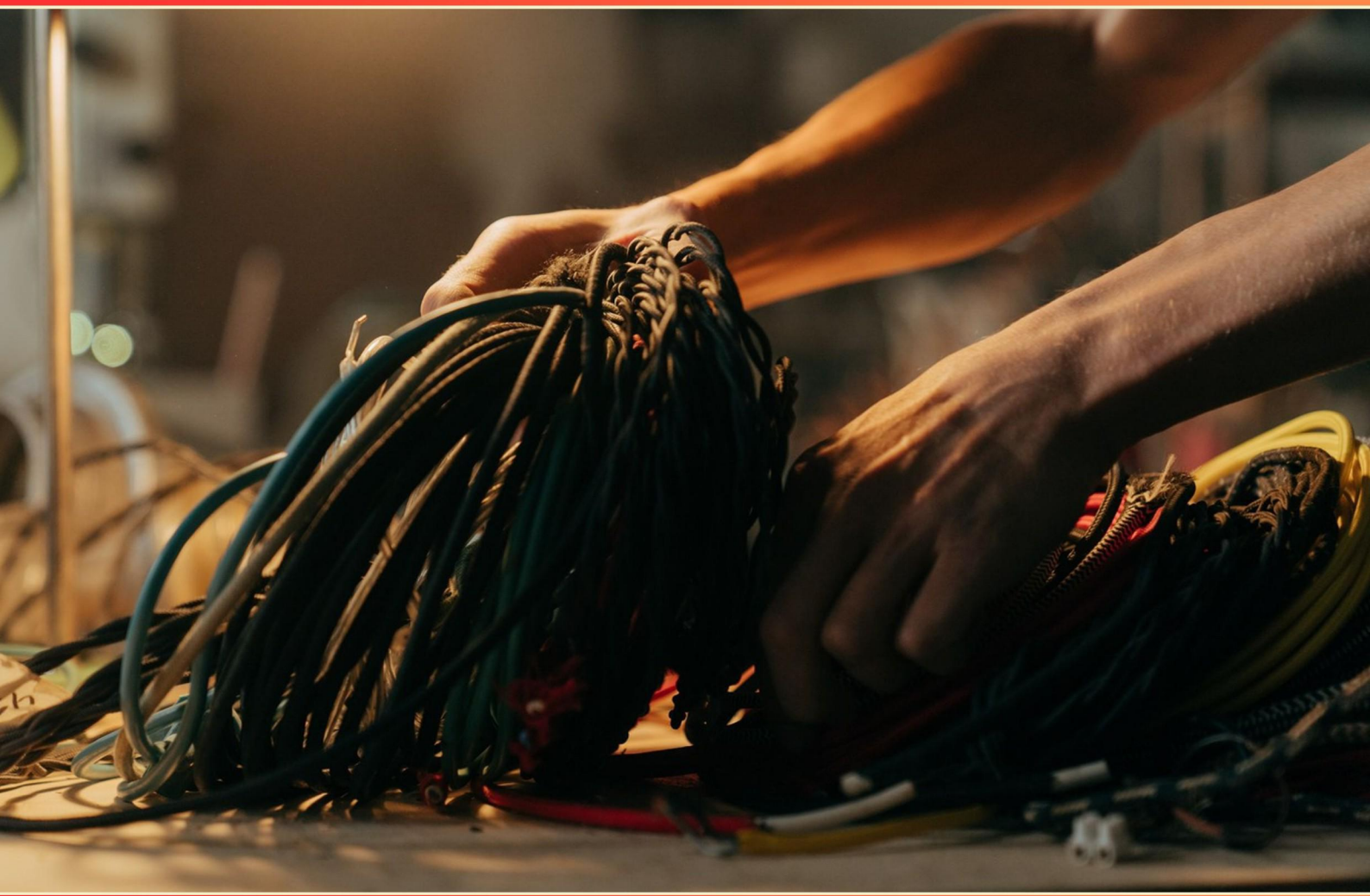
CCNP 350-401 – IMPLEMENTING AND OPERATING CISCO ENTERPRISE NETWORK CORE TECHNOLOGIES (ENCOR) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://ccnp350401.examzify.com

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 is the recommended overlap percentage for access points in a wireless network that supports voice and video?

