Cisco Certified Support Technician (CCST) Networking Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. For the full version with hundreds of questions, visit:
https://ccstnetworking.examzify.com

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

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. What does the acronym SNMP stand for?

A. Simple Network Management Protocol

B. Standard Network Management Protocol

C. Simple Network Maintenance Procedure

D. Standard Network Monitoring Protocol

2. What does latency measure in a network?

A. Total time for a packet to travel between two points

B. Time taken for data to be processed

C. Maximum data throughput in a network

D. Time taken to establish a network connection

3. What aspect does a firewall at the internet boundary primarily focus on?

A. Incoming and outgoing traffic

B. Only incoming traffic

C. Only outgoing traffic

D. Network performance optimization

4. What does the term "bandwidth" refer to in a network context?

A. The range of frequencies in a transmission

B. The maximum rate of data transfer across a network

C. The number of connected devices on a network

D. The physical devices used to transmit data

5. Which routing protocol uses a distance vector mechanism?

A. OSPF

B. RIP

C. EIGRP

D. BGP

6. **Which version of Wi-Fi Protected Access became a requirement for certification in 2006?**

   A. WPA

   B. WPA2

   C. WPA3

   D. WEP

7. **What does the green LED status indicate for a duplex connection?**

   A. Half-duplex

   B. Full-duplex

   C. Link down

   D. No connection

8. **What is the theoretical maximum bandwidth of the 802.11b Wi-Fi standard?**

   A. 1 - 2 mbps

   B. 1 - 11 mbps

   C. 6 - 54 mbps

   D. 72 - 600 mbps

9. **What type of cable is typically used to connect to the console port of a Cisco device?**

   A. Ethernet cable

   B. USB cable

   C. Serial cable

   D. Cisco console cable

10. **Which protocol is associated with ports 20 and 21?**

    A. SFTP

    B. FTP

    C. TFTP

    D. HTTP

Answers

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

Explanations

1. What does the acronym SNMP stand for?

A. Simple Network Management Protocol

B. Standard Network Management Protocol

C. Simple Network Maintenance Procedure

D. Standard Network Monitoring Protocol

The correct answer is "Simple Network Management Protocol." SNMP is a protocol used for network management, allowing administrators to monitor network devices, gather information, and manage network performance. The term "simple" reflects the protocol's focus on ease of use and implementation for managing devices on an IP network. SNMP operates by using a client-server model where network devices (referred to as agents) send information to a management system (often referred to as a manager). This management system can poll the agents for information, such as performance metrics or error statuses, and it can also send commands to network devices to modify their configurations or respond to certain conditions. Understanding SNMP is crucial for network professionals, as it plays an integral role in maintaining the health and efficiency of networks. The other options do not accurately represent the purpose and functionality of SNMP, which is why they are incorrect.

2. What does latency measure in a network?

A. Total time for a packet to travel between two points

B. Time taken for data to be processed

C. Maximum data throughput in a network

D. Time taken to establish a network connection

Latency measures the total time it takes for a packet to travel from one point in a network to another. This time includes the delays incurred during the transmission across different network segments, which can be influenced by various factors such as propagation delay, transmission delay, queuing delay, and processing delay within network devices. Understanding latency is crucial for assessing network performance because high latency can lead to delays in data transmission, which may affect applications sensitive to timing, such as video conferencing or online gaming. This characteristic distinguishes latency from other network performance metrics, such as bandwidth or throughput, which measure data transfer rates rather than the time taken for individual packets to arrive at their destination. The other choices refer to different aspects of network performance: processing time pertains to how long it takes devices to handle data, maximum data throughput indicates the highest rate of data transfer possible in the network, and connection establishment time focuses on the duration required to set up a connection between devices. Each of these is important in its own context but does not specifically define latency.

3. What aspect does a firewall at the internet boundary primarily focus on?

A. Incoming and outgoing traffic

B. Only incoming traffic

C. Only outgoing traffic

D. Network performance optimization

A firewall at the internet boundary primarily focuses on monitoring and controlling both incoming and outgoing traffic. This is crucial for establishing a secure network environment, as firewalls act as a barrier between a trusted internal network and untrusted external networks such as the internet. By inspecting incoming traffic, the firewall can prevent unauthorized access and protect against various threats, such as malware or hacking attempts. On the other hand, managing outgoing traffic is equally important because it can help prevent internal users from accessing malicious sites or sending sensitive information outside the organization. This dual capability ensures that the firewall provides comprehensive security by allowing or denying traffic based on predefined security rules. As a result, firewalls are essential for maintaining the integrity and confidentiality of the network while enabling legitimate communication. In contrast, focusing solely on either incoming or outgoing traffic would leave the network susceptible to threats from either direction. Additionally, network performance optimization is a separate function that may involve other networking equipment and strategies, rather than being the primary focus of a firewall.

4. What does the term "bandwidth" refer to in a network context?

A. The range of frequencies in a transmission

B. The maximum rate of data transfer across a network

C. The number of connected devices on a network

D. The physical devices used to transmit data

In a network context, "bandwidth" primarily refers to the maximum rate of data transfer across a network. This metric indicates the capacity of the network to transmit data, often measured in bits per second (bps). The greater the bandwidth, the more data can be transmitted simultaneously over the connection, which directly impacts the performance and speed at which information can be sent and received. For example, in a home network, if the bandwidth is high, multiple devices can stream videos, download files, and conduct video calls at the same time without experiencing significant slowdowns. This makes bandwidth a crucial factor when considering network performance, especially in environments where multiple users or applications require high data transfer rates. While other aspects of networking, such as frequency range or the number of connected devices, can influence performance, they do not define bandwidth itself. Therefore, understanding bandwidth as the maximum data transfer rate helps individuals and professionals optimize network configurations to meet their specific needs.

