JNCIS – ENTERPRISE ROUTING AND SWITCHING (JNCIS-ENT) PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://jncisent.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 VLAN ID value is associated by default with the default VLAN on EX Series switches?**

   A. 0

   B. 1

   C. 100

   D. 255

2. **What happens when a Junos firewall filter permits the initial connection?**

   A. It tracks every packet individually.

   B. It automatically permits bidirectional communications.

   C. It requires additional configuration for each connection.

   D. It stops processing once the initial connection is established.

3. **Which three statements accurately describe IP source guard?**

   A. IP source guard checks the IP/MAC address of packets received against entries stored in the DHCP snooping database.

   B. Packets with a valid IP address and MAC address are always accepted.

   C. IP source guard can be used with any type of interface regardless of configuration.

   D. IP source guard can only be configured on trunk interfaces.

4. **In VRRP, what factor does not contribute to the selection of the master router?**

   A. The IP address of the router

   B. The configuration of the no-preempt option

   C. The router's ability to respond to ARP requests

   D. The priority value in the configuration

5. **Which two OSPF LSA types can be used to advertise routes between areas?**

   A. A. router

   B. B. network

   C. C. external

   D. D. summary

6. On which VLAN interface would an IP address typically be configured for a routed VLAN interface?

A. ge-0/0/20.100

B. rvi.100

C. vlan.100

D. ge-0/0/1

7. Which protocol is considered an Interior Gateway Protocol (IGP)?

A. LACP

B. STP

C. OSPF

D. PAGP

8. What is the result of dynamic VLAN tagging on a switch port?

A. The switch learns all VLAN IDs instantly.

B. The switch dynamically associates VLANs based on traffic.

C. The switch can only support static VLAN associations.

D. The switch prioritizes one VLAN over another based on traffic type.

9. Which statement regarding internal BGP sessions is true?

A. Routers advertise all BGP-learned routes to all internal BGP neighbors.

B. The TTL of BGP control packets is set to 255.

C. Peering sessions only use physical interface IP addresses.

D. Plain text authentication can be used.

10. What is the default IP time-to-live (TTL) value for an EBGP session?

A. 1

B. 63

C. 128

D. 255

Answers

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

Explanations

1. What VLAN ID value is associated by default with the default VLAN on EX Series switches?

A. 0

B. 1

C. 100

D. 255

The default VLAN on EX Series switches is associated with the VLAN ID value of 1. This is a standard configuration found in most VLAN-capable networking devices, not just limited to Juniper EX Series switches. VLAN 1 is commonly used as the default VLAN for management and default traffic, making it essential for initial switch configuration and communication within the network. In practice, when you connect a device to a switch port and do not configure a specific VLAN, it will automatically belong to VLAN 1, unless the switch is specifically configured to place untagged traffic into a different VLAN. This default behavior facilitates ease of setup for basic networking requirements. The other values provided do not represent the default VLAN ID for the EX Series switches, as they typically denote reserved or specific-purpose VLANs. For instance, VLAN ID 0 is typically used to indicate that the frame does not have a VLAN tag, while numbers such as 100 and 255 are commonly used for specific applications or custom VLAN configurations, but they are not the default settings for outgoing and incoming traffic on a new switch.

2. What happens when a Junos firewall filter permits the initial connection?

A. It tracks every packet individually.

B. It automatically permits bidirectional communications.

C. It requires additional configuration for each connection.

D. It stops processing once the initial connection is established.

When a Junos firewall filter permits the initial connection, it automatically permits bidirectional communications. This behavior is a result of the stateful processing capabilities of the firewall. When a new session is established and the initial packet is permitted by the filter, the firewall maintains a session state for that connection. As a result, once the initial connection is allowed, the subsequent packets belonging to that session, whether inbound or outbound, are automatically permitted without requiring additional checks through the firewall filters. This means that the stateful firewall can track the connection and ensure that traffic for that session is allowed in both directions, making network communication more efficient and manageable. In contrast, options that suggest tracking every packet individually or requiring additional configuration for each connection do not align with how stateful firewalls operate, as they utilize session states to allow seamless communication once a connection is established. The notion that processing stops once the initial connection is established is also misleading, as the firewall continues to manage the session while it is active.

