JNCIA-Junos Voucher Assessment Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Copyright © 2025 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

SAMPLE

Questions

SAMPLE

1. What defines an "X" release of the Junos OS?

A. A major bug fix release

B. A special feature release

C. A security update

D. A minor patch release

2. Which two statements describe PFE functions?

A. The PFE implements rate limiting using policers.

B. The PFE stores a local copy of the layer 2 and layer 3 forwarding tables.

C. The PFE is responsible for data encryption during transmission.

D. The PFE requires manual configuration for every route.

3. What does a static route in Junos specify?

A. A predefined path for IP traffic to a certain destination.

B. Dynamic updating of routes based on changes.

C. A method for temporarily bypassing a routing policy.

D. A method for balancing loads between multiple links.

4. What happens if the TACACS+ server is available and rejects the user’s credentials in a Junos OS device?

A. The user is allowed access with limited privileges

B. The user is not allowed to access the device

C. The device will attempt to connect to another TACACS+ server

D. The local user database is always checked first

5. What are two default password requirements on Junos devices? (Choose two.)

A. Must include special characters

B. Must be at least six characters in length

C. Must be all numeric

D. Must use alphanumeric character classes

SAMPLE

6. What is the consequence of configuring the system authentication order with TACACS+ if the server is not available?

A. The user cannot access the device

B. The device will default to the local database

C. Access will be granted automatically

D. Access is limited until the server is back online

7. Which protocol is primarily used for dynamic routing in Junos devices?

A. Static Routing Protocol

B. Routing Information Protocol (RIP)

C. Open Shortest Path First (OSPF)

D. Internet Control Message Protocol (ICMP)

8. Which command allows for a specific number of lines to display in the operational mode of a Junos device?

A. set cli screen-length 50

B. set cli screen-length 40

C. set cli lines 40

D. set cli output 40

9. What occurs when ping packets are sent to the management interface address of the local router?

A. The ping packets are blocked.

B. The ping packets cause an error.

C. The ping packets are accepted.

D. The ping packets are forwarded to the default gateway.

10. In OSPF, what is the term for the routers that exchange routing information within the same area?

A. Designated Routers

B. Area Border Routers

C. Internal Routers

D. Backbone Routers

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What defines an "X" release of the Junos OS?

A. A major bug fix release

B. A special feature release

C. A security update

D. A minor patch release

An "X" release of the Junos OS is defined as a special feature release, which indicates that this particular version introduces new features or enhancements that were not present in previous versions. These releases are designed to provide additional functionality and improvements to the system, differentiating them from standard maintenance updates or security patches. By focusing on feature enhancements, "X" releases allow users to take advantage of the latest capabilities and optimizations offered by the Junos OS. In contrast, major bug fix releases and security updates are typically classified under different categories that do not emphasize new functionality, while minor patch releases are usually more about correcting issues or minor improvements without introducing significant new features.

2. Which two statements describe PFE functions?

A. The PFE implements rate limiting using policers.

B. The PFE stores a local copy of the layer 2 and layer 3 forwarding tables.

C. The PFE is responsible for data encryption during transmission.

D. The PFE requires manual configuration for every route.

The statement about the PFE implementing rate limiting using policers is accurate because the Packet Forwarding Engine (PFE) in Junos OS is responsible for the efficient handling of data packets. One of its key functions is to apply traffic management features, such as rate limiting through the use of policers. Policers allow for controlling the amount of bandwidth a particular class of traffic can consume, thus helping manage network resources effectively and ensuring that no single stream of data can overwhelm the network. In the context of network design and operation, this is essential for quality of service (QoS) strategies that prioritize or limit data flows based on specific criteria, which the PFE actively manages to maintain optimal network performance.

3. What does a static route in Junos specify?

A. A predefined path for IP traffic to a certain destination.

B. Dynamic updating of routes based on changes.

C. A method for temporarily bypassing a routing policy.

D. A method for balancing loads between multiple links.

A static route in Junos specifies a predefined path for IP traffic to a certain destination. This means that when configuring a static route, the network administrator manually sets the next-hop IP address or the exit interface for a specific destination subnet. The route remains consistent and does not change unless the administrator modifies it, unlike dynamic routes, which adjust automatically based on conditions in the network. Static routes are commonly used for situations where the route to a specific destination is known and will not change frequently. This can be beneficial in a static network environment or when connecting to specific external networks. They provide a clear, straightforward way to dictate how packets should flow toward a destination, ensuring that traffic is efficiently routed according to the administrator's specification.

SAMPLE

4. What happens if the TACACS+ server is available and rejects the user’s credentials in a Junos OS device?

A. The user is allowed access with limited privileges

B. The user is not allowed to access the device

C. The device will attempt to connect to another TACACS+ server

D. The local user database is always checked first

When a TACACS+ server is available and it rejects the user's credentials on a Junos OS device, the user is not allowed to access the device. This is because TACACS+ is designed to provide centralized access control, and if the server denies access based on authentication failure, it will prevent the user from logging in to the device entirely. In environments that utilize TACACS+, the default behavior is to strictly adhere to the authentication results provided by the TACACS+ server. If a user's credentials do not match those stored on the server, access is denied, ensuring that only authorized users can gain entry to the system. Other choices propose scenarios that do not apply in this situation. For instance, limited access would only occur if the server allowed some form of access based on roles or permissions, and attempting connections to another TACACS+ server happens only if specified in the configuration and only after the local database has been checked. In this case, since the focus is on a rejected user credential scenario, denial of access is the definitive outcome.

