Juniper.JN0-106.v2026-11-04.q43

Exam Code:	JN0-106
Exam Name:	Junos, Associate (JNCIA-Junos)
Certification Provider:	Juniper
Free Question Number:	43
Version:	v2026-11-04
# of views:	102
# of Questions views:	431
https://www.freecram.net/torrent/Juniper.JN0-106.v2026-11-04.q43.html	

NEW QUESTION: 1
Which two statements about firewall filters are correct? (Choose two.)
A. Firewall filters are stateful.
B. Firewall filters can match Layer 4 parameters.
C. Firewall filters can match Layer 7 parameters.
D. Firewall filters are stateless.
Answer: (SHOW ANSWER)
In Junos OS, standard firewall filters operate as a primary security and traffic management tool within the forwarding plane. These filters are fundamentally stateless, meaning they evaluate each packet individually and in isolation without maintaining a session table or tracking the state of network connections. This stateless nature allows the Packet Forwarding Engine (PFE) to process filters at hardware speeds, ensuring minimal latency for transit traffic. This distinguishes them from the stateful security policies found on Junos security devices like the SRX Series, which track the entire lifecycle of a flow.
Furthermore, firewall filters are designed to inspect and match header information up to Layer 4 of the OSI model. This capability allows administrators to define terms based on parameters such as source and destination IP addresses (Layer 3) as well as TCP or UDP port numbers and protocol types (Layer 4). While they provide granular control over packet flow, they do not natively inspect Layer 7 application payloads, which is typically reserved for advanced services like Intrusion Detection and Prevention (IDP). By combining stateless execution with Layer 4 matching, Junos firewall filters provide an efficient method for implementing transit protection, rate limiting through policing, and protecting the local Routing Engine through loopback interface filtering. Reference: Routing Policy and Firewall Filters, Firewall Filter Framework.

NEW QUESTION: 2
You committed a new configuration on a Junos router, but users report connectivity issues. You must quickly restore the previous working configuration without manually editing the candidate configuration. Which command should you use to load the required configuration into the candidate configuration?
A. rollback 0
B. show | compare rollback
C. rollback 1
D. load override

Answer: (SHOW ANSWER)
In Junos OS, the configuration database is designed with a robust versioning system that facilitates rapid recovery from administrative errors. Every time a commit command is successfully executed, the system automatically archives the previous active configuration and assigns it a " rollback " index. The rollback command is used within configuration mode to revert the candidate configuration to a previously saved state.
The indices are zero-based, where rollback 0 represents the currently active configuration that was just committed. To restore the configuration that was functional immediately before the most recent, problematic commit, the administrator must use rollback 1. This command replaces the current candidate configuration with the contents of the last known working state. It is important to note that executing rollback 1 only populates the candidate buffer; to make this previous configuration active and restore connectivity, the administrator must subsequently issue the commit command. This mechanism is a cornerstone of Junos OS ' s commitment to high availability and operational resilience, allowing for nearly instantaneous restoration of services without the need for manual line-by-line configuration edits during a network outage.
Reference: Configuration Basics, Managing Configurations, Rollback configurations.

NEW QUESTION: 3
Which two traffic types are processed by a Routing Engine using Junos OS? (Choose two.)
A. traffic with CoS markings
B. transit traffic
C. routing updates
D. local management traffic
Answer: (SHOW ANSWER)
The Routing Engine (RE) in a Junos device serves as the centralized intelligence and management hub, primarily responsible for the control and management planes of the system. In this capacity, the RE is tasked with processing routing updates, such as OSPF Link State Advertisements (LSAs) or BGP Update messages.
These updates are vital for the RE to maintain the Routing Information Base (RIB), calculate the shortest paths, and subsequently populate the Forwarding Information Base (FIB) which is then pushed to the Packet Forwarding Engine (PFE).
Furthermore, the Routing Engine handles all local management traffic. This category encompasses administrative access through the Command Line Interface (CLI) via SSH or Telnet, SNMP queries from network management systems, and system logging processes. Because the RE runs the Junos OS kernel, it must directly interpret and respond to these management-level requests to ensure the device remains configurable and observable. Conversely, transit traffic-the data passing through the device from one ingress port to an egress port-is offloaded to the PFE to be handled at wire speed. While the PFE manages the heavy lifting of data forwarding and Class of Service (CoS) application, the RE remains focused on high-level protocol maintenance and system administration, ensuring that control plane stability is maintained even under heavy traffic loads. Reference: Junos OS Fundamentals, Control Plane Functions, Routing Engine Traffic.

