# Network Implementation: Routing, Switching, and Wireless Protocols 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. Which OSPF area type explicitly allows Type-7 LSAs to summarize external routes and does not carry Type-5 LSAs?**

**A. Totally Stubby Area**

**B. Normal**

**C. NSSA**

**D. Stub**

**2. Which protocol uses AES-CCMP encryption?**

**A. WEP**

**B. WPA**

**C. WPA2**

**D. WPA3**

**3. What term describes a rogue wireless access point that broadcasts the same SSID as a legitimate network?**

**A. Impostor AP**

**B. Eavesdropping AP**

**C. Honeypot AP**

**D. Evil Twin**

**4. Which statement about CAM table aging is true?**

**A. Entries never age.**

**B. Entries age out after a period of inactivity.**

**C. Aging increases CAM size automatically.**

**D. Aging causes frames to be dropped.**

**5. Which statement describes the purpose of Quality of Service in networks?**

**A. Prioritize critical traffic to improve performance**

**B. Encrypt all data by default**

**C. Map IP addresses to MAC addresses**

**D. Determine device IP assignments**

**6. What are the advantages and limitations of using QoS in networks, and how would you implement basic QoS for VoIP traffic?**

**A. QoS always improves throughput and has no downsides.**

**B. QoS provides predictable performance but adds complexity and may reduce throughput if misconfigured; implement by classifying traffic, marking DSCP/CoS, creating queues, and prioritizing VoIP with strict or high priority.**

**C. QoS is only for wireless networks; VoIP does not require QoS.**

**D. QoS eliminates all congestion with no configuration.**

**7. Which standard corresponds to 5 GHz only and can reach up to 3.5 Gbps?**

**A. 802.11ax**

**B. 802.11b**

**C. 802.11n**

**D. 802.11ac**

**8. How does IPv6 neighbor discovery function, and what are the roles of ICMPv6 messages in address resolution and duplicate address detection?**

**A. NDP uses ICMPv6 messages (Neighbor Solicitation and Neighbor Advertisement) to map IPv6 addresses to MACs; DAD uses NS/NA to detect duplicates; these mechanisms replace ARP for IPv6.**

**B. NDP uses IPv4 ARP packets; ICMPv6 is not used.**

**C. NDP uses Router Advertisements only.**

**D. IPv6 uses DNS for address resolution.**

**9. What is the original wireless security protocol?**

**A. WPA**

**B. WEP**

**C. WPA2**

**D. WPA3**

**10. 802.11r fast BSS transition is designed to...**

**A. Reduces handoff delay for real-time applications.**

**B. Increases channel width.**

**C. Enables RADIUS-based authentication.**

**D. Requires separate VLAN for roaming.**

# Answers

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

# Explanations

## 1. Which OSPF area type explicitly allows Type-7 LSAs to summarize external routes and does not carry Type-5 LSAs?

**A. Totally Stubby Area**

**B. Normal**

**C. NSSA**

**D. Stub**

**Not-So-Stubby Areas (NSSA) are designed to carry external routes in a controlled way inside the area. Inside an NSSA, external routes are advertised as Type-7 LSAs, which allows external networks to be imported without flooding the entire domain with Type-5 LSAs. Importantly, the NSSA itself does not carry Type-5 LSAs; those external routes are kept as Type-7 within the area. When the routes must reach the rest of the OSPF domain, the NSSA's ABR converts the Type-7 LSAs into Type-5 LSAs for distribution to non-NSSA areas. This combination—Type-7 LSAs for external routes inside the area, with no internal Type-5 LSAs—fits the described behavior. Other area types either do not support Type-7 LSAs in the area or rely on Type-5 LSAs inside the area, so NSSA is the correct fit.**

## 2. Which protocol uses AES-CCMP encryption?

**A. WEP**

**B. WPA**

**C. WPA2**

**D. WPA3**

**AES-CCMP encryption is what WPA2 uses. CCMP (Counter Mode with CBC-MMAC Protocol) is an AES-based method that provides both confidentiality and integrity for wireless data frames. WPA2 adopted AES-CCMP as the default, replacing the older WEP and the TKIP-based approach used by WPA. WEP relies on a weak RC4-based scheme with poor integrity, and WPA introduced TKIP to improve on WEP but it isn't as robust as AES-CCMP. WPA3 introduces newer, even stronger methods, but the encryption most commonly associated with WPA2 is AES-CCMP. So the protocol that uses AES-CCMP encryption is WPA2.**