3. Which three statements accurately describe IP source guard?

A. IP source guard checks the IP/MAC address of packets received against entries stored in the DHCP snooping database.

B. Packets with a valid IP address and MAC address are always accepted.

C. IP source guard can be used with any type of interface regardless of configuration.

D. IP source guard can only be configured on trunk interfaces.

IP source guard is a security feature designed to prevent IP address spoofing by ensuring that only valid IP and MAC address pairs are allowed to send traffic from a specific port. The first statement accurately describes the function of IP source guard, as it relies on the DHCP snooping database. This database contains bindings of MAC addresses to IP addresses that were dynamically assigned to devices, allowing IP source guard to verify that packets received on an interface match the expected IP and MAC addresses. When a packet arrives, IP source guard checks its source IP address and corresponding MAC address against the entries in the DHCP snooping database. If they match, the packet is considered valid and is forwarded; if not, it is dropped. This mechanism is vital for protecting the network from unauthorized access and mitigating certain types of attacks, such as man-in-the-middle attacks. The remaining statements do not accurately reflect the capabilities of IP source guard. For instance, valid pairs are not always accepted if they are not in the DHCP snooping database. Additionally, IP source guard can be configured on access interfaces—it's not limited to trunk interfaces—making it a versatile security feature across different interface types.

4. In VRRP, what factor does not contribute to the selection of the master router?

A. The IP address of the router

B. The configuration of the no-preempt option

C. The router's ability to respond to ARP requests

D. The priority value in the configuration

In VRRP (Virtual Router Redundancy Protocol), the selection of the master router is determined by specific criteria, and among these, the ability to respond to ARP requests does not play a role in this selection process. Instead, the factors that influence the master router election include the priority value set in the configuration, the presence of the no-preempt option, and the IP address of the router. The priority value is a key determining factor; routers configured with a higher priority will take precedence in the election process. If there are routers with the same priority, the one with the numerically highest IP address becomes the master. The no-preempt option affects whether a higher-priority router can reclaim the master role once it comes back online; without it, a router with a higher priority will take over if it becomes available. Responding to ARP requests is related to the operation of the protocol but is not a factor in determining which router becomes the master. The selection and election process relies on the pre-defined configurations and priorities rather than the operational responsiveness of the routers in terms of ARP.

5. Which two OSPF LSA types can be used to advertise routes between areas?

A. A. router

B. B. network

C. C. external

D. D. summary

Correctly identifying the LSA types used to advertise routes between OSPF areas involves an understanding of how OSPF (Open Shortest Path First) operates across multi-area networks. OSPF uses Link State Advertisements (LSAs) to exchange routing information, with different types serving specific purposes. External type LSAs, which are also known as Type 5 LSAs, are employed when routes from outside the OSPF routing domain need to be advertised into OSPF. These LSAs allow OSPF routers to learn about external routes, typically originating from other routing protocols, and thus support inter-area routing when external networks are involved. Summary type LSAs, identified as Type 3 LSAs, are used to summarize routes between OSPF areas. They're generated by Area Border Routers (ABRs) and help to minimize the amount of routing information that needs to be exchanged between areas. By summarizing routes, OSPF can manage larger networks more efficiently, reducing the routing table size in non-backbone areas and enhancing scalability. Both summary and external LSAs play vital roles in the functioning of OSPF in multi-area environments, facilitating the exchange of routing information between areas effectively.

6. On which VLAN interface would an IP address typically be configured for a routed VLAN interface?

A. ge-0/0/20.100

B. rvi.100

C. vlan.100

D. ge-0/0/1

A routed VLAN interface is commonly configured on a VLAN interface, which is designated primarily for Layer 3 IP addressing. In Juniper Networks devices, these VLAN interfaces are identified as 'vlan.x' where 'x' corresponds to the VLAN ID. Therefore, configuring an IP address on a VLAN interface allows the router to perform routing functions for that specific VLAN. In this context, the option indicating a VLAN interface, using the format 'vlan.100', reflects the standard convention in which IP addressing for a routed VLAN occurs. This interface acts as a gateway for devices within that VLAN, allowing them to communicate with other VLANs by routing packets through this interface. Other options represent different interface types or structures which do not serve the same purpose as a routed VLAN interface. For instance, ge-0/0/20.100 suggests a sub-interface of an Ethernet interface, which is suitable for 802.1Q encapsulated traffic but not specifically for routing at the VLAN level. The rvi.100 format refers to a routing virtual interface, which is used in other architectures, and the ge-0/0/1 represents a physical Ethernet interface without specific VLAN association. None of these appropriately signifies a routed VLAN interface where an IP address is

