Cisco Learning Network 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. What command applies a distribute list specifically to OSPF?

A. network distribute-list 1 in

B. distribute-list 1 out

C. distribute-list prefix-list

D. apply distribute-list 1

2. What are three important changes implemented in IGMP v2 compared to IGMP v1?

A. Group-specific queries

B. Querier election mechanism

C. Leave-group message

D. All of the above

3. What distinguishes a firewall as a Next-Generation Firewall (NGFW)?

A. Increased throughput and simplicity

B. Additional features such as Context Awareness and Advanced Malware Protection

C. Higher cost and lower deployment complexity

D. Basic traffic filtering and monitoring

4. What TCP port does BGP use for establishing a session?

A. Port 80

B. Port 443

C. Port 179

D. Port 8080

5. Which command sequence sets up a GRE tunnel interface on a Cisco IOS router?

A. conf t, interface tunnel1, ip address 172.16.99.1 255.255.255.0

B. conf t, interface tunnel0, ip address 172.16.99.2 255.255.255.0

C. conf t, interface tunnel0, set ip address 172.16.99.2 255.255.255.0

D. conf t, interface tunnel1, ip address 172.16.99.0 255.255.255.0

6. Which command is used to control the severity level for syslog messages?

A. logging trap all

B. logging trap severity

C. logging console severity

D. logging buffered severity

7. What is a primary function of GRE in network communication?

A. It provides encryption for secure transmission.

B. It allows routing information to pass between connected networks.

C. It compresses data for faster transmission.

D. It ensures data integrity during transfer.

8. Which SD-WAN component provides programmatic interfaces for DevOps operations?

A. vSmart

B. vEdge

C. vManage

D. vBond

9. Which severity level is used to indicate that a system is unusable?

A. Warning

B. Critical

C. Emergency

D. Info

10. What are two historical perspectives of AMP for endpoints?

A. File Trajectory and Device Trajectory

B. Network Trajectory and Behavior Analysis

C. Malware Detection and Prevention Strategies

D. Cloud Security and On-Premise Solutions

Answers

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

Explanations

1. What command applies a distribute list specifically to OSPF?

A. network distribute-list 1 in

B. distribute-list 1 out

C. distribute-list prefix-list

D. apply distribute-list 1

The command that specifically applies a distribute list to OSPF is "distribute-list 1 out." This command is used to control the distribution of routing information in OSPF by filtering the routes that the OSPF process advertises to its neighboring routers. When you apply a distribute list in this context, the number "1" refers to an access list number or a prefix list identifier that has been defined elsewhere in the configuration. By using "out," the command specifies that the filtering should apply to the routes being sent out of the router to its OSPF neighbors. This functionality is crucial for managing which routes are advertised, helping to ensure that only relevant or desired routes are shared with neighboring routers, thus controlling the routing table size and preserving bandwidth. In contrast, the other options do not appropriately fit the context of OSPF. For instance, using "network distribute-list 1 in" is not a valid command syntax for OSPF; OSPF does not use the "network" keyword in this manner. The third option, "distribute-list prefix-list," lacks the necessary context such as "in" or "out" to define the direction, making it incomplete for the specific application in OSPF. Lastly

2. What are three important changes implemented in IGMP v2 compared to IGMP v1?

A. Group-specific queries

B. Querier election mechanism

C. Leave-group message

D. All of the above

IGMP version 2 introduced several important enhancements over IGMP version 1, which are crucial for more efficient multicast group management. Group-specific queries are one of the key changes in IGMP v2. While IGMP v1 only allowed a general query to be sent to all multicast group members, IGMP v2 enables the multicast router to send queries specifically directed to a particular multicast group. This improves the accuracy of membership management since the router can pinpoint which groups have active members, resulting in more efficient bandwidth use. The querier election mechanism is another significant enhancement in IGMP v2. This feature allows multicast routers on the same LAN segment to elect one router as the querier, responsible for soliciting membership information from hosts. This reduces unnecessary query traffic because only the designated querier will send group membership queries, helping to streamline communication and decrease the load on the network. The leave-group message feature adds functionality that was not present in IGMP v1. With this message, a host can inform the multicast router immediately when it wants to leave a group, facilitating prompt updates to multicast group membership. This allows the multicast router to quickly manage and optimize traffic for active group members, enhancing overall network efficiency. The combination of these three improvements—group

