CCNP 350-401 – Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) Practice Test (Sample)

Study Guide

BY EXAMZIFY

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

SAMPLE

1. **In which frequency range does 802.11g operate?**
   A. 2.4-2.485 GHz
   B. 2.4-2.4835 GHz
   C. 5-5.825 GHz
   D. 900-928 MHz

2. **What is the function of a Switching Database Manager (SDM)?**
   A. Determining memory availability for applications
   B. Managing network security protocols
   C. Determining TCAM space and usage on switches
   D. Monitoring switch temperature and health

3. **What distinguishes CAPWAP data messages from control messages?**
   A. Usage of different types of encryption
   B. Encapsulation of wireless client packets
   C. Different UDP ports are utilized
   D. Control messages do not require authentication

4. **What is Active-Active Weighted application traffic forwarding?**
   A. Multiple active paths that are load balanced
   B. Multiple active paths, but with weighting to allow certain paths to take on more traffic than others
   C. A single active path for all traffic forwarding
   D. Paths are inactive until needed

5. **What type of BPDU is used to communicate changes in Layer 2 topology?**
   A. Configuration BPDU
   B. Forwarding BPDU
   C. Topology Change Notification BPDU
   D. Blocking BPDU

6. What happens during wireless signal scattering?

    A. The signal travels uninterrupted

    B. The signal increases in strength

    C. The signal is absorbed entirely

    D. The signal breaks apart and weakens

7. What is an OSPF Inter-Area route?

    A. Routes learned from external sources

    B. Routes learned from static routes configured on the router

    C. Network routes learned from other OSPF routers in the same area

    D. Network routes learned from other OSPF routers in different areas

8. What does RTLS stand for in the context of networking technology?

    A. Rapid Technology Location Services

    B. Real-Time Location Services

    C. Remote Test Location Services

    D. Real-Time Traffic Location Services

9. How is BPDU Guard configured globally on all access ports?

    A. spanning-tree bpduguard all

    B. spanning-tree portfast bpduguard

    C. spanning-tree portfast bpduguard default

    D. spanning-tree bpduguard default

10. What is the primary function of Deep Packet Inspection (DPI)?

    A. To monitor bandwidth usage

    B. To identify application type by examining packet contents

    C. To encrypt traffic for security

    D. To block unauthorized access

Answers

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

Explanations

1. In which frequency range does 802.11g operate?

A. 2.4-2.485 GHz

B. 2.4-2.4835 GHz

C. 5-5.825 GHz

D. 900-928 MHz

The 802.11g standard operates in the 2.4 GHz frequency range, specifically within the band of 2.4 to 2.4835 GHz. This range allows for wireless networking at speeds of up to 54 Mbps, while also maintaining backward compatibility with earlier standards like 802.11b, which also operated in the 2.4 GHz band.   The option indicating 2.4-2.485 GHz, while close, extends slightly beyond the official 802.11g range, which specifies up to 2.4835 GHz. The choice of 5-5.825 GHz pertains to the 802.11a standard, which does not align with 802.11g specifications. Similarly, the range of 900-928 MHz refers to different wireless communication standards and is not applicable to 802.11g. Thus, the defined frequency range of 2.4-2.4835 GHz in the correct choice accurately reflects the operational parameters for 802.11g in the context of wireless networking.

2. What is the function of a Switching Database Manager (SDM)?

A. Determining memory availability for applications

B. Managing network security protocols

C. Determining TCAM space and usage on switches

D. Monitoring switch temperature and health

The Switching Database Manager (SDM) plays a crucial role in the operation of Cisco switches by managing the hardware resources that are essential for performing various switching tasks. Its primary function is to determine the TCAM (Ternary Content Addressable Memory) space and usage on switches. TCAM is a specialized type of memory that allows for fast lookups, which is important in handling tasks like routing and access control. Since TCAM can store multiple bits of information and perform lookups based on more than just binary states (success, failure), it is particularly useful for advanced features such as Access Control Lists (ACLs) and Quality of Service (QoS) policies. The SDM ensures that the TCAM is allocated properly according to the configuration and operational requirements of the switch, helping to optimize performance and resource utilization. By managing TCAM allocation effectively, SDM ensures that the switch can handle the intended network traffic and security policies without resource bottlenecks. This functionality is fundamental in high-performance networking environments where efficiency and speed are critical.