5. What are two default password requirements on Junos devices? (Choose two.)

A. Must include special characters

B. Must be at least six characters in length

C. Must be all numeric

D. Must use alphanumeric character classes

On Junos devices, one of the default password requirements is that the password must be at least six characters in length. This ensures a minimum level of complexity and security, as shorter passwords are generally easier to guess or crack. Setting a minimum length helps protect the device from unauthorized access by requiring users to create passwords that are more robust and challenging to compromise. Additionally, another requirement that aligns with best practices for creating secure passwords is that they must use alphanumeric character classes. This means that passwords should include both letters and numbers, which increases complexity and enhances the security of the password. By incorporating different types of characters, it becomes more difficult for attackers to guess the password, as they have to consider a larger set of possible combinations. In summary, a minimum length of six characters and the use of alphanumeric character classes are fundamental requirements that contribute to the security posture of Junos devices.

SAMPLE

6. What is the consequence of configuring the system authentication order with TACACS+ if the server is not available?

A. The user cannot access the device

B. The device will default to the local database

C. Access will be granted automatically

D. Access is limited until the server is back online

When the system authentication order includes TACACS+ and the server is unavailable, the configured behavior is to fall back to the local authentication database. This fallback mechanism is essential for ensuring that device access remains possible even when the primary authentication method (TACACS+) is not reachable. In many network environments, relying solely on a remote authentication method can pose risks, especially if that server experiences downtime. By allowing the device to revert to using the local database, users with valid credentials in the local store can still access the device, maintaining operational continuity. This design provides a safeguard for network devices, ensuring that administrators and users with local access privileges are not entirely locked out due to external server issues. Thus, the configuration of the authentication order is crucial in maintaining accessibility and control over network devices during server outages.

7. Which protocol is primarily used for dynamic routing in Junos devices?

A. Static Routing Protocol

B. Routing Information Protocol (RIP)

C. Open Shortest Path First (OSPF)

D. Internet Control Message Protocol (ICMP)

Open Shortest Path First (OSPF) is a widely-used dynamic routing protocol designed to facilitate the exchange of routing information between devices in a network. It operates on the principle of link-state routing and uses a link-state database to maintain an accurate and up-to-date view of the network topology. This allows OSPF to quickly converge and adapt to changes in the network, making it efficient for larger and more complex environments. Junos devices implement OSPF to enable dynamic routing, allowing routers to automatically discover the best paths for data transmission without requiring manual configuration of routing tables. OSPF supports different areas within a network, providing scalability and hierarchy, which is essential for managing large networks effectively. The protocol's ability to quickly recalculate routes in response to changes ensures that data can flow efficiently even as network conditions change. In contrast, static routing requires manual configuration and does not adapt to network changes. While Routing Information Protocol (RIP) is another dynamic routing protocol, it is less efficient and scalable than OSPF, particularly in larger networks. Internet Control Message Protocol (ICMP) serves a different purpose related to error reporting and diagnostics, such as informing hosts about unreachable destinations, rather than being a routing protocol. This makes OSPF

SAMPLE

8. Which command allows for a specific number of lines to display in the operational mode of a Junos device?

A. set cli screen-length 50

B. set cli screen-length 40

C. set cli lines 40

D. set cli output 40

The command that allows you to set the number of lines displayed in the operational mode of a Junos device is designed to help manage the output on the screen when viewing command results. By issuing the command "set cli screen-length 40," you are configuring the device to limit the displayed output to 40 lines at a time. This helps in making the output more manageable, especially for commands that produce a large amount of data. Setting the screen length to a specific number ensures that the output is neither too long to scroll through easily nor too short to miss important information. This feature is particularly useful when working in a terminal environment where excessive scrolling can hinder the ability to review the information efficiently. In this context, the number "40" is significant because it defines the exact limit of lines that will appear before further output is paused, allowing you to process the information in a controlled manner.

9. What occurs when ping packets are sent to the management interface address of the local router?

A. The ping packets are blocked.

B. The ping packets cause an error.

C. The ping packets are accepted.

D. The ping packets are forwarded to the default gateway.

When ping packets are sent to the management interface address of a local router, the packets are accepted. This is because management interfaces are specifically designed for management purposes, allowing network administrators to communicate with the device for configuration, monitoring, or troubleshooting tasks. The design of these interfaces ensures that they can respond to management protocols and ICMP echo requests, commonly used in ping operations. Thus, when a ping is directed to the management interface, the router processes these packets and generates responses appropriately, confirming its availability over the network. In contrast, other options, such as blocking the ping packets or causing an error, do not typically occur with management interfaces, as their primary function is to facilitate management communications. Forwarding the packets to the default gateway is also incorrect in this context because the management interface should handle the packets directly without needing to route them elsewhere.

SAMPLE

10. In OSPF, what is the term for the routers that exchange routing information within the same area?

A. Designated Routers

B. Area Border Routers

C. Internal Routers

D. Backbone Routers

In OSPF (Open Shortest Path First), the term for routers that exchange routing information within the same area is "Internal Routers." Internal routers are those that have all their interfaces within a single OSPF area. They participate in the OSPF protocol by exchanging LSAs (Link State Advertisements) with other routers in that area, which helps them build a consistent and accurate view of the network topology. Internal routers play a critical role in OSPF by ensuring that the routing information within a specific area is updated and propagated to maintain optimal routing paths. They contribute to the area's link-state database, which is utilized to calculate the OSPF routing table. In contrast, Designated Routers are responsible for reducing OSPF traffic in broadcast and non-broadcast multi-access networks by acting as a central point for exchanging routing information. Area Border Routers connect different OSPF areas and handle routing information between them. Backbone Routers are those that are part of the OSPF backbone area (Area 0), but they may not necessarily operate solely within a single area. This distinction is crucial for understanding how OSPF organizes routing within areas and across larger hierarchies.

SAMPLE