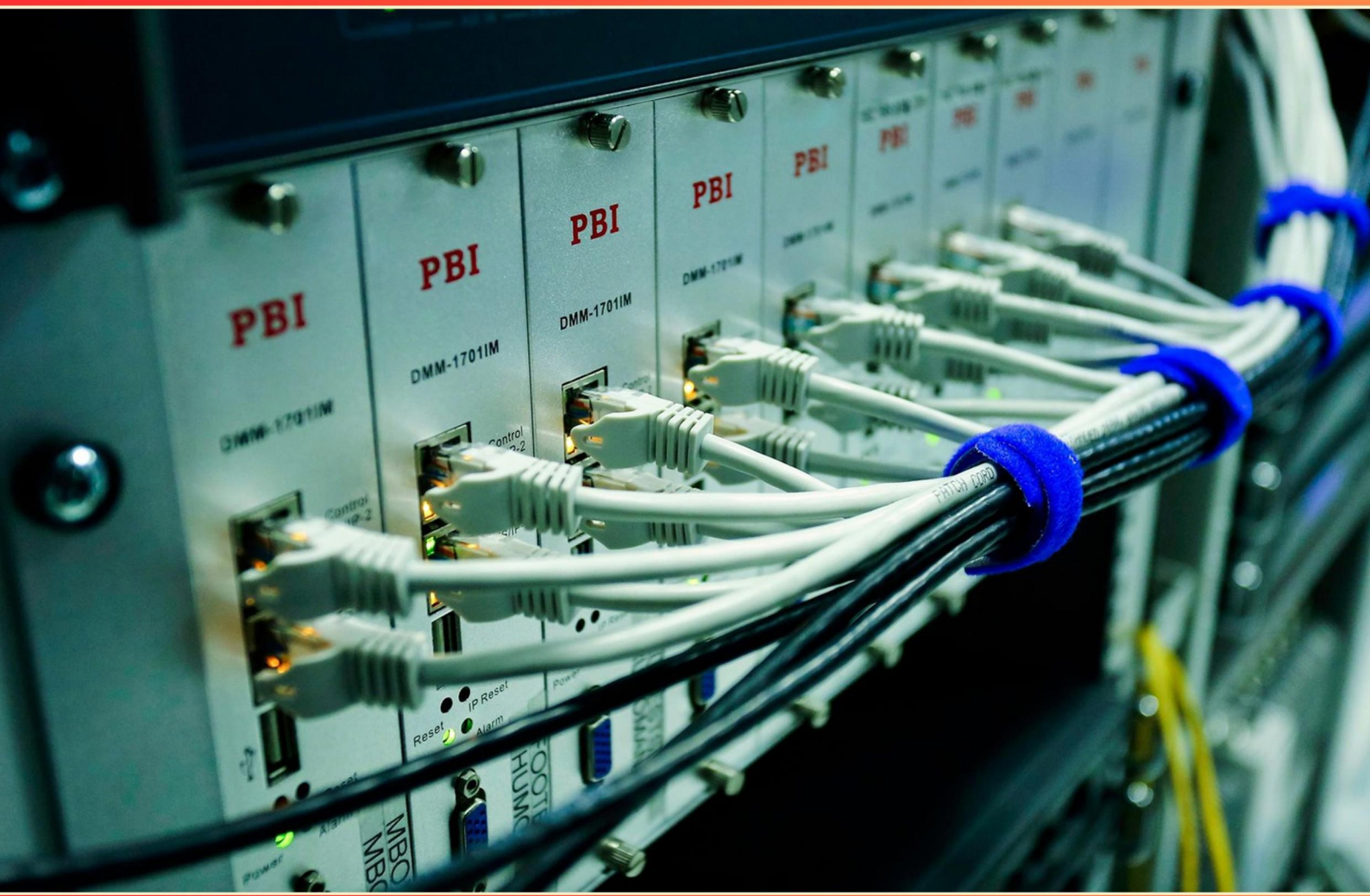
CCNP SOFTWARE-DEFINED WIDE AREA NETWORK (SD-WAN) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://ccnpsdwan.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. **Which component authenticates WAN Edge devices before allowing them into the overlay fabric?**

   A. vManage

   B. vBond

   C. vSmart

   D. Cisco ISE

2. **How does a Cisco SD-WAN device bootstrap using vBond during first-time enrollment?**

   A. Device contacts vBond to obtain the address of vSmart/vManage and a service URL, gets authenticated, then enrolls with vManage using certificates.