3. What distinguishes CAPWAP data messages from control messages?

A. Usage of different types of encryption

B. Encapsulation of wireless client packets

C. Different UDP ports are utilized

D. Control messages do not require authentication

The distinction between CAPWAP data messages and control messages lies in the encapsulation of wireless client packets. CAPWAP (Control and Provisioning of Wireless Access Points) is designed to facilitate communication between access points and a controller in a wireless LAN architecture. Data messages are responsible for carrying encapsulated packets that are transmitted between the wireless client devices and the wired network, effectively handling user traffic. In contrast, control messages are utilized for managing and configuring the access points. These messages include information needed for the setup, maintenance, and operation of the wireless access point, without actually carrying the user traffic itself. This encapsulation process ensures that user data can be efficiently transported while control messages remain focused on the configuration and control aspects of the wireless network. The correct choice highlights this essential aspect of CAPWAP communication, emphasizing the role of data messages in transporting user packets and differentiating them from control messages.

4. What is Active-Active Weighted application traffic forwarding?

A. Multiple active paths that are load balanced

B. Multiple active paths, but with weighting to allow certain paths to take on more traffic than others

C. A single active path for all traffic forwarding

D. Paths are inactive until needed

Active-Active Weighted application traffic forwarding refers to a scenario in which multiple paths are simultaneously active, and traffic is distributed across these paths based on assigned weights. Each path is designated a weight which determines the proportion of traffic it will handle. This allows for a more efficient use of available resources as certain paths can accommodate more traffic due to their capacity or performance characteristics, while still having other paths participate in traffic forwarding. This method enhances load balancing by allowing for dynamic adjustments based on the capabilities of each path, ensuring that no single path becomes a bottleneck while maximizing throughput and redundancy. In networks where bandwidth and performance can vary significantly from one path to another, leveraging weights is crucial for optimizing traffic flows.

5. What type of BPDU is used to communicate changes in Layer 2 topology?

A. Configuration BPDU

B. Forwarding BPDU

C. Topology Change Notification BPDU

D. Blocking BPDU

The Topology Change Notification BPDU is specifically designed to inform switches of changes in the Layer 2 topology. When a switch detects that a port has transitioned into a forwarding state, or when a device is added or removed from the network, it generates a Topology Change Notification BPDU to alert other switches about the change. This timely notification allows the switches to update their spanning tree calculations and ensure that the network continues to function efficiently and without loops. Configuration BPDUs are used primarily to convey the configuration of the spanning tree protocol itself, such as the bridge ID and root port, but not necessarily focused on immediate changes in the topology. Forwarding BPDUs do not exist as a distinct category; typically, BPDUs serve the configuration and notification roles. Blocking BPDUs also do not exist as a standalone category but rather refer to the state of a port that does not participate in frame forwarding to prevent loops, rather than communicating topology changes. Understanding the specific role of each type of BPDU helps in grasping how Spanning Tree Protocol (STP) works to maintain a loop-free network environment.

6. What happens during wireless signal scattering?

A. The signal travels uninterrupted

B. The signal increases in strength

C. The signal is absorbed entirely

D. The signal breaks apart and weakens

During wireless signal scattering, the signal encounters obstacles, such as buildings, trees, or even atmospheric conditions, leading to a change in its trajectory. Rather than traveling in a straight line, the signal disperses in various directions. This scattering effect can result in a broken or weakened signal as it propagates, causing issues like reduced data transmission rates or increased latency in wireless networks. This phenomenon is critical to understand when designing and deploying wireless networks, as it can significantly impact coverage and signal quality. The other options do not accurately represent the physical processes involved in scattering, as they imply scenarios where the signal remains intact or improves, which is contrary to how scattering affects signal strength and integrity.