A. 20%

B. 35%

C. 50%

D. 70%

2. Which wireless standard operates at both 2.4 GHz and 5 GHz?

A. 802.11a

B. 802.11b

C. 802.11g

D. 802.11n

3. What is the primary purpose of a BPDU Guard?

A. To ignore all BPDUs on the interface

B. To prevent STP loops by disabling the interface if BPDUs are received

C. To enable Portfast on trunk links

D. To globally enable STP on all interfaces

4. What does the "On" mode indicate for PAgP?

A. Interface successfully negotiates to become an EtherChannel

B. No negotiation takes place

C. Interface will wait for the other side to negotiate

D. Interface will actively start negotiation

5. What is the duration a switch will keep a dynamic MAC address entry if it is not seen again?

A. 60 seconds

B. 120 seconds

C. 300 seconds

D. 600 seconds

6. In what mode does an AP serve as a dedicated point-to-point or point-to-multipoint bridge?

A. FlexConnect Mode

B. Bridge/Mesh Mode

C. Sniffer Mode

D. Local Mode

7. What is the purpose of an Independent Basic Service Set (IBSS)?

A. Connecting multiple access points in a large building

B. Enabling direct communication between wireless devices without an AP

C. Providing centralized management for a network

D. Serving as the main access point for wireless networks

8. What does UDLD stand for in networking?

A. Unidirectional Link Detection

B. Unilateral Link Distribution

C. Unified Data Link Definition

D. Universal Data Link Detection

9. Which of the following is NOT a characteristic of cloud computing?

A. On-demand self-service

B. Limited network access

C. Rapid elasticity

D. Resource pooling

10. Which wireless network type utilizes a mesh structure to connect access points?

A. Independent Basic Service Set

B. Extended Service Set

C. Mesh Basic Service Set

D. Basic Service Set

Answers

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

Explanations

1. What is the recommended overlap percentage for access points in a wireless network that supports voice and video?

A. 20%

B. 35%

C. 50%

D. 70%

In a wireless network designed to support voice and video applications, achieving seamless connectivity and high-quality service is essential. The recommended overlap percentage of 35% ensures that there are enough overlapping coverage areas between access points to maintain a strong and consistent signal for users, especially for bandwidth-heavy applications like voice and video. This overlap allows for smoother handoffs between access points as devices move within the coverage area. It prevents dropped connections and ensures call quality is maintained, as both voice and video require a reliable connection to function effectively. A lower overlap percentage might lead to inconsistent coverage, while a higher overlap could result in excessive co-channel interference, degrading the overall network performance. Thus, adhering to a 35% overlap strikes a balance between ensuring strong coverage and minimizing interference, making it the recommended setting for networks that cater to real-time traffic such as voice and video.

2. Which wireless standard operates at both 2.4 GHz and 5 GHz?

A. 802.11a

B. 802.11b

C. 802.11g

D. 802.11n

The wireless standard that operates at both 2.4 GHz and 5 GHz is 802.11n. This standard was introduced to enhance the capabilities of previous standards by utilizing multiple-input multiple-output (MIMO) technology, which allows for increased throughput and better performance in diverse environments. One of the key features of 802.11n is its ability to operate in both the 2.4 GHz and 5 GHz frequency bands. This dual-band capability provides flexibility in network design and allows users to select the band that offers the best performance based on their specific conditions. The 2.4 GHz band typically provides better range but can be more congested due to interference from other devices, while the 5 GHz band offers higher speeds and less interference, albeit with a shorter range. This dual-band functionality distinguishes 802.11n from earlier standards such as 802.11a, which only operates in the 5 GHz range; 802.11b, which operates solely in the 2.4 GHz range; and 802.11g, which operates at 2.4 GHz but does not support the 5 GHz frequency. Thus, 802.11n stands out as the option that supports both frequency ranges