   B. Device directly connects to vSmart and downloads the configuration from vManage without authentication.

   C. Device boots from an embedded certificate and skips vBond; enrolls with vManage using pre-shared key.

   D. Device uses DNS to locate vManage and enrolls with vBond after obtaining the certificate.

3. **Which Cisco SD-WAN feature segments traffic into isolated VPNs across the overlay fabric?**

   A. Service chaining

   B. VPN segmentation

   C. BFD echo

   D. OMP reflection

4. **What is OMP used for in SD-WAN?**

   A. STP calculation

   B. Route and policy exchange in SD-WAN

   C. DHCP relay

   D. NAT translation

5. **Which of the following is a typical failure mode when a vSmart or vBond becomes unavailable?**

   A. OMP updates stop

   B. Loss of control-plane signaling

   C. QoS policy misalignment

   D. Tunnels reconfigure normally

6. During initial WAN Edge onboarding, what is the primary role of the vBond orchestrator?

A. Distributes routing policies

B. Performs data-plane encryption only

C. Authenticates devices and facilitates secure control connections

D. Acts as a DNS resolver

7. Which policy type directly influences traffic forwarding behavior on WAN Edge routers?

A. Centralized data policy

B. Localized AAA policy

C. STP filtering policy

D. CAPWAP discovery policy

8. Which Cisco SD-WAN component handles centralized policy processing?

A. vSmart

B. vManage

C. WAN Edge

D. vBond

9. Which OMP route type advertises transport locators in Cisco SD-WAN?

A. Service route

B. TLOC route

C. VPN route

D. Overlay route

10. How is TLS handshake and certificate trust managed across many SD-WAN devices?

A. TLS handshake negotiates the lowest common version and can use self-signed certificates.

B. TLS handshake negotiates the highest supported version, uses certificates issued by a trusted CA, validates certificate chains, and handles revocation if needed.

C. TLS handshake is not used in SD-WAN.

D. Each device uses a single certificate shared across all devices.

Answers

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

Explanations

1. Which component authenticates WAN Edge devices before allowing them into the overlay fabric?

A. vManage

B. vBond

C. vSmart

D. Cisco ISE

Authenticating WAN Edge devices before they join the overlay fabric is handled by the vBond Orchestrator. It sits at the edge of the control plane as the first contact point for a new edge device, validating its identity using certificates and the policy defined in vManage. Once vBond approves the device, it tells the edge which vSmart controllers to connect to and provides the necessary reachability information so secure control-plane connections can be established and the edge can join the overlay. This bootstrap role also helps with NAT traversal if needed. vManage is for centralized provisioning and management, not the initial authentication of edges. vSmart runs the overlay control plane after the edge has joined. Cisco ISE is an external security product and not used to bootstrap SD-WAN overlay authentication.

2. How does a Cisco SD-WAN device bootstrap using vBond during first-time enrollment?

A. Device contacts vBond to obtain the address of vSmart/vManage and a service URL, gets authenticated, then enrolls with vManage using certificates.

B. Device directly connects to vSmart and downloads the configuration from vManage without authentication.

C. Device boots from an embedded certificate and skips vBond; enrolls with vManage using pre-shared key.

D. Device uses DNS to locate vManage and enrolls with vBond after obtaining the certificate.

The flow being tested is how a Cisco SD-WAN edge securely bootstraps using vBond to discover and enroll with the control plane. On first boot, the device uses its bootstrap certificate to contact vBond. vBond authenticates the device and then provides the addresses of the vSmart and vManage controllers along with a service URL. With those endpoints, the device establishes a TLS session with vManage and enrolls there, using its certificate for mutual authentication. This sequence—reach vBond, get vSmart/vManage addresses and service URL, authenticate, then enroll with vManage using certificates—is what ensures a secure, authenticated first-time enrollment. Options that skip vBond, connect directly to vSmart, or rely on a pre-shared key or DNS-only discovery don't reflect this secure bootstrap flow.

3. Which Cisco SD-WAN feature segments traffic into isolated VPNs across the overlay fabric?

A. Service chaining

B. VPN segmentation

C. BFD echo

D. OMP reflection

The main idea this question tests is how traffic is kept separate in a Cisco SD-WAN environment. VPN segmentation means creating separate virtual routing domains (VRFs) for different traffic streams, tenants, or applications. Each VPN has its own routing table, security policies, QoS, and service settings, so traffic assigned to one VPN remains isolated from traffic in another—even though all use the same physical underlay. This allows multiple customers or apps to share the same network without interference or address conflicts because routes and policies live in distinct VPN contexts. In Cisco SD-WAN, VPNs form the overlay segments, so isolating traffic into different VPNs across the fabric is how isolation is achieved. The other options address different functions: service chaining is about routing traffic through a sequence of services, BFD echo is for quick liveness checks of links, and OMP reflection relates to route distribution mechanics, not segmentation into isolated VPNs.

4. What is OMP used for in SD-WAN?

A. STP calculation

B. Route and policy exchange in SD-WAN

C. DHCP relay

D. NAT translation

In SD-WAN, the Overlay Management Protocol is the control-plane channel that carries routing information, VPN reachability, and policy data across the SD-WAN overlay. It enables vEdges, vSmart controllers, and other components to exchange routes and the associated policies that govern how traffic should be steered between sites. This is what makes the overlay aware of which remote sites are reachable, through which transports, and what rules to apply for traffic between VPNs. This isn't about Layer 2 STP calculations, DHCP relay, or NAT translation—the functions those options describe happen at different layers or devices. OMP's purpose is to synchronize the overlay by distributing routes, VPN memberships, and policy configurations so traffic can be securely and efficiently routed across the WAN.