7. What is an OSPF Inter-Area route?

   A. Routes learned from external sources

   B. Routes learned from static routes configured on the router

   C. Network routes learned from other OSPF routers in the same area

   D. Network routes learned from other OSPF routers in different areas

An OSPF Inter-Area route refers to routes that are learned from other OSPF routers that reside in different areas. OSPF (Open Shortest Path First) is a link-state routing protocol that organizes networks into areas to optimize routing and manage bandwidth. When OSPF routers exchange information, they share routes within their own area as well as summarize and share routing information between different areas. Inter-Area routes are identified by Type 3 Link-State Advertisements (LSAs), which are used to inform routers in one area about the network information present in another area. This type of route allows OSPF to maintain a hierarchical and segmented routing structure while still ensuring connectivity across the entire OSPF domain. In contrast, routes learned from external sources refer to OSPF external routes (Type 5 LSAs) and are not classified as Inter-Area routes. Static routes configured on the router do not involve OSPF and are defined manually, while routes learned from OSPF routers within the same area pertain to intra-area routes rather than inter-area routes. Thus, the distinction lies in the origin of the routing information, which emphasizes the importance of understanding how OSPF structures its routing tables across different areas for efficiency

8. What does RTLS stand for in the context of networking technology?

   A. Rapid Technology Location Services

   B. Real-Time Location Services

   C. Remote Test Location Services

   D. Real-Time Traffic Location Services

The correct answer, Real-Time Location Services, refers to a technology that enables the real-time tracking of assets within a defined area. In the context of networking, RTLS utilizes wireless networks, such as Wi-Fi, to determine the precise location of devices or items. This is highly beneficial in various applications, such as inventory management, asset tracking, and monitoring the movements of individuals within environments like hospitals, factories, or offices. Real-Time Location Services leverage various technologies, including RFID, infrared, and ultrasound, to provide accurate location data. This capability allows organizations to improve operational efficiency, enhance security, and deliver better services by ensuring that assets are located quickly and accurately. The other choices, while containing phrases that seem plausible, do not reflect the widely recognized definition and application of RTLS. Each of those alternatives does not accurately capture the essence of what RTLS provides in networking contexts, particularly in terms of real-time tracking and asset management capabilities.

9. How is BPDU Guard configured globally on all access ports?

A. spanning-tree bpduguard all

B. spanning-tree portfast bpduguard

C. spanning-tree portfast bpduguard default

D. spanning-tree bpduguard default

The correct configuration for enabling BPDU Guard globally on all access ports is through the command that specifies the default setting for BPDU Guard in conjunction with PortFast. By using the command that includes "default," it allows the BPDU Guard feature to be activated automatically on all access ports where PortFast is enabled. This is particularly important in a network to prevent loops caused by unexpected Bridge Protocol Data Units (BPDUs) being received on ports that should not participate in the spanning tree. When BPDU Guard is enabled globally, it ensures that any access port configured for PortFast will transition to an error-disabled state if it receives a BPDU. This is a protective mechanism that helps maintain the stability of the network by preventing possible loops or topology changes that could disrupt the network operation. The other options focus on either enabling BPDU Guard without the global default application or do not correctly relate to configuring it for all access ports. By using the command that includes "default," administrators ensure consistency across the network without needing to individually configure each access port.

10. What is the primary function of Deep Packet Inspection (DPI)?

A. To monitor bandwidth usage

B. To identify application type by examining packet contents

C. To encrypt traffic for security

D. To block unauthorized access

The primary function of Deep Packet Inspection (DPI) is to identify application type by examining packet contents. DPI goes beyond standard packet filtering by analyzing the data within packets, which allows for more granular inspection of network traffic. This capability enables network administrators to classify and manage applications based on their specific protocols and content, rather than just their headers. This level of inspection can assist in enforcing policies, optimizing bandwidth usage, and ensuring compliance with regulatory requirements. DPI helps in identifying the applications that are consuming the most resources or are involved in potentially malicious behavior, thereby providing better insight into network performance and security. The other options presented serve different purposes that are not the primary focus of DPI. Monitoring bandwidth usage typically pertains to tools designed for traffic analysis rather than detailed inspection of packet contents. Encrypting traffic is a separate function related to securing data, and blocking unauthorized access pertains to firewall capabilities and security measures that differ from the packet inspection process. Thus, while these options relate to network management and security, they do not embody the core functionality of Deep Packet Inspection.

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!