CCNA 3 ENTERPRISE NETWORKING, SECURITY, AND AUTOMATION, VERSION 7.0 PRACTICE EXAM (SAMPLE)

STUDY GUIDE

Prepare with structure. Pass with confidence

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. **In a WAN architecture, what is the primary purpose of a CSU/DSU?**

   A. To connect digital circuits to a router

   B. To provide redundancy in WAN links

   C. To encrypt WAN traffic

   D. To aggregate multiple WAN connections

2. **Which two types of attacks are typically used on DNS open resolvers? (Choose two.)**

   A. Amplification and reflection attacks.

   B. Data theft and phishing schemes.

   C. Resource utilization and packet sniffing.

   D. SQL injection and XSS attacks.

3. **Which two scenarios are examples of remote access VPNs? (Choose two.)**

   A. A mobile sales agent connecting via hotel Internet

   B. An office network with multiple users

   C. A user connecting through a corporate LAN

   D. An employee working from home using VPN client software

4. **Which OSPF table is the same on all converged routers within an OSPF area?**

   A. Routing table

   B. Link-state database

   C. Topology table

   D. Neighbor table

5. **In which OSPF state is the Designated Router (DR) and Backup Designated Router (BDR) election conducted?**

   A. Exstart

   B. Two-way

   C. Full

   D. Loading

6. What term refers to adding a value to the packet header to ensure it matches a defined policy?

A. Packet filtering

B. Traffic shaping

C. Traffic marking

D. Packet encapsulation

7. Why would a security testing team use fuzzers during a penetration test?

A. To improve network performance

B. To identify security vulnerabilities

C. To conduct routine maintenance

D. To optimize the routing protocols

8. In the context of network management, what role does NAT serve?

A. Assigning IP addresses dynamically

B. Routing data packets to the destination

C. Mapping private IP addresses to a public IP address

D. Securing the network by firewalling

9. Which protocol provides authentication, integrity, and confidentiality services as a type of VPN?

A. SSL.

B. IPsec.

C. PPTP.

D. L2TP.

10. How can an outside host gain access to the Cisco AnyConnect client if it is not preinstalled?

A. By using command line to download

B. By initiating a clientless VPN connection via a web browser

C. By accessing the company intranet

D. By calling tech support for assistance

Answers

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

Explanations

1. In a WAN architecture, what is the primary purpose of a CSU/DSU?

A. To connect digital circuits to a router

B. To provide redundancy in WAN links

C. To encrypt WAN traffic

D. To aggregate multiple WAN connections

The primary purpose of a CSU/DSU (Channel Service Unit/Data Service Unit) is to connect digital circuits to a router. In a WAN environment, it serves as an interface between the end-user equipment, such as a router, and the digital telephone line or circuit provided by the telecommunication carrier. When a router is connected to a digital circuit, it cannot directly interface with the line that carries the data. The CSU/DSU handles the necessary signal conditioning and line monitoring to ensure that the data can be transmitted effectively. It translates the digital signals from the router into a format compatible with the WAN circuit and vice versa. This allows routers and other network devices to communicate over various types of WAN connections like T1 or E1 lines, making the CSU/DSU a critical component in establishing a reliable WAN connection. Additionally, it performs error correction and line monitoring to maintain the integrity of the connection. This functionality enables smooth operations and optimal data transmission rates over long distances, which is essential in wide area networks.

2. Which two types of attacks are typically used on DNS open resolvers? (Choose two.)

A. Amplification and reflection attacks.

B. Data theft and phishing schemes.

C. Resource utilization and packet sniffing.

D. SQL injection and XSS attacks.

The choice of amplification and reflection attacks as the correct answer highlights the vulnerabilities associated with DNS open resolvers. These attacks exploit the way DNS operates, particularly when open resolvers are misconfigured to respond to requests from any source on the internet. In an amplification attack, an attacker sends a small query to a DNS resolver that results in a much larger response being sent to the targeted victim's address. This is possible due to the inherent nature of DNS, where a single query can produce a significantly larger reply, often many times greater in size than the original request. This can overwhelm the victim's network resources. Reflection attacks, similarly, involve an attacker sending a request to a DNS server with the source address spoofed to that of the intended victim. The DNS server responds to what it believes is a legitimate query but actually sends that response to the victim. This can also lead to network congestion and denial of service. These two attack types are particularly relevant to DNS open resolvers because they highlight how DNS can be misused if strict security measures are not implemented. Open resolvers that accept and respond to queries from any source can easily become targets for these forms of abuse, making it critical for administrators to configure DNS servers to limit who can query them.

