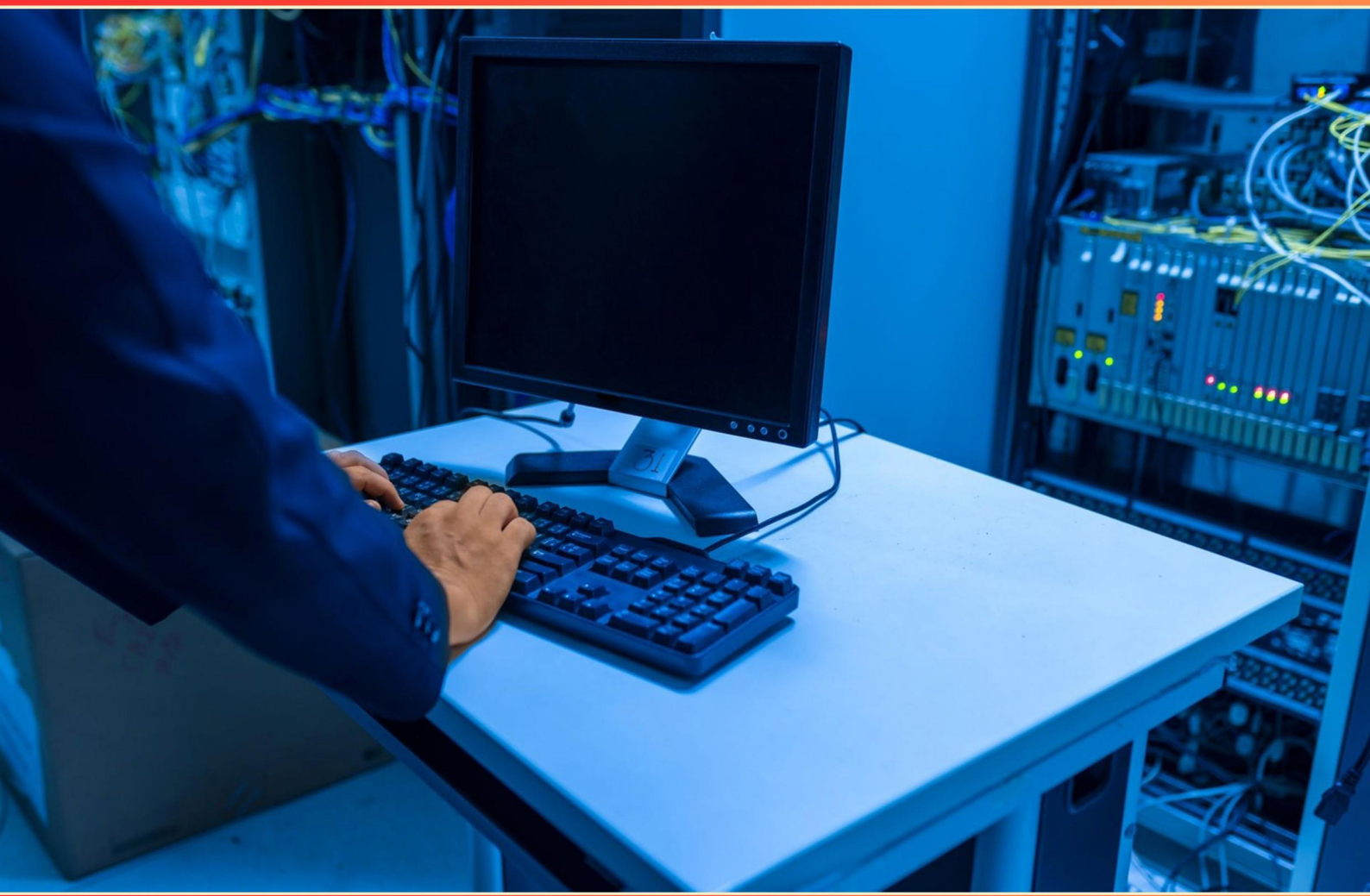
COMPTIA NETWORK+ PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://comptia-networkplus.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.

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. What could cause a port to become suspended in an EtherChannel?