NEW QUESTION: 4
Which two statements describe the result when you enter ? at the command-line prompt? (Choose two.)
A. It lists the available commands and options.
B. It lists tips for the help menu.
C. It displays help about a text string contained in a statement.
D. It displays summary information about the commands and options.
Answer: (SHOW ANSWER)
The Junos Command Line Interface (CLI) is designed with an intuitive, context-sensitive help system that assists users in navigating the command hierarchy. When an administrator enters a question mark (?) at the prompt, the CLI provides immediate feedback based on the current

location within the hierarchy. First, it lists all available commands and options that are valid at that specific point. This allows the user to see the breadth of possible next steps without needing to refer to external documentation.
Second, the ? character triggers the display of summary information for each of those commands and options.
This brief descriptive text provides a clinical overview of what each command achieves, helping the user select the appropriate tool for their task.
This " help-on-demand " feature is functional in both operational and configuration modes. It is important to distinguish this from the help command; while help (such as help topic or help reference) provides more exhaustive documentation and usage examples, the ? prompt is primarily a quick-reference tool for command completion and syntax discovery. This mechanism ensures that even complex configurations can be built accurately by exploring the available options and their summarized purposes directly within the terminal environment. Reference: User Interfaces, CLI Help Facilities, Command Discovery.

NEW QUESTION: 5
Which protocol provides secure remote CLI access to a Junos device?
A. FTP
B. SNMP
C. Telnet
D. SSH
Answer: (SHOW ANSWER)
Securing the management plane is a core requirement for any Junos OS deployment. Secure Shell (SSH) is the industry-standard protocol used to provide encrypted, authenticated remote access to the Junos Command Line Interface (CLI). Unlike Telnet, which transmits both administrative credentials and command data in cleartext, SSH utilizes public-key cryptography to establish a secure tunnel, protecting the session from eavesdropping, man-in-the-middle attacks, and unauthorized interception.
In Junos OS, SSH is typically enabled within the [edit system services] hierarchy. Once active, it allows administrators to perform operational and configuration tasks with the assurance that their management traffic remains confidential. Beyond simple terminal access, SSH serves as the transport mechanism for other secure management functions, such as the NETCONF XML management protocol and Secure Copy (SCP) for file transfers. For high-security environments, Junos supports advanced SSH features including key-based authentication, strong cipher suites, and multi-factor authentication integration. Disabling insecure protocols like Telnet and FTP in favor of SSH and SFTP/SCP is a foundational best practice for hardening the Routing Engine against external threats.
Reference: User Interfaces, Accessing the Junos CLI, System Services.

NEW QUESTION: 6
Which command is used to view real-time traffic statistics for all interfaces?
A. show interfaces extensive
B. monitor interface traffic
C. monitor traffic interface all
D. show interfaces statistics
Answer: (SHOW ANSWER)
In Junos OS, there is a distinct difference between show commands and monitor commands. While show commands provide a static snapshot of the current state of the device or its interfaces at the moment the command is executed, monitor commands provide dynamic, real-time updates.
To view live traffic statistics across all physical and logical interfaces, the correct command is monitor interface traffic.
When this command is executed, the CLI enters an interactive text-based interface (TUI) that displays a list of interfaces along with their input and output rates in bits per second (bps) and packets per second (pps). The display refreshes automatically (usually every few seconds),

allowing an administrator to observe traffic spikes or drops as they occur without manually re-running a command. This is an invaluable tool for troubleshooting congestion or verifying that traffic is flowing as expected after a configuration change.
Commands like show interfaces extensive provide significantly more detail-including error counters and physical layer parameters-but they are not real-time and require manual execution to update the statistics.
The monitor interface traffic command simplifies the view to focus specifically on throughput metrics across the entire device. Reference: Operational Monitoring and Maintenance, Interface Monitoring, Real-time Statistics.