## 3. What term describes a rogue wireless access point that broadcasts the same SSID as a legitimate network?

**A. Impostor AP**

**B. Eavesdropping AP**

**C. Honeypot AP**

**D. Evil Twin**

**An evil twin is a rogue wireless access point that copies the SSID of a legitimate network to trick devices into connecting. By mirroring the network name (and often mimicking security settings), users see what looks like the trusted network and join, enabling the attacker to intercept traffic, capture credentials, or redirect users to fake portals. The tactic hinges on the perceived authenticity of the SSID, making the connection appear legitimate even though it's controlled by an attacker. Other terms describe different ideas—for example, an impostor AP is a casual label, an eavesdropping AP would simply listen without impersonating a network name, and a honeypot AP is a trap used to study attackers rather than to deceive legitimate users. The defining feature here is the duped, trusted-looking SSID that lures clients to connect to a rogue device, hence the term evil twin.**

## 4. Which statement about CAM table aging is true?

**A. Entries never age.**

**B. Entries age out after a period of inactivity.**

**C. Aging increases CAM size automatically.**

**D. Aging causes frames to be dropped.**

**CAM table aging keeps the MAC address table lively by removing entries that aren't used for a while. A switch learns where devices are by inspecting source MAC addresses on frames and storing the MAC with the port it was seen on. To avoid wasting memory on devices that are gone or have moved, each learned entry has an aging timer. If that device stops sending frames and the timer runs out, the entry is deleted. When the device next transmits, the switch learns its MAC again—potentially on a different port if the device moved—so the table stays accurate and memory isn't tied up by stale entries. That's why the statement that entries age out after inactivity is the correct one. CAM size doesn't automatically increase due to aging, and aging itself doesn't drop frames; it only removes old entries so the switch can relearn as needed. Aging timers are typically a matter of minutes and are reset by activity from the associated MAC.**

## 5. Which statement describes the purpose of Quality of Service in networks?

**A. Prioritize critical traffic to improve performance**

**B. Encrypt all data by default**

**C. Map IP addresses to MAC addresses**

**D. Determine device IP assignments**

**Quality of Service is about controlling how network resources are shared so that time-sensitive traffic gets priority. By classifying different kinds of traffic, marking packets, and using queuing and shaping methods, a network can ensure that critical applications—like voice and video—experience lower latency and less jitter even when the link is congested. In other words, QoS is designed to improve the performance of important traffic by giving it preferential treatment. Encrypting all data by default is a security function, not QoS. Mapping IP addresses to MAC addresses is what ARP does, a process for local address resolution. Determining device IP assignments is related to IP addressing management or DHCP.**

## 6. What are the advantages and limitations of using QoS in networks, and how would you implement basic QoS for VoIP traffic?

**A. QoS always improves throughput and has no downsides.**

**B. QoS provides predictable performance but adds complexity and may reduce throughput if misconfigured; implement by classifying traffic, marking DSCP/CoS, creating queues, and prioritizing VoIP with strict or high priority.**

**C. QoS is only for wireless networks; VoIP does not require QoS.**

**D. QoS eliminates all congestion with no configuration.**

**QoS is about ensuring latency-sensitive traffic like VoIP gets timely treatment even when the network is busy. The best answer captures that QoS can provide predictable performance for voice, but it also adds complexity and can reduce throughput if misconfigured. Implementing basic VoIP QoS follows a simple pattern: identify VoIP traffic so it can be handled differently, mark those packets so devices understand their priority, and place VoIP into a high-priority queue. Practically, you classify traffic (using policies or ACLs) to separate VoIP from other traffic, mark it with a DSCP value (often Expedited Forwarding) or CoS, and configure network devices to trust those marks and route VoIP into a high-priority or low-latency queue (such as a strict priority or LLQ). You typically reserve or guarantee a minimum path for VoIP, and you monitor jitter, delay, and packet loss to tune the setup. Remember, QoS doesn't create extra bandwidth and can harm overall throughput if configured incorrectly, and it won't eliminate congestion on its own.**