A. Configuration mismatch

B. Faulty hardware

C. High traffic volume

D. Unplugged cables

2. What does ransomware typically do to a user's data?

A. Deletes the data permanently

B. Encrypts the data and demands a ransom for decryption

C. Copies the data to another location

D. Corrupts the data irreversibly

3. How does WPA2/3-Enterprise authentication function?

A. It relies on a single password for all users

B. It authenticates users individually through a server

C. It uses a static IP address for identification

D. It prevents access points from communicating

4. Which of the following is a method used by attackers to hop VLANs?

A. IP spoofing

B. Switch spoofing

C. Packet sniffing

D. Port scanning

5. What does the netstat command with the option '-b' accomplish on a Windows system?

A. Shows only established connections

B. Displays the binaries associated with active connections

C. Lists active TCP connections without resolving names

D. Provides network statistics summary

6. What is a limitation of DHCP in an enterprise environment?

A. High bandwidth requirements

B. Limited communication range

C. Requires multiple devices

D. Only works in local networks

SAMPLE

7. What is a major benefit of using dynamic routing protocols?

A. Manual route calculation

B. Automatic population of new routes

C. Management of static routes

D. Enhancement of network security

8. The term "baseband" in networking signifies what characteristic?

A. The use of multiple frequencies

B. The use of a single frequency across the medium

C. Support for both analog and digital signals

D. Enhanced security features

9. What is required for Syslog to manage logging effectively over time?

A. High network bandwidth

B. A significant amount of disk space

C. Low latency connections

D. Encryption of logs

10. What is an SVI in the context of VLANs?

A. Scalable Virtual Interface

B. Switched Virtual Interface

C. Shared Virtual Interface

D. Secure Virtual Interface

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What could cause a port to become suspended in an EtherChannel?

A. Configuration mismatch

B. Faulty hardware

C. High traffic volume

D. Unplugged cables

A port can become suspended in an EtherChannel due to a configuration mismatch. EtherChannel is a technology used to combine multiple physical links between network devices into a single logical link to increase bandwidth and provide redundancy. For EtherChannel to work, all the individual ports that are being aggregated must have identical settings, including MTU size, speed, duplex mode, and other configurations. If there is any discrepancy in these settings between the ports, the switch will detect the mismatch and may suspend the problematic port to prevent issues, such as traffic misrouting or operational anomalies, in the aggregated link. In the context of the other options, while faulty hardware could lead to connectivity issues, it typically would not specifically cause a port to enter a suspended state in the way that a configuration mismatch does. High traffic volume may lead to performance issues or congestion but wouldn't directly cause a port to suspend. Likewise, unplugged cables would result in a link failure or loss of connectivity rather than a suspended state due to a configuration issue. Hence, a configuration mismatch is the key factor that directly leads to a port being suspended in an EtherChannel scenario.

2. What does ransomware typically do to a user's data?

A. Deletes the data permanently

B. Encrypts the data and demands a ransom for decryption

C. Copies the data to another location

D. Corrupts the data irreversibly

Ransomware is a type of malicious software that primarily focuses on obtaining ransom from users by encrypting their data. When ransomware infects a system, it typically encrypts files and makes them inaccessible to the user. In order to regain access to their data, the user is then presented with a demand for payment, usually in cryptocurrencies, to receive a decryption key. This method of operation creates significant stress for the victim, as they face a dilemma of potentially losing valuable data or paying the ransom without any guarantee of recovery. The other options describe actions that are either not typically associated with ransomware or do not align with its primary function. For instance, permanently deleting data or corrupting it irreversibly are not direct strategies used by ransomware, as the main goal is to leverage the encrypted data for financial gain rather than outright destruction. Similarly, while copying data does occur in some other types of malware, it is not a characteristic feature of ransomware, which focuses on encryption and extorting the user for access.