5. Which routing protocol uses a distance vector mechanism?

A. OSPF

B. RIP

C. EIGRP

D. BGP

RIP, or Routing Information Protocol, is considered a distance vector routing protocol. This means that it determines the best path for data packets based on the distance to the destination, quantified as the number of hops. Each router maintains a table of distances to other routers, and they periodically share these tables with their neighbors to inform them of any changes in the network topology. In distance vector protocols like RIP, routers use a simple metric system to evaluate the paths, where each hop to a router counts as one unit. This method makes RIP relatively easy to configure and implement, although it can be less efficient and slower to converge compared to link-state protocols, such as OSPF, which utilize a different mechanism for routing decisions. Understanding this fundamental characteristic of RIP is essential for grasping the distinctions between various routing protocols and their respective methodologies, especially for someone studying for the Cisco Certified Support Technician certification. It highlights how routing decisions can be made based on simple metrics and the collaborative nature of distance vector protocols in exchanging routing information.

6. Which version of Wi-Fi Protected Access became a requirement for certification in 2006?

A. WPA

B. WPA2

C. WPA3

D. WEP

The requirement for Wi-Fi Protected Access to be certified in 2006 was indeed WPA2. This version brought significant improvements over its predecessor, WPA, by introducing stronger security protocols and encryption methods. WPA2 utilizes the Advanced Encryption Standard (AES) for encryption, which provides a much higher level of security compared to the Temporal Key Integrity Protocol (TKIP) used in the original WPA. WPA2 also mandates the use of robust security mechanisms, which were necessary to protect wireless communications against various attacks that were common by that time. As a result, it became critical for devices and networks to adopt WPA2 to ensure a secure wireless environment. WEP, which predates both WPA and WPA2, was deemed insecure and is no longer considered a viable security protocol, while WPA3, which is a more recent standard, did not become available until later. Therefore, understanding the evolution of these protocols highlights why WPA2's adoption became a standard requirement for certification in 2006.

7. What does the green LED status indicate for a duplex connection?

A. Half-duplex

B. Full-duplex

C. Link down

D. No connection

The green LED status indicating full-duplex operation signifies that a device is capable of transmitting and receiving data simultaneously. In networking, full-duplex is an advanced mode of data transmission where both parties can send and receive information at the same time, which effectively doubles the capacity of communication as compared to half-duplex modes. A full-duplex configuration is beneficial for network efficiency because it reduces collision domains and allows for smoother communication between devices. The presence of a green LED typically signals that the connection is not only active but also optimized for full-duplex communication, confirming that both devices connected can effectively handle simultaneous data flows without interference. In contrast, indicators for half-duplex or link down states do not meet this standard for simultaneous bidirectional communication, and setups that show no connection would lack the necessary signaling altogether. Thus, the green LED specifically highlighting a full-duplex status is a clear indication of an operational and efficient communication pathway between devices.

8. What is the theoretical maximum bandwidth of the 802.11b Wi-Fi standard?

A. 1 - 2 mbps

B. 1 - 11 mbps

C. 6 - 54 mbps

D. 72 - 600 mbps

The theoretical maximum bandwidth of the 802.11b Wi-Fi standard is indeed 11 Mbps. This standard was introduced as part of the IEEE 802.11 specification and is one of the earlier standards for wireless networking. It operates in the 2.4 GHz frequency band and utilizes a modulation technique called Direct Sequence Spread Spectrum (DSSS). The 802.11b standard supports data rates of 1, 2, 5.5, and 11 Mbps, where the highest rate of 11 Mbps is where the maximum bandwidth aligns. This makes it suitable for basic wireless tasks such as web browsing and email during its peak usage, although modern applications often exceed what 802.11b can reliably support. Other standards mentioned in the choices relate to more advanced Wi-Fi technologies that offer significantly higher bandwidths, which are not applicable to the 802.11b specification. This historical context emphasizes the evolution of wireless networking capabilities as technology progressed beyond what 802.11b can provide.

9. What type of cable is typically used to connect to the console port of a Cisco device?

A. Ethernet cable

B. USB cable

C. Serial cable

D. Cisco console cable

The most common type of cable used to connect to the console port of a Cisco device is referred to as a Cisco console cable. This cable is typically a rolled cable with a RJ-45 connector on one end that connects to the console port of the Cisco device and a serial connector (such as DB-9) on the other end that connects to the computer or terminal emulator for configuration purposes.   The design of the Cisco console cable allows for serial communication, which is required to access the command-line interface of the networking equipment. It facilitates direct management and monitoring of the device, especially in situations where remote access is not available. Other cable options, while they may serve specific functions in networking scenarios, do not serve the same purpose as the Cisco console cable. Ethernet cables are primarily meant for network connections and data transmission between devices, while USB cables are generally used for direct device connections, and standard serial cables would not have the necessary pinouts to connect to the console port of most Cisco devices effectively. Thus, the distinguishing features of the Cisco console cable make it the correct choice for this application.

10. Which protocol is associated with ports 20 and 21?

A. SFTP

B. FTP

C. TFTP

D. HTTP

The correct association of ports 20 and 21 with a specific protocol is FTP, which stands for File Transfer Protocol. FTP is a standard network protocol used to transfer files between a client and a server over a Transmission Control Protocol (TCP) connection. Port 21 is typically used for the control connection, which is responsible for sending commands and responses between the FTP client and server. Port 20 is designated for the data connection, which is utilized when files are being transferred. This division allows for separate management of commands and the actual file transfer process, enhancing the efficiency of the protocol. Understanding this port assignment is crucial for network configuration and troubleshooting, as it assists in determining which services are operating on which ports, ensuring the proper functioning of file transfer operations within networking environments.

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://ccstnetworking.examzify.com

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