3. What is the primary purpose of a BPDU Guard?

A. To ignore all BPDUs on the interface

B. To prevent STP loops by disabling the interface if BPDUs are received

C. To enable Portfast on trunk links

D. To globally enable STP on all interfaces

The primary purpose of BPDU Guard is to enhance the stability and security of a network by preventing potential loops in the Spanning Tree Protocol (STP). When BPDU Guard is enabled on an interface, it actively monitors for Bridge Protocol Data Units (BPDUs). If any BPDUs are received on an interface that has BPDU Guard activated—typically an edge port configured with PortFast—the interface will be disabled immediately to prevent any risk of a loop forming. This feature is particularly useful in scenarios where an end host or device, which should not participate in STP, is inadvertently connected to a port that is configured to monitor for BPDUs. By disabling the interface upon detection of these packets, BPDU Guard helps to maintain the integrity of the network topology and ensures that the STP process remains effective in preventing loops. The other options, such as ignoring all BPDUs, enabling PortFast on trunk links, or globally enabling STP on all interfaces, do not accurately capture the essential function of BPDU Guard, which focuses specifically on reacting to the presence of BPDUs to secure the network.

4. What does the "On" mode indicate for PAgP?

A. Interface successfully negotiates to become an EtherChannel

B. No negotiation takes place

C. Interface will wait for the other side to negotiate

D. Interface will actively start negotiation

The "On" mode for Port Aggregation Protocol (PAgP) indicates that the interface will not engage in any negotiation to form an EtherChannel. When an interface is configured in "On" mode, it assumes that an EtherChannel will be established without the need for any protocol exchanges or negotiation with the connected device. This means that the port will try to bundle with the other end immediately, expecting it to also be configured in a compatible mode (like "On") without the use of PAgP or any other negotiation mechanism. In contrast to other modes, such as "Desirable" or "Auto," which involve negotiation, "On" mode simplifies the configuration by eliminating the need for any interaction or checks to determine if the other interface is ready to form an EtherChannel. This approach can lead to more straightforward setups but demands identical configurations on both ends to successfully create an EtherChannel, as there's no fallback to handle mismatches.

5. What is the duration a switch will keep a dynamic MAC address entry if it is not seen again?

A. 60 seconds

B. 120 seconds

C. 300 seconds

D. 600 seconds

A switch maintains dynamic MAC address entries in its MAC address table for a specific duration if there is no further communication from that MAC address. The correct duration for retaining a dynamic MAC address entry is 300 seconds, or 5 minutes. This time allows the network to accommodate nodes that may go inactive temporarily, while still cleaning up the MAC address table to remove entries that are no longer needed. After 300 seconds of inactivity, the switch will remove the MAC address from its table, which helps conserve memory and ensures that the address table remains updated with active devices. This behavior is part of the switch's functionality in managing its MAC address learning and aging process. Understanding this timeframe is important for network design and troubleshooting, as it can affect how quickly new devices can communicate on the network and how the switch optimally manages its resources.

6. In what mode does an AP serve as a dedicated point-to-point or point-to-multipoint bridge?

A. FlexConnect Mode

B. Bridge/Mesh Mode

C. Sniffer Mode

D. Local Mode

The correct answer is Bridge/Mesh Mode. In this configuration, an access point (AP) functions as a dedicated bridge, allowing it to connect multiple networks over a wireless link. This mode can be particularly useful in scenarios where extending wired networks wirelessly is desirable, such as connecting two buildings without running cables between them. In Bridge/Mesh Mode, the AP can operate in either a point-to-point or point-to-multipoint manner, thus enabling communication between various endpoints. Point-to-point communication typically involves connecting two specific locations, while point-to-multipoint facilitates a single AP to communicate with multiple clients or endpoints, significantly enhancing network flexibility and coverage. FlexConnect Mode is primarily aimed at allowing APs to function as standalone devices while still being managed by a centralized controller, especially in remote locations. This mode focuses on local switching and is not specifically designed for bridging functions. Sniffer Mode allows an AP to capture wireless packets for monitoring purposes, which is useful in network analysis and troubleshooting, but it does not provide any bridging capabilities. Local Mode is the most common operational mode where an AP handles client data and control traffic locally, but it does not serve as a dedicated bridge for point-to-point or point-to-multipoint connections. Understanding the function