SAMPLE

3. How does WPA2/3-Enterprise authentication function?

A. It relies on a single password for all users

B. It authenticates users individually through a server

C. It uses a static IP address for identification

D. It prevents access points from communicating

WPA2/3-Enterprise authentication functions by authenticating users individually through a centralized authentication server, typically employing the IEEE 802.1X protocol. This model enhances network security by requiring each user to provide their unique credentials, which are verified against a database managed by the authentication server (like a RADIUS server). This individualized authentication process allows network administrators to have greater control over who accesses the network. They can easily manage user access, revoke credentials, and implement various security policies. As opposed to a shared password, which could be disseminated and become less secure over time, the enterprise model utilizes unique credentials for each user session. This ensures that only authorized users can access the network, enhancing both security and accountability. In contrast, relying on a single password for all users would lead to significant security risks. Using a static IP address for identification does not directly relate to the authentication method itself, as IP addresses can be easily spoofed or manipulated. Preventing access points from communicating would also conflict with the operational requirements of a wireless network. Thus, the approach of authenticating users individually is a fundamental aspect of WPA2/3-Enterprise, promoting a secure and manageable network environment.

4. Which of the following is a method used by attackers to hop VLANs?

A. IP spoofing

B. Switch spoofing

C. Packet sniffing

D. Port scanning

Switch spoofing is a technique that attackers use to gain unauthorized access to multiple VLANs (Virtual Local Area Networks) by exploiting the way switches handle VLAN tagging. In this method, the attacker connects a device to a network switch and tricks the switch into thinking that the device is another switch. This can be accomplished by configuring the attacker's device to send out VLAN trunking protocol (VTP) or Dynamic Trunking Protocol (DTP) messages, which are used by switches to establish trunk links. A trunk link allows traffic from multiple VLANs to pass through the same physical connection, which means if an attacker successfully creates a trunk link with the switch, they can access all the VLANs that the trunk carries, effectively hopping from one VLAN to another. This poses a significant security risk because it can allow attackers to access sensitive data and resources on VLANs that they should not have access to. Other techniques, while they can be related to network security issues, do not specifically enable VLAN hopping. IP spoofing involves altering the source address in IP packets to masquerade as another device, but it does not inherently allow access to other VLANs. Packet sniffing is the act of capturing network packets to analyze traffic, and port scanning is a

SAMPLE

5. What does the netstat command with the option '-b' accomplish on a Windows system?

A. Shows only established connections

B. Displays the binaries associated with active connections

C. Lists active TCP connections without resolving names

D. Provides network statistics summary

The netstat command with the '-b' option on a Windows system specifically displays the binaries associated with active connections. This feature allows users to see which executable files are involved in the current network activities. When this command is run, it will provide a list of the active TCP connections alongside the associated process names and the executable paths. This is particularly useful for troubleshooting purposes, as it lets administrators identify which applications are making connections over the network, potentially helping to pinpoint rogue or resource-intensive processes that may be affecting network performance. The other options do not accurately describe the functionality of the '-b' option. For instance, showing only established connections focuses solely on connection status, which is not the primary intent of the '-b' switch. Similarly, listing active TCP connections without resolving names would use a different switch that omits the binary information. Lastly, providing a network statistics summary pertains to broader network metrics rather than the specific functional focus of the '-b' option, which centers on the binaries related to active connections.

6. What is a limitation of DHCP in an enterprise environment?

A. High bandwidth requirements

B. Limited communication range

C. Requires multiple devices

D. Only works in local networks

The correct choice highlights a significant limitation of DHCP (Dynamic Host Configuration Protocol) in enterprise environments. DHCP operates by allowing a server to assign IP addresses dynamically to devices on a network, facilitating the management of IP address allocation. However, its communication range can be limited by the broadcast nature of its messages. In a typical scenario, DHCP uses broadcast messages to communicate with clients, which means that devices can only receive these messages within the same local area network (LAN). When it comes to larger enterprise networks that span multiple subnets or VLANs, this can pose a challenge. Routers, which connect different networks, typically do not forward broadcast messages. As a result, in order for devices in different subnets to acquire IP addresses, additional configurations or DHCP relay agents (using the IP Helper address feature, for example) are required to enable DHCP traffic forwarding across routers. This limitation makes the efficient use and administration of IP addresses more complex in larger, segmented networks, where devices need to communicate across different segments. Consequently, enterprises often need to implement additional strategies or infrastructures, such as DHCP relay agents or multiple DHCP servers, to ensure smooth operation across their networks. The other options pertain to concerns that are not intrinsic limitations of DHCP itself, making