NEW QUESTION: 7



The MX204 has 12 built-in ports. Referring to the exhibit, to which interface does the arrow point?
A. ##-0/2/7
B. ##-0/0/7
C. ##-0/1/7
D. ##-0/1/6
Answer: (SHOW ANSWER)
The Juniper MX204 is a fixed-configuration router that utilizes a specific hierarchical naming convention for its physical interfaces: type-fpc/pic/port. In the MX204 architecture, there is a single built-in Flexible PIC Concentrator (FPC), which is always designated as FPC 0 . This FPC is subdivided into two logical Physical Interface Cards (PICs): PIC 0 and PIC 1 .
As shown in the exhibit, PIC 0 contains four high-speed ports (labeled 0/0 through 0/3) that typically support 40GbE or 100GbE speeds. PIC 1 contains eight ports (labeled 1/0 through 1/7) designed for 1GbE or 10GbE connectivity. These ports are arranged in a stacked, 2×4 grid. The labeling system on the chassis indicates the port numbers for each column. In the fourth column of the PIC 1 block, the top port is identified as 1/6 and the bottom port as 1/7 .
The blue arrow in the exhibit points directly to the bottom-right interface in the PIC 1 section. Correlating this physical location with the chassis labels confirms that the port number is 7. When combined with the FPC and PIC identifiers, the full interface name is xe-0/1/7 (assuming a 10GbE transceiver is installed). Understanding this physical-to-logical mapping is essential for accurate cabling and configuration within the Junos OS, ensuring that administrators apply the correct logical unit and protocol settings to the intended physical hardware.
Reference: Junos OS Fundamentals, Interface Naming, MX204 Hardware Overview.

NEW QUESTION: 8
Exhibit:

Route	Next Hop
10.0.0.0/24	192.168.0.1
10.0.0.0/26	192.168.1.1
10.0.0.8/27	192.168.2.1
10.0.0.4/30	192.168.3.1

Referring to the exhibit, what is the next hop for IP address 10.0.0.9?

A. 192.168.2.1

B. 192.168.1.1

C. 192.168.3.1

D. 192.168.0.1

Answer: (SHOW ANSWER)

In Junos OS, the Packet Forwarding Engine (PFE) determines the next hop for a packet by performing a lookup in the forwarding table and identifying all valid matches for the destination IP address. When multiple routes encompass the same destination, the router strictly follows the Longest Prefix Match (LPM) rule to select the most specific entry.

For the destination address 10.0.0.9 , the following evaluation occurs based on the exhibit:

* 10.0.0.0/24 : This route matches, as the address falls within the 10.0.0.0-10.0.0.255 range.

* 10.0.0.0/26 : This route matches, as the address falls within the 10.0.0.0-10.0.0.63 range.

* 10.0.0.8/27 : This route matches, as the address falls within the 10.0.0.8-10.0.0.39 range.

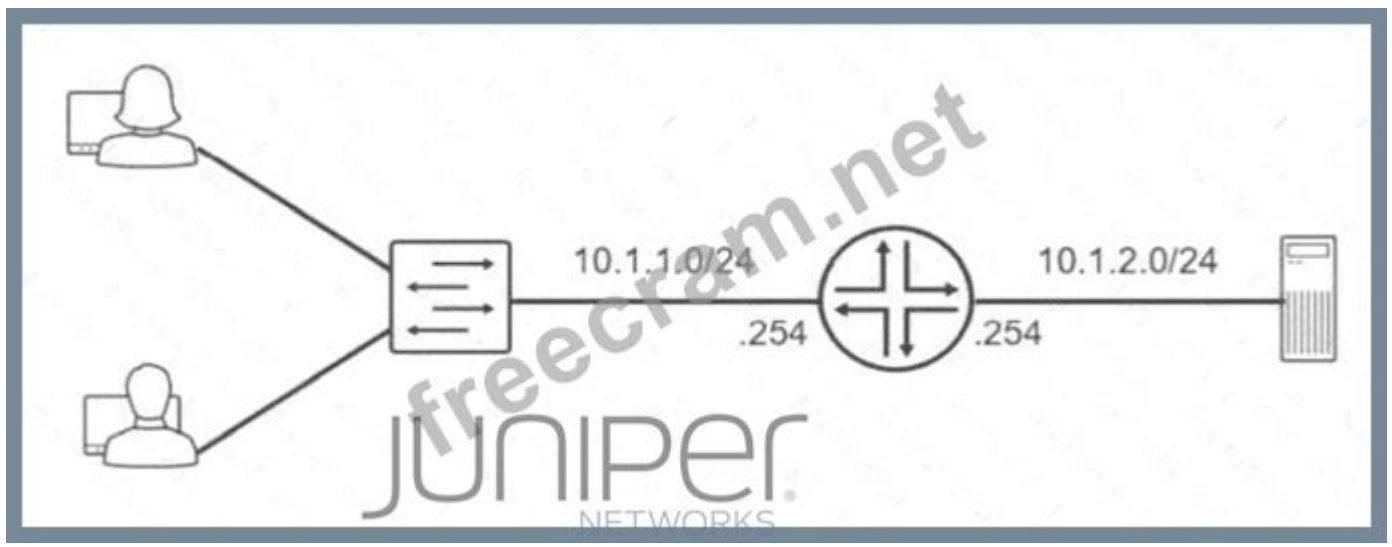
* 10.0.0.4/30 : This route does not match, as its range ends at 10.0.0.7.