3. What distinguishes a firewall as a Next-Generation Firewall (NGFW)?

A. Increased throughput and simplicity

B. Additional features such as Context Awareness and Advanced Malware Protection

C. Higher cost and lower deployment complexity

D. Basic traffic filtering and monitoring

A Next-Generation Firewall (NGFW) is distinguished by its integration of advanced capabilities that go beyond traditional firewall features. These additional features include Context Awareness, which allows the firewall to understand and apply security policies based not only on IP addresses and ports but also on the user identity, application type, and the specific content being transmitted. This context-sensitive approach enables more precise and effective filtering. Moreover, Advanced Malware Protection (AMP) is another critical aspect of an NGFW. It allows for the identification and mitigation of sophisticated threats that may bypass conventional security measures. NGFWs are equipped to analyze traffic more deeply by inspecting payloads and using techniques like intrusion prevention, threat intelligence, and application awareness to protect networks from modern, multi-faceted attacks. In contrast, the other options focus on attributes that don't encapsulate the full capabilities or purposes of an NGFW. Increased throughput and simplicity while important for performance, do not represent the defining characteristics of next-generation firewalls. Higher cost and lower deployment complexity do not accurately reflect the value and strategic importance of NGFWs either, as they are designed to offer robust security features that justify their investment. Lastly, basic traffic filtering and monitoring represent traditional firewalls, lacking the advanced analytical features that characterize NGFW

4. What TCP port does BGP use for establishing a session?

A. Port 80

B. Port 443

C. Port 179

D. Port 8080

Border Gateway Protocol (BGP) uses TCP port 179 to establish sessions between BGP peers. This is a well-defined standard within the protocol specifications, and all BGP implementations are designed to use this specific port for communication. The choice of port 179 is crucial because it allows for reliable transmission of routing information between different autonomous systems on the internet. Using TCP ensures that BGP can handle issues such as packet loss and retransmission, which are imperative for maintaining consistent routing information. By establishing connections on this designated port, routers can efficiently manage and exchange routing updates, which is essential for the dynamic routing process across diverse networks. This port assignment is part of the Internet Assigned Numbers Authority (IANA) Service Name and Transport Protocol Port Number Registry, reflecting the standardization and widespread adoption of BGP in internet routing practices.

5. Which command sequence sets up a GRE tunnel interface on a Cisco IOS router?

A. conf t, interface tunnel1, ip address 172.16.99.1 255.255.255.0

B. conf t, interface tunnel0, ip address 172.16.99.2 255.255.255.0

C. conf t, interface tunnel0, set ip address 172.16.99.2 255.255.255.0

D. conf t, interface tunnel1, ip address 172.16.99.0 255.255.255.0

The command sequence for setting up a GRE tunnel interface on a Cisco IOS router involves entering global configuration mode and then specifying the interface type as a tunnel, followed by assigning an IP address to that tunnel interface. In this case, the correct answer specifies the use of "interface tunnel0," which is a valid option for establishing a GRE tunnel, and it assigns an appropriate IP address of "172.16.99.2" with a corresponding subnet mask of "255.255.255.0." Using "tunnel0" is common because GRE tunnels are often referred to with the first logical tunnel interface starting at 0. The IP address chosen should be part of the same subnet that will be used on the other end of the GRE tunnel to ensure proper communication and routing through the tunnel. Other options may contain correct elements but fail to meet the criteria for properly defining the tunnel or using the appropriate addresses. For instance, specifying "tunnel1" could be valid, but the combination of address and subnet mask in other options may either not conform to the expected IP addressing practices associated with tunneling or could be referencing an IP address range not suitable for this implementation.

6. Which command is used to control the severity level for syslog messages?

A. logging trap all

B. logging trap severity

C. logging console severity

D. logging buffered severity

The command that controls the severity level for syslog messages is "logging trap severity." This command specifically sets the threshold for the messages that will be sent to a logging server based on their severity level. Severity levels in syslog range from 0 (emergency) to 7 (debug), allowing network administrators to filter out messages based on their importance. By using this command, an administrator can specify what level of log messages should be sent to the configured syslog server, thereby ensuring that only relevant information is logged according to the operational requirements. For example, if the severity is set to "warning," only messages classified as warning level or higher (error, critical, alert, and emergency) will be sent to the syslog server, while informational and debug messages will be ignored. The other options relate to different logging contexts or locations but do not specifically control the severity level for syslog messages directed to a logging server. Instead, they pertain to logging messages to other destinations, such as the console or a buffered log, rather than configuring the severity of messages sent to a syslog server.

