSI/TIA-568**
- 4. What is the role of an IT help desk?**
  - A. To provide technical support and assistance**
  - B. To manage network infrastructure**
  - C. To create software applications**
  - D. To perform hardware repairs**
- 5. What does firewalls rule base typically control?**
  - A. The physical layout of the network infrastructure**
  - B. The types of network traffic allowed or denied**
  - C. The redundancy of data storage systems**
  - D. The user interface of the operating system**
- 6. Routing is essential for which of the following?**
  - A. Data packet reception**
  - B. Data packet delivery**
  - C. Network topology design**
  - D. Network security measures**

**7. What are common symptoms of a computer virus infection?**

- A. Faster performance and better security**
- B. Unexpected crashes and unauthorized access to files**
- C. No change in performance**
- D. Reduced disk space and shorter battery life**

**8. What is social engineering in the context of cybersecurity?**

- A. Creating software to enhance security**
- B. Manipulating individuals to divulge confidential information**
- C. Encrypting sensitive data**
- D. Installing security updates**

**9. What is the primary purpose of implementing firewalls in a network?**

- A. To manage bandwidth consumption**
- B. To encrypt sensitive data**
- C. To prevent unauthorized access to or from a private network**
- D. To enhance network speed and efficiency**

**10. What process involves extracting the original information signal from the modulated carrier wave?**

- A. Modulation**
- B. Transmission**
- C. Demodulation**
- D. Encryption**

## **Answers**

SAMPLE

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

SAMPLE

## **Explanations**

SAMPLE

## 1. How do you check for open ports on a network?

- A. By resetting the router
- B. By using a port scanning tool like Nmap**
- C. By disabling the firewall
- D. By checking system logs manually

Using a port scanning tool like Nmap is an effective way to check for open ports on a network because it employs various techniques to send packets to specified ports and analyzes the responses. With this information, it can determine which ports are open, closed, or filtered, thereby giving a clear indication of the network's security posture. Nmap is widely used by IT professionals for network discovery and security auditing, making it a reliable choice for this task. Port scanners can scan a range of IP addresses, offering insights into the devices that are actively listening for connections and those that might be vulnerable to attacks. This method is efficient and allows for automated checking across multiple devices, which manual methods would struggle to match in terms of speed and thoroughness.

## 2. What aspect does the Physical Layer of the OSI model focus on?

- A. Data formatting and representation
- B. Logical addressing and routing
- C. Connectors and cabling**
- D. Connection management

The Physical Layer of the OSI model is primarily concerned with the tangible aspects of networking, specifically the medium through which data is transmitted. This includes the physical connections such as cables, jacks, and the electrical or optical signaling used in the transmission of data. The focus of this layer is on the various types of physical media used (like Ethernet cables, fiber optics, etc.), the connectors that physically join devices, and the specifications for electrical signals, voltage levels, and data rates. It essentially deals with the hardware elements that enable data to be transferred over a network. This explains why choosing the correct answer emphasizes the importance of connectors and cabling — these are critical for establishing a physical link between devices on a network, allowing higher layers to function effectively. Other aspects of the OSI model, such as data formatting and representation, logical addressing, and connection management, pertain to higher layers which build upon the foundational work of the Physical Layer.

### 3. Which wiring standard uses White/Orange as its first color code?

- A. T568A
- B. T568B**
- C. ISO/IEC 11801
- D. ANSI/TIA-568

The wiring standard that uses White/Orange as its first color code is T568B. This standard is primarily used in structured cabling and is widely implemented in Ethernet networks. In the T568B wiring scheme, White/Orange is designated as the first pair, corresponding to the transmit data and is critical in ensuring proper communication between network devices. T568B is often preferred in commercial installations and has become the most widely used standard in the United States. The first color code assignment is essential for maintaining proper pin alignment and consistent performance across the network. Understanding these wiring standards is crucial for any Information Technology Specialist, as improper wiring can lead to connectivity issues and network failures.

### 4. What is the role of an IT help desk?

- A. To provide technical support and assistance**
- B. To manage network infrastructure
- C. To create software applications
- D. To perform hardware repairs

The role of an IT help desk is primarily to provide technical support and assistance to users experiencing issues with their technology. This can include troubleshooting problems, answering questions about software and hardware, and guiding users in resolving technical issues they may encounter. A help desk is often the first point of contact for users facing difficulties, and its purpose is to ensure that users can effectively utilize technology resources, thus minimizing downtime and improving productivity. While managing network infrastructure, creating software applications, and performing hardware repairs are essential IT functions, these responsibilities typically fall outside the scope of a help desk. The help desk is focused on direct user support rather than the backend management or development tasks associated with those roles. Therefore, providing technical support and assistance is the primary function that defines an IT help desk.

## 5. What does firewalls rule base typically control?

- A. The physical layout of the network infrastructure
- B. The types of network traffic allowed or denied**
- C. The redundancy of data storage systems
- D. The user interface of the operating system

The correct answer focuses on the primary function of a firewall, which is to regulate network traffic based on a set of predetermined rules. The rule base of a firewall is a critical aspect of its operation, as it determines which types of data packets can enter or exit the network. By specifying criteria such as source IP addresses, destination IP addresses, port numbers, and protocols, the rule base enables the firewall to either allow or deny traffic. This control helps protect the network by blocking unauthorized access and ensuring that only legitimate traffic is permitted, thus maintaining network security and integrity. The other options relate to different aspects of network management and security but do not accurately describe the role of a firewall's rule base. For instance, the physical layout of the network infrastructure pertains to how devices are connected, while redundancy of data storage systems focuses on data backup and recovery strategies. Additionally, the user interface of the operating system involves the interaction design and user experience, which is unrelated to the traffic management functions handled by firewalls.