7. What is the purpose of an Independent Basic Service Set (IBSS)?

A. Connecting multiple access points in a large building

B. Enabling direct communication between wireless devices without an AP

C. Providing centralized management for a network

D. Serving as the main access point for wireless networks

The purpose of an Independent Basic Service Set (IBSS) is to enable direct communication between wireless devices without the need for an access point (AP). In this configuration, devices can communicate with each other in an ad hoc manner, which is beneficial for scenarios where a wireless infrastructure is not available or when devices need to connect temporarily without the overhead of a centralized network. Each device acts as a peer, facilitating a decentralized network that allows for the sharing of resources directly among connected devices. This setup is particularly useful in situations such as meetings or collaboration sessions where users quickly need to exchange data without relying on a traditional network setup. The other options relate to different aspects of wireless networking. Connecting multiple access points is typical of an Extended Service Set (ESS), which provides a larger coverage area. Centralized management is associated with wireless LAN controllers and infrastructures that manage multiple APs and devices optimally. Serving as the main access point implicates the functioning of a basic service set (BSS), which utilizes a single AP to manage client connections instead of allowing peer-to-peer communication as in an IBSS.

8. What does UDLD stand for in networking?

A. Unidirectional Link Detection

B. Unilateral Link Distribution

C. Unified Data Link Definition

D. Universal Data Link Detection

UDLD stands for Unidirectional Link Detection. This networking protocol is designed to detect unidirectional links that can occur due to a misconfiguration or a physical fault. Unidirectional links can lead to undesirable network behavior because they may cause traffic to flow in one direction without the ability to return effectively, potentially resulting in a network loop or loss of connectivity. In environments where redundant paths are present, it's crucial to identify and disable unidirectional links to maintain the stability and efficiency of the network. UDLD sends messages over a link to ensure that devices on both ends can communicate in both directions. If a device does not receive a response from its counterpart within a specified timeframe, it will assume that the link is unidirectional and can take appropriate action, such as disabling the port to prevent issues. Other choices, while they may seem plausible, do not accurately reflect the meaning or function of UDLD, which specifically emphasizes its role in detecting communication issues related to directionality in network links.

9. Which of the following is NOT a characteristic of cloud computing?

A. On-demand self-service

B. Limited network access

C. Rapid elasticity

D. Resource pooling

Cloud computing is characterized by several key features that distinguish it from traditional computing environments. On-demand self-service allows users to provision resources as needed without requiring human intervention from the service provider. Rapid elasticity highlights the ability to scale resources quickly, either up or down, in response to demand. Resource pooling refers to the efficient use of resources to serve multiple consumers, where physical and virtual resources are dynamically assigned and reassigned based on demand. Limited network access is not a characteristic of cloud computing. In fact, cloud computing typically emphasizes broad network access, allowing users to access services and resources over the internet from a variety of devices, including smartphones, tablets, and computers. This contrasts with the notion of being limited in access, which would not align with the fundamental principles of cloud services that prioritize availability and connectivity. Thus, the correct answer that identifies something that is NOT characteristic of cloud computing is the aspect regarding limited network access.

10. Which wireless network type utilizes a mesh structure to connect access points?

A. Independent Basic Service Set

B. Extended Service Set

C. Mesh Basic Service Set

D. Basic Service Set

The Mesh Basic Service Set (MBSS) is specifically designed to connect multiple access points in a mesh configuration, enabling a decentralized and self-healing network layout. This structure allows each access point to communicate with others, ensuring that if one link fails, the data can still find alternate routes through the mesh. This choice supports improved reliability and coverage, particularly in environments where traditional wiring may not be feasible or where extended range and resilience against single points of failure are crucial. In contrast, the other types of networks mentioned do not leverage a mesh architecture. The Independent Basic Service Set (IBSS) typically refers to an ad-hoc network where devices connect directly without any centralized access points. The Extended Service Set (ESS) is designed to expand coverage across multiple access points using a common SSID, but it maintains a centralized hierarchical structure. The Basic Service Set (BSS) represents a simple service set where devices connect to a single access point, lacking the redundancy and dynamic routing capabilities found in mesh networking. Hence, the Mesh Basic Service Set stands out as the correct answer due to its unique structure that enables robust interconnectivity among access points in a wireless network.

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://ccnp350401.examzify.com

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