7. What is a primary function of GRE in network communication?

A. It provides encryption for secure transmission.

B. It allows routing information to pass between connected networks.

C. It compresses data for faster transmission.

D. It ensures data integrity during transfer.

Generic Routing Encapsulation (GRE) is primarily used to encapsulate a wide variety of network layer protocols into point-to-point links over the Internet Protocol (IP). One of its key functions is to enable the transmission of routing information between connected networks, thereby facilitating the creation of virtual point-to-point links. This capability allows different types of network traffic to traverse networks as if they were on the same physical network, making it easier to implement complex network topologies and configurations like site-to-site connectivity. By allowing for the encapsulation of different protocols, GRE can support the use of multiple routing protocols and distinct addressing schemes across interconnected networks, enhancing overall interoperability and connectivity. While GRE does not provide encryption, compression, or ensure data integrity specifically, its primary role is to function as a tunneling protocol that bridges various networks and carries routing information effectively.

8. Which SD-WAN component provides programmatic interfaces for DevOps operations?

A. vSmart

B. vEdge

C. vManage

D. vBond

The correct response identifies vManage as the component that provides programmatic interfaces suitable for DevOps operations in an SD-WAN architecture. vManage is the centralized management component of Cisco's SD-WAN solution, allowing for the orchestration and management of network policies, monitoring, and analytics. In the context of DevOps, having programmatic interfaces is crucial because they enable automation and integration with existing workflows. vManage offers RESTful APIs, which allow developers and network operators to automate configurations, gather telemetry data, and manage network policies programmatically. This integration facilitates more streamlined operations, continuous deployment, and quicker response times to network changes or issues, aligning with DevOps principles that emphasize collaboration and automation. Each of the other components, while integral to the Cisco SD-WAN architecture, serves different functions: - vSmart handles the control and data plane security while ensuring policy distribution across the WAN. - vEdge is primarily responsible for the WAN edge routing and traffic handling. - vBond establishes secure connections between the other SD-WAN components. While these components are essential for the overall operation of the SD-WAN, they do not provide the same level of programmatic access and orchestration capabilities that vManage does, which is specifically designed to enable automation

9. Which severity level is used to indicate that a system is unusable?

A. Warning

B. Critical

C. Emergency

D. Info

The severity level that indicates a system is unusable is "Emergency." This classification reflects the highest level of urgency and severity, typically signifying that the system is down or in a state that prevents any normal operation. In practice, when an emergency occurs, immediate action is required to restore functionality, as operations are severely impacted and may halt altogether. In contrast, the other severity levels serve different purposes. A warning indicates potential issues that might escalate but do not currently impede system performance. Critical severity is serious and indicates significant problems that could cause major issues, yet the system may still be operational to some extent. The info level simply represents informational messages, which do not imply that any immediate action or concern is necessary. Understanding these distinctions is essential for effective IT service management and incident response.

10. What are two historical perspectives of AMP for endpoints?

A. File Trajectory and Device Trajectory

B. Network Trajectory and Behavior Analysis

C. Malware Detection and Prevention Strategies

D. Cloud Security and On-Premise Solutions

The concept of AMP (Advanced Malware Protection) for endpoints involves understanding the historical perspectives that have shaped its evolution. The correct answer highlights the significance of File Trajectory and Device Trajectory in tracking and analyzing malicious activities. File Trajectory refers to the ability to monitor a file's journey across the network and determine its origins, behaviors, and interactions with other files or systems over time. This provides insights into how malware infiltrates and propagates within an environment. Device Trajectory, on the other hand, focuses on the behavior of devices over time, examining how they interact with files, network traffic, and user behaviors. By understanding these trajectories, security teams can piece together the timeline of an attack and assess the full scope of its impact on the network. Utilizing both perspectives aids in developing a more comprehensive approach to endpoint security, enabling effective detection and response to threats. This historical context is crucial as it informs the design and functionality of contemporary AMP solutions.

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://ciscolearningnet.examzify.com

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