Among the matching entries, the prefix lengths are /24, /26, and /27. The longest prefix match is /27 , as it specifies the most granular network segment. Because 10.0.0.8/27 is the most specific match for the destination 10.0.0.9 , the router selects its associated next hop, which is 192.168.2.1 . This deterministic behavior ensures that traffic follows the most precise path calculated by the routing protocols or defined by the administrator, overriding broader routes like the default or summary advertisements.

Reference: Routing Fundamentals, Longest Prefix Match, Forwarding Table Selection.

NEW QUESTION: 9

Exhibit:



freecram.net

Referring to the exhibit, which routing configuration is required for these two users to access the remote server?

A. Users and the server require a default gateway.

B. Trunk ports must be enabled on the switch.

C. Users must connect directly to the router.

D. A routing protocol must be enabled on the router.

Answer: (SHOW ANSWER)

The network topology illustrates two distinct IP subnets, 10.1.1.0/24 and 10.1.2.0/24 , separated by a Layer 3 router. For hosts on the first subnet to communicate with the server on the second subnet, an intermediary device must perform inter-subnet routing. The router acts as the exit point for each local segment, utilizing its interfaces assigned with the .254 host address as the logical path to external networks.

The fundamental requirement for this communication is the configuration of a default gateway on all end- nodes. When the users (on 10.1.1.0/24) attempt to send data to the server (on 10.1.2.0/24), their local TCP/IP stack recognizes the destination is not on the local wire. Without a defined default gateway, the hosts would simply drop the traffic as unroutable. By setting the default gateway to 10.1.1.254 for users and 10.1.2.254 for the server, the hosts are instructed to forward all off-net traffic to the router. The router then consults its routing table-which contains these directly connected routes-and forwards the packets to the appropriate egress interface. While VLAN tagging or routing protocols could exist in more complex environments, the primary necessity for basic reachability between these two specific segments is a correctly configured gateway on the terminal devices. Reference: Networking Fundamentals, IP Routing Basics, Default Gateway Configuration.

NEW QUESTION: 10

You asked a network engineer to configure a new logical interface on a Juniper router. The interface must use the fourth usable host address from the 172.16.40.128/29 subnet. Which IP address is correct in this scenario?

Freecram.net

A. 172.16.40.135

B. 172.16.40.132

C. 172.16.40.130

D. 172.16.40.131

Answer: (SHOW ANSWER)

In the Junos OS environment, precise IP addressing and subnet calculation are foundational for interface configuration. A /29 subnet mask (255.255.255.248) provides a total of 8 IP addresses. To identify the usable host range, we must first identify the network and broadcast addresses. For the subnet 172.16.40.128/29, the network address is 172.16.40.128. The broadcast address is the last address in the block, which is

172.16.40.135.
Following standard IPv4 conventions, the first and last addresses in a block are reserved for the network identity and the directed broadcast, respectively. This leaves 6 usable host addresses: 172.16.40.129 through
172.16.40.134. Counting sequentially from the beginning of the usable range: the first usable host is .129, the second is .130, the third is .131, and the fourth usable host is 172.16.40.132. Assigning this specific address ensures that the Packet Forwarding Engine can correctly route traffic within the intended segment. As a Senior Architect, it is critical to verify these boundaries when using the set interfaces unit 0 family inet address command to prevent address overlapping or the accidental assignment of reserved network/broadcast IDs.
Reference: Networking Fundamentals, IPv4 Addressing, CIDR Subnetting.