5. Which of the following is a typical failure mode when a vSmart or vBond becomes unavailable?

A. OMP updates stop

B. Loss of control-plane signaling

C. QoS policy misalignment

D. Tunnels reconfigure normally

In this SD-WAN setup, vSmart is the hub for the control plane and vBond handles onboarding and reachability. They drive the overlay by distributing policies and routing information to the edge devices. If either component becomes unavailable, the overlay loses its control-plane signaling. Without those control messages, edge devices stop receiving policy and route updates, so the fabric cannot adapt or reconfigure in response to changes. Existing tunnels may keep passing traffic, but the dynamic management and coordination that keeps the network aligned fail. That's why loss of control-plane signaling best describes the typical failure mode when vSmart or vBond is down.

6. During initial WAN Edge onboarding, what is the primary role of the vBond orchestrator?

A. Distributes routing policies

B. Performs data-plane encryption only

C. Authenticates devices and facilitates secure control connections

D. Acts as a DNS resolver

The vBond orchestrator is the authentication and control-plane rendezvous point for a new WAN Edge. Its job is to verify the edge's identity (using certificates or tokens) and help the edge discover and establish secure control-plane connections to the vSmart controllers, so the device can join the SD-WAN fabric. This bootstrapping role is distinct from policy distribution (that's handled by vSmart) and from data-plane encryption itself, and it isn't used as a DNS resolver. By authenticating devices and facilitating the initial secure control connections, vBond ensures only trusted Edges become part of the network and can communicate with the control-plane components.

7. Which policy type directly influences traffic forwarding behavior on WAN Edge routers?

A. Centralized data policy

B. Localized AAA policy

C. STP filtering policy

D. CAPWAP discovery policy

This item tests how traffic forwarding on WAN Edge routers is governed by centralized data policies. A centralized data policy defines the rules that determine how data-plane traffic is handled across the WAN—how applications are identified, which paths are chosen when multiple links exist, and how traffic is shaped, marked, or steered. By pushing these rules from a central controller to the edge devices, forwarding decisions become consistent and dynamic, enabling optimal path selection, fast failover, and policy-compliant handling across sites. The other policy types don't directly shape how traffic is forwarded: an AAA policy governs who can access devices and what they can do, not forwarding behavior; an STP filtering policy affects layer-2 loop prevention and frame handling; and a CAPWAP discovery policy relates to wireless tunnel setup and controller association, not general WAN edge forwarding.

8. Which Cisco SD-WAN component handles centralized policy processing?

A. vSmart

B. vManage

C. WAN Edge

D. vBond

Centralized policy processing is handled by the vSmart controller. It serves as the overlay's control plane, receiving policy definitions from the management plane and distributing them to the WAN Edge devices. This setup ensures consistent routing decisions, traffic engineering, QoS, and security policies across the entire SD-WAN fabric. The WAN Edge devices enforce the policies locally, while vBond handles onboarding and initial authentication, and vManage is used to design and push configurations but does not perform the policy decision-making itself.

9. Which OMP route type advertises transport locators in Cisco SD-WAN?

A. Service route

B. TLOC route

C. VPN route

D. Overlay route

In Cisco SD-WAN, the route type that carries the underlay connection details—the transport locators—is the TLOC route. TLOC routes advertise the transport locators, which are the IP addresses (underlay endpoints) of a site's edge, along with attributes like the transport color (types of links such as MPLS, Internet, or 4G) and encapsulation. This information lets other devices in the fabric know how to reach that site over the chosen transports and enables the SD-WAN to build and optimize the overlay path across multiple underlay links. VPN routes carry the actual customer networks inside a VPN, not the underlay endpoints. Overlay routes pertain to destinations learned across the fabric, not the underlay reachability. Service routes relate to services rather than transport endpoints.

10. How is TLS handshake and certificate trust managed across many SD-WAN devices?

A. TLS handshake negotiates the lowest common version and can use self-signed certificates.

B. TLS handshake negotiates the highest supported version, uses certificates issued by a trusted CA, validates certificate chains, and handles revocation if needed.

C. TLS handshake is not used in SD-WAN.

D. Each device uses a single certificate shared across all devices.

TLS handshake in SD-WAN establishes a secure, trusted channel by negotiating the highest TLS version both ends support, authenticating identities with certificates issued by trusted authorities, and validating the certificate chain along with revocation status. In practice, devices present certificates signed by a CA, the peer verifies the chain up to a trusted root, checks that the certificate is still valid, and performs revocation checks (via OCSP or CRLs) if needed. This combination provides mutual authentication and a fresh, encrypted session key for secure communication across many devices. This scale matters: using CA-issued, unique certificates per device lets you manage trust centrally and revoke or rotate credentials for a single device without affecting others. Relying on a single shared certificate or using self-signed certs would complicate trust management and weaken security across a large fleet. The approach described ensures robust, scalable trust across all SD-WAN devices.

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://ccnpsdwan.examzify.com

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