7. Which protocol is considered an Interior Gateway Protocol (IGP)?

A. LACP

B. STP

C. OSPF

D. PAGP

The protocol considered an Interior Gateway Protocol (IGP) is OSPF. OSPF, which stands for Open Shortest Path First, is designed specifically for routing within a single autonomous system or a local area network. It operates by using a link-state routing algorithm, allowing routers within the same area to share information about the network topology efficiently. OSPF provides several key advantages, including fast convergence, support for large networks, and the ability to segment networks using areas, which enhances scalability and management. Additionally, it is widely used due to its open standards nature, allowing interoperability between different vendors' equipment. In contrast, the other protocols listed serve different purposes. LACP (Link Aggregation Control Protocol) is used for bundling multiple Ethernet links into a single logical link for greater bandwidth and redundancy. STP (Spanning Tree Protocol) is primarily a protocol to prevent loops in Ethernet networks by managing the active paths and blocking redundant paths. PAGP (Port Aggregation Protocol) is similar to LACP, used for dynamically managing Port Aggregation on Cisco devices. Understanding the roles and functionalities of these protocols helps clarify OSPF's unique position as an IGP, designed explicitly for managing internal routing within networks.

8. What is the result of dynamic VLAN tagging on a switch port?

A. The switch learns all VLAN IDs instantly.

B. The switch dynamically associates VLANs based on traffic.

C. The switch can only support static VLAN associations.

D. The switch prioritizes one VLAN over another based on traffic type.

Dynamic VLAN tagging on a switch port allows the switch to automatically associate VLANs based on the traffic it receives. This means that instead of manually configuring each port to be assigned to a specific VLAN, the switch can identify the appropriate VLAN based on various parameters, such as the source address of incoming traffic. This feature is particularly beneficial in environments where devices move frequently between different VLANs, as it helps streamline network management and reduces administration overhead. By using protocols such as VLAN Trunking Protocol (VTP) or through mechanisms like GVRP (GARP VLAN Registration Protocol), the switch is able to facilitate dynamic VLAN assignments. This enables the network to adapt to changing conditions automatically, promoting efficiency and scalability within the network infrastructure.

9. Which statement regarding internal BGP sessions is true?

A. Routers advertise all BGP-learned routes to all internal BGP neighbors.

B. The TTL of BGP control packets is set to 255.

C. Peering sessions only use physical interface IP addresses.

D. Plain text authentication can be used.

When discussing internal BGP (iBGP) sessions, it's important to understand the characteristics that define their operation. The statement regarding the Time to Live (TTL) of BGP control packets being set to 255 is true. In the context of BGP, the default configuration for the TTL of its control plane packets is indeed set to 255. This design choice allows for the BGP session to be established between routers that may not be directly connected; it essentially limits the scope of BGP control packet transmission to a single hop unless explicitly configured otherwise. When it comes to iBGP, routers typically only advertise routes to their iBGP peers that they have learned from other sources, but they must also adhere to the rule that iBGP peers must be fully meshed or utilize route reflectors to propagate routing information effectively. Therefore, the statement that routers advertise all BGP-learned routes to all internal BGP neighbors does not hold true in the traditional sense without additional configurations. Regarding the use of physical interface IP addresses, while it's common to use such addresses for iBGP peering, it is not a strict requirement; routers can be configured to use loopback addresses as well, which are often preferred for stability and

10. What is the default IP time-to-live (TTL) value for an EBGP session?

A. 1

B. 63

C. 128

D. 255

The default IP time-to-live (TTL) value for an EBGP session is 255. TTL is a field in the IP header that indicates how many hops a packet can traverse before it is discarded. In the case of EBGP (External Border Gateway Protocol), the TTL value is critical because EBGP sessions typically occur between routers that may not be directly connected. The higher the TTL value, the more hops a packet can make without being dropped. By default, EBGP uses a TTL of 255 to ensure that packets can travel across multiple networks. Values like 1, 63, and 128 are not standard defaults for EBGP, as they would limit the scope considerably, potentially dropping packets if they traverse more than the allowed hops. A TTL of 1 would only allow packets to be sent to directly connected neighbors, which contradicts the purpose of EBGP, as it is designed for external connections.

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://jncisent.examzify.com

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