## 7. Which standard corresponds to 5 GHz only and can reach up to 3.5 Gbps?

**A. 802.11ax**

**B. 802.11b**

**C. 802.11n**

**D. 802.11ac**

**This question tests knowing which Wi-Fi standard uses only the 5 GHz band and can deliver around 3.5 Gbps. 802.11ac fits this description because it operates exclusively in the 5 GHz spectrum (unlike some earlier standards that used 2.4 GHz as well) and achieves high throughput through wider channel bonding and advanced modulation. Specifically, it can use channels up to 160 MHz and 256-QAM with MU-MIMO, giving a theoretical maximum around 3.46 Gbps (often rounded to 3.5 Gbps) under ideal conditions. In contrast, 802.11b runs at 2.4 GHz with very low speeds; 802.11n can operate on both 2.4 and 5 GHz with lower maximums; and 802.11ax, while faster and more efficient, also uses 2.4 GHz and now 6 GHz in Wi-Fi 6E, so it isn't restricted to 5 GHz only.**

## 8. How does IPv6 neighbor discovery function, and what are the roles of ICMPv6 messages in address resolution and duplicate address detection?

**A. NDP uses ICMPv6 messages (Neighbor Solicitation and Neighbor Advertisement) to map IPv6 addresses to MACs; DAD uses NS/NA to detect duplicates; these mechanisms replace ARP for IPv6.**

**B. NDP uses IPv4 ARP packets; ICMPv6 is not used.**

**C. NDP uses Router Advertisements only.**

**D. IPv6 uses DNS for address resolution.**

**IPv6 uses ICMPv6-based Neighbor Discovery to handle how devices learn about each other on the same link and how they map addresses to hardware addresses. When a device needs to contact another host on the local link, it sends a Neighbor Solicitation to the target's solicited-node multicast address asking for the target's MAC address. The owner of that IPv6 address responds with a Neighbor Advertisement that includes its link-layer address, allowing the requester to fill its neighbor cache and communicate at layer 2 directly. This NS/NA exchange replaces the need for ARP in IPv6, since ICMPv6 handles the address resolution process. For duplicate address detection, a host that is configuring a new IPv6 address performs a similar NS/NA exchange to its own tentative address. It sends a Neighbor Solicitation to the solicited-node multicast address for that tentative address with an unspecified source address. If another device already uses that address, it will reply with a Neighbor Advertisement, signaling a conflict. If no conflicting response is received, the address is considered unique and can be used. Other options don't fit because IPv6 address resolution and duplicate address detection rely on ICMPv6-based Neighbor Discovery, not IPv4 ARP, not Router Advertisements alone, and not DNS for address resolution.**

## 9. What is the original wireless security protocol?

**A. WPA**

**B. WEP**

**C. WPA2**

**D. WPA3**

**WEP was the first security protocol for Wi-Fi, defined for the original 802.11 standard. It was designed to provide confidentiality similar to wired networks but relied on RC4 encryption with a short, 24-bit initialization vector that is sent in the clear. This combination allows IVs to repeat and be reused, making the key easy to recover with relatively little data. The early 40- or 64-bit keys also offered limited protection, and the integrity check (CRC) isn't robust against active tampering. These weaknesses meant WEP could be cracked with basic tools, so subsequent standards were developed to fix the flaws, leading to WPA, then WPA2, and later WPA3.**

## 10. 802.11r fast BSS transition is designed to...

**A. Reduces handoff delay for real-time applications.**

**B. Increases channel width.**

**C. Enables RADIUS-based authentication.**

**D. Requires separate VLAN for roaming.**

**Reducing the handoff delay when a client roams from one AP to another is what 802.11r fast BSS transition is designed to achieve. It enables faster re-authentication by allowing PMK caching and pre-auth between APs, so the new AP can quickly authenticate the client without going through the full EAP/RADIUS exchange. This minimizes disruption for time-sensitive traffic, making roaming nearly seamless for real-time applications. The other options don't capture this purpose: increasing channel width affects throughput, not roaming speed; RADIUS-based authentication is a general mechanism and not specific to fast roaming; using a separate VLAN for roaming is a deployment detail, not the function of 802.11r.**

# 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://netimproutingswitchingwirelessprot.examzify.com**

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