SAMPLE

7. What is a major benefit of using dynamic routing protocols?

A. Manual route calculation

B. Automatic population of new routes

C. Management of static routes

D. Enhancement of network security

The major benefit of using dynamic routing protocols is that they provide the automatic population of new routes. This capability allows routers within a network to exchange information about reachable networks, making real-time adjustments to routing tables without requiring manual intervention. As network topologies change, such as when new devices are added or when links go down, dynamic routing protocols can quickly adapt and find the best paths for data packets. This enhances network reliability and efficiency, particularly in larger networks where manual route management would be too cumbersome or impractical. The other choices reflect aspects of routing but do not capture the primary advantage of dynamic routing protocols. Manual route calculation would imply a lack of automation, which contradicts the purpose of dynamic protocols. Management of static routes does not leverage the automation capabilities inherent in dynamic protocols. Finally, while dynamic routing can improve aspects of network security indirectly by ensuring that routes are current and optimal, enhancing network security is not its primary function.

8. The term "baseband" in networking signifies what characteristic?

A. The use of multiple frequencies

B. The use of a single frequency across the medium

C. Support for both analog and digital signals

D. Enhanced security features

The term "baseband" refers specifically to the use of a single frequency across the medium for transmitting signals. In baseband systems, the entire bandwidth of the medium is utilized to send a single signal, typically a digital signal, which allows for efficient communication but limits overall capacity to one channel at a time. This means that when multiple devices are transmitting data, they must take turns using the medium, which is often achieved through various multiplexing techniques. This concept is distinct from "broadband," where multiple signals can be sent simultaneously over different frequencies within the same medium. Therefore, the emphasis on a single frequency in baseband is central to its definition and usage in networking contexts, particularly in local area networks (LANs) where Ethernet is a common example.

9. What is required for Syslog to manage logging effectively over time?

A. High network bandwidth

B. A significant amount of disk space

C. Low latency connections

D. Encryption of logs

For Syslog to manage logging effectively over time, a significant amount of disk space is essential. Syslog is designed to collect and store log messages from various network devices and applications, which can generate a substantial volume of data, especially in large or complex environments. As time passes and more events are logged, adequate disk space becomes crucial to ensure that all logs are retained without loss. Moreover, maintaining historical logs is often necessary for troubleshooting, compliance, and security audits. A lack of sufficient disk space can lead to overwriting of older logs or the failure to record new logs, compromising the integrity of the logging system. While high network bandwidth, low latency connections, and encryption might be important for certain aspects of network management and security, they do not directly address the fundamental requirement of having enough storage capacity to retain logs over time.

SAMPLE

10. What is an SVI in the context of VLANs?

A. Scalable Virtual Interface

B. Switched Virtual Interface

C. Shared Virtual Interface

D. Secure Virtual Interface

An SVI, or Switched Virtual Interface, is a virtual interface on a switch used to facilitate communication between different VLANs. SVIs enable Layer 3 communication for VLANs, which means they can provide an IP address and support routing to allow devices within different VLANs to communicate with each other. When a switch operates with multiple VLANs, each VLAN can have a corresponding SVI that serves as the gateway for devices within that VLAN. By using SVIs, network devices connected to different VLANs can route traffic through the switch, allowing for efficient communication without needing a dedicated router for each VLAN. This capability is crucial in modern networking environments, where virtualized networks are common, and efficient traffic management is necessary. The alternative choices do not accurately describe the function or purpose of SVIs. For example, Scalable Virtual Interface and Secure Virtual Interface do not reflect the actual function provided by SVIs in VLANs, while Shared Virtual Interface does not exist in this context. The correct term that captures the essential function of an SVI in VLAN communication is Switched Virtual Interface.

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://comptia-networkplus.examzify.com

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

SAMPLE