3. Which two scenarios are examples of remote access VPNs? (Choose two.)

A. A mobile sales agent connecting via hotel Internet

B. An office network with multiple users

C. A user connecting through a corporate LAN

D. An employee working from home using VPN client software

Remote access VPNs enable individual users to connect to a private network from a remote location over the internet. This type of VPN allows users to access the organization's resources as though they were directly connected to the corporate network. A mobile sales agent connecting via hotel Internet represents a typical scenario for remote access VPNs. In this situation, the sales agent uses a public Internet connection from a hotel to create a secure tunnel back to the company's network, facilitating access to necessary resources while on the go. The use of a remote access VPN in this case ensures that sensitive data remains secure over potentially insecure networks. An employee working from home using VPN client software is another clear example of a remote access VPN scenario. In this case, the employee is connecting to the corporate network from home, using VPN client software to establish a secure connection. This allows them to work as if they were physically in the office, providing access to the company's internal resources while maintaining security through encryption and tunneling protocols. The other scenarios presented do not fit the definition of remote access VPNs. An office network with multiple users typically involves site-to-site VPN connections that link entire networks together rather than individual remote access. Connecting through a corporate LAN implies that the user is already within the secure network environment and

4. Which OSPF table is the same on all converged routers within an OSPF area?

A. Routing table

B. Link-state database

C. Topology table

D. Neighbor table

The link-state database (LSDB) contains the complete information about the topology of the network as seen by each OSPF router within an area. When OSPF routers exchange link-state advertisements (LSAs) during the process of establishing connectivity and maintaining routes, they all build their LSDBs based on the same set of LSAs. This results in each router within the same OSPF area having an identical view of the network topology. Maintaining a consistent LSDB is crucial for OSPF to function correctly since all routers will calculate their own routing tables using the same topology information from the LSDB. This synchronization leads to a stable and loop-free routing environment within the OSPF area. Other choices do not provide the same level of consistency across routers. The routing table varies based on individual router configurations and paths learned from the routing decisions made after processing the LSDB. The topology table is not a standard term used in OSPF; instead, OSPF utilizes the LSDB and the routing table. The neighbor table, which lists neighboring routers, can differ between routers due to their individual adjacency relationships. Therefore, the link-state database is the only component that is uniform across all routers within an OSPF area.

5. In which OSPF state is the Designated Router (DR) and Backup Designated Router (BDR) election conducted?

A. Exstart

B. Two-way

C. Full

D. Loading

The OSPF state where the Designated Router (DR) and Backup Designated Router (BDR) election takes place is the Two-way state. During this state, OSPF routers exchange hello packets to establish neighbor relationships and to determine which routers are on the same segment. In the Two-way state, each router will recognize the other routers it can communicate with and will identify eligible routers that can participate in the election of the DR and BDR. The criteria for election usually favor the router with the highest OSPF priority, or if the priorities are the same, the highest Router ID. Once the election process is completed in this state, the selected DR and BDR will be responsible for generating and distributing link state updates within that broadcast domain, which is essential for efficient OSPF operation. This process helps to minimize routing traffic, as only the DR will communicate with other OSPF routers, and the BDR provides redundancy in case the DR fails. Subsequent states, such as Exstart, Full, and Loading, focus on the exchange of link-state information but do not involve the election of the DR and BDR; this is why the Two-way state is specifically significant in the context of establishing who will serve

6. What term refers to adding a value to the packet header to ensure it matches a defined policy?

A. Packet filtering

B. Traffic shaping

C. Traffic marking

D. Packet encapsulation

The term that refers to adding a value to the packet header to ensure it aligns with a defined policy is traffic marking. Traffic marking involves adding specific identifiers, often referred to as tags or markings, to packets as they traverse through a network. This practice is essential in quality of service (QoS) implementations, where priority and resource allocation need to be defined based on the type of traffic or specific network policies. By marking packets, network devices such as routers and switches can make informed decisions about how to handle each packet as it moves through the network. For instance, packets marked for higher priority might be given preferential treatment in terms of bandwidth allocation or reduced latency. In contrast, while packet filtering involves examining and approving or denying packets based on specific criteria, it does not involve modifying the packet itself. Traffic shaping manages congestion by controlling the flow of packets, but it doesn't typically entail adding values to headers like traffic marking does. Packet encapsulation refers to wrapping data with headers and trailers for transport but is not specifically about adding values for policy enforcement.