## 6. Routing is essential for which of the following?

- A. Data packet reception
- B. Data packet delivery**
- C. Network topology design
- D. Network security measures

Routing is essential primarily for data packet delivery, as it involves determining the optimal path for data packets to travel across a network from the source to the destination. This process ensures that data is directed through various nodes, routers, and switches effectively, reaching the intended endpoint. When a data packet is created at the source device, it does not inherently know the best path to its destination. Routers use routing tables and algorithms to decide how to forward the packet, taking into consideration factors such as network congestion, packet size, and the destination address. This delivery process is vital for enabling communication across complex networks, such as the internet, where numerous paths and potential routes exist. While data packet reception is important, it occurs after routing has already taken place. Network topology design and security measures are also important aspects of network management, but they do not directly relate to the functional process of routing packets for effective data delivery. Therefore, the focus of routing lies specifically on ensuring that packets arrive at their correct destinations efficiently.

## 7. What are common symptoms of a computer virus infection?

- A. Faster performance and better security**
- B. Unexpected crashes and unauthorized access to files**
- C. No change in performance**
- D. Reduced disk space and shorter battery life**

The presence of unexpected crashes and unauthorized access to files is a typical indication of a computer virus infection. A virus is designed to disrupt the normal operation of a computer's software and can lead to instability, causing applications or the operating system itself to crash unexpectedly. Additionally, many viruses are capable of compromising system security, allowing unauthorized users to gain access to files and sensitive information. This behavior highlights how viruses can undermine the integrity and functionality of a system. The other options do not align with the behaviors normally associated with a virus. For instance, faster performance and better security are contradictory to the impact of a virus, as such infections generally degrade performance and can compromise security. Similarly, no visible change in performance would suggest that the system is functioning normally, which is generally not the case when a virus is present. Lastly, while reduced disk space may result from certain types of malware that create unnecessary files, it does not specifically indicate unauthorized access or the kind of comprehensive issues typically linked with virus infections. Therefore, the symptoms of unexpected crashes and unauthorized file access make option B the accurate choice.

## 8. What is social engineering in the context of cybersecurity?

- A. Creating software to enhance security**
- B. Manipulating individuals to divulge confidential information**
- C. Encrypting sensitive data**
- D. Installing security updates**

In the context of cybersecurity, social engineering refers to the psychological manipulation of individuals to obtain confidential or sensitive information. This technique exploits human behavior rather than relying on technical hacking methods. The goal is often to trick individuals into providing personal information, such as passwords or financial details, or to gain unauthorized access to systems and networks. Understanding this concept is vital for cybersecurity awareness, as many breaches result from social engineering tactics rather than direct attacks on systems. Training individuals to recognize and respond to these manipulations is a key component of a robust cybersecurity strategy. The other options, while related to cybersecurity, do not capture the essence of social engineering, which fundamentally relies on the interaction between people rather than on technical safeguards or measures.

## 9. What is the primary purpose of implementing firewalls in a network?

- A. To manage bandwidth consumption**
- B. To encrypt sensitive data**
- C. To prevent unauthorized access to or from a private network**
- D. To enhance network speed and efficiency**

The primary purpose of implementing firewalls in a network is to prevent unauthorized access to or from a private network. Firewalls act as a security barrier between an internal network and external sources, monitoring and controlling incoming and outgoing traffic based on predetermined security rules. This helps maintain the integrity of the network by blocking unauthorized users and potentially malicious traffic from accessing sensitive information or resources. While bandwidth management, data encryption, and enhancing network speed are important aspects of network management, they do not define the core function of a firewall. Bandwidth management focuses on optimizing the network's data capacity, encryption deals with securing data during transmission, and increasing network speed pertains to performance enhancements. In contrast, the firewall's main duty is to enforce security policies to safeguard the network against unauthorized intrusions and attacks, highlighting its critical role in overall network security.

## 10. What process involves extracting the original information signal from the modulated carrier wave?

- A. Modulation**
- B. Transmission**
- C. Demodulation**
- D. Encryption**

The process that involves extracting the original information signal from the modulated carrier wave is demodulation. This is a critical step in communication systems where information is transmitted over distances. When information, such as voice or data, is sent over a carrier wave, it is modulated to ensure that it can travel efficiently and properly through various mediums. Demodulation, therefore, is the reverse of modulation. It takes the modulated carrier and separates the information signal from it at the receiving end. This allows the original message to be reconstructed and understood. It is essential in scenarios such as radio transmission, where audio signals are carried over electromagnetic waves, or in digital communications, where binary data is transmitted over the Internet. Understanding demodulation is vital for anyone in the field of information technology and telecommunications, as it plays a crucial role in ensuring that communication systems function correctly and that data can be accurately retrieved and interpreted.

# 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](mailto:hello@examzify.com).**

**Or visit your dedicated course page for more study tools and resources:**

**<https://bcm25b.examzify.com>**

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

**SAMPLE**