7. Why would a security testing team use fuzzers during a penetration test?

A. To improve network performance

B. To identify security vulnerabilities

C. To conduct routine maintenance

D. To optimize the routing protocols

Using fuzzers during a penetration test is primarily aimed at identifying security vulnerabilities within software applications and systems. Fuzzing is a technique that involves sending a wide range of invalid, unexpected, or random data—commonly known as "fuzz"—to the inputs of a program. The objective is to discover how the application handles improperly formatted or unexpected inputs, which may lead to crashes, memory leaks, buffer overflows, or other unintended behaviors that can be exploited by attackers. By systematically testing various inputs, security testing teams can uncover flaws that may not be evident through traditional testing methods. This proactive approach enables organizations to address potential weaknesses before they can be exploited, thereby enhancing the overall security posture of the application or system being tested. The other options relate to different goals that are not aligned with the primary function of fuzzing. Improving network performance and optimizing routing protocols focus on efficiency and effectiveness of network operations, while conducting routine maintenance pertains to regular upkeep tasks that do not directly relate to security testing.

8. In the context of network management, what role does NAT serve?

A. Assigning IP addresses dynamically

B. Routing data packets to the destination

C. Mapping private IP addresses to a public IP address

D. Securing the network by firewalling

NAT, or Network Address Translation, serves a critical role in mapping private IP addresses to a public IP address. This is particularly important in networking because it allows multiple devices on a local network to communicate with external networks using a single public IP address. NAT ensures that devices with private IP addresses, which are not routable on the internet, can still access the internet while providing an essential layer of IP address conservation. When a device with a private IP requests data from the internet, the NAT-enabled router changes the source IP address in the outgoing data packets to its own public IP address. When a response comes back, the router translates the public IP address back to the corresponding private IP address, directing the data back to the correct device on the local network. This process not only facilitates communication but also helps to enhance security by obscuring the internal network structure from potential external threats. In summary, the primary function of NAT is to allow private IP addresses to be mapped to a single public IP address, effectively enabling internet connectivity for devices that would otherwise be unable to communicate externally.

9. Which protocol provides authentication, integrity, and confidentiality services as a type of VPN?

A. SSL.

B. IPsec.

C. PPTP.

D. L2TP.

IPsec, or Internet Protocol Security, is the correct answer because it is specifically designed to provide comprehensive security services, which include authentication, integrity, and confidentiality for data being transmitted over networks, particularly those using the Internet Protocol (IP). By utilizing encryption and authentication protocols, IPsec ensures that data packets are securely communicated between two endpoints. This is particularly vital for virtual private networks (VPNs), as it creates a secure tunnel for transferring sensitive data over public networks. IPsec works at the network layer, which allows it to protect all IP traffic, and can operate in two modes: transport mode, which encrypts only the payload of the IP packet, and tunnel mode, which encrypts the entire IP packet. While other protocols mentioned also have roles in establishing VPNs, they do not provide the same level of combined security services as IPsec. For instance, SSL is primarily used for secure web communications and does not natively include IP-level protection. PPTP and L2TP are older protocols that may not offer the same strength of encryption and are often paired with IPsec to enhance security. Thus, IPsec stands out as the robust choice for VPN implementations requiring comprehensive security measures.

10. How can an outside host gain access to the Cisco AnyConnect client if it is not preinstalled?

A. By using command line to download

B. By initiating a clientless VPN connection via a web browser

C. By accessing the company intranet

D. By calling tech support for assistance

An outside host can gain access to the Cisco AnyConnect client by initiating a clientless VPN connection via a web browser because this process allows users to connect to the VPN without needing the client preinstalled on their device. When a user navigates to the VPN login page using a browser, they can log in and, as part of the process, are often provided with a prompt or link to download the necessary AnyConnect client. This method is efficient for users who may not have administrative access to install software on their machines or want to avoid complex installations. In contrast, simply using the command line to download the client is usually not straightforward or user-friendly for most users who may not be tech-savvy. Accessing the company intranet directly does not provide the necessary VPN capabilities unless the client is already installed. Calling tech support could assist the user but does not directly enable access to the VPN in a timely manner. Therefore, initiating a clientless VPN connection is the most user-friendly and intuitive method for obtaining the AnyConnect client when it is not preinstalled.

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://ccna3enterprisenetsecautomationv7.examzify.com

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