NEW QUESTION: 11
Which two statements describe rollback configuration behavior in Junos OS? (Choose two.)
A. Rollback configurations are applied automatically after a commit confirmed timeout.
B. Rollback 0 always refers to the factory default configuration.
C. Rollback files are stored automatically after each commit.
D. Up to 100 rollback configurations are maintained by default.
Answer: (SHOW ANSWER)
Junos OS incorporates a robust configuration versioning and recovery system designed to protect against configuration errors and human oversight. A key feature of this system is that rollback files are stored automatically by the device after each successful commit. These files represent a historical record of previous active configurations. By default, the system maintains a set number of these files, allowing an administrator to revert to a previous state (e.g., rollback 1) if the most recent changes result in unexpected network instability.
Another critical safety mechanism is the behavior associated with the commit confirmed command. If an administrator issues this command but fails to provide a subsequent confirmation within a designated timeframe (defaulting to 10 minutes), the system assumes a loss of management connectivity. Consequently, the rollback configurations are applied automatically after the commit confirmed timeout to restore the previous known-good state. This is an essential best practice for remote configuration management. It is important to note that rollback 0 refers to the currently active configuration, not the factory default, and that while Junos supports maintaining a large number of rollback files, the primary operational benefit lies in the automated storage and confirmation-based recovery processes that ensure the device remains reachable and stable. Reference: Configuration Basics, Rollback Configurations, Commit Confirmed Logic.

NEW QUESTION: 12
Which statement accurately describes the Junos OS CLI?
A. The operational mode CLI is used to make persistent changes.
B. Changes made in configuration mode immediately affect the active configuration.
C. The commit confirmed 5 command activates the candidate configuration and automatically reverts if not confirmed in 5 minutes.
D. The rollback 0 command restores the device to factory defaults.
Answer: (SHOW ANSWER)
The statement describing commit confirmed 5 is correct. In Junos OS, configuration changes are first made to a candidate configuration . They do not become the active operational configuration merely because they have been entered in configuration mode. A commit operation is required to validate and activate those changes.
The commit confirmed mechanism provides an important administrative safety feature. When the administrator enters:
commit confirmed 5

Junos OS activates the candidate configuration but requires confirmation within 5 minutes . If the configuration is not confirmed before the timer expires, Junos OS automatically rolls back to the previously committed configuration. Juniper explicitly documents that the optional number following commit confirmed specifies the confirmation period in minutes.
Option A is incorrect because operational mode is primarily used for monitoring, troubleshooting, maintenance, and operational commands rather than making persistent configuration changes. Option B is incorrect because configuration-mode edits remain candidate changes until committed. Option D is also incorrect: rollback 0 does not restore factory defaults . It loads the most recently committed configuration and effectively removes pending uncommitted modifications.
Study Guide Reference Topics: Configuration Basics - candidate versus active configuration, commit operations, confirmed commits, configuration rollback, and Junos CLI modes.

NEW QUESTION: 13
An administrator wants to set up a remote user authentication service for the many users that access a Juniper security device. In this scenario, what are two supported authentication protocols? (Choose two.)
A. RADIUS
B. TACACS+
C. SHA
D. IPsec
Answer: (SHOW ANSWER)
For managing high volumes of administrative users, Junos OS supports externalizing the authentication, authorization, and accounting (AAA) process. The two primary industry-standard protocols supported for this purpose are RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System Plus).
Using these protocols allows an architect to maintain a centralized user database on an external server (like Cisco ACS, FreeRADIUS, or Microsoft NPS) rather than configuring every individual user account locally on every Junos device. When a user attempts to log in via SSH or the console, the Junos device acts as a client, forwarding the credentials to the remote server. RADIUS is often preferred for its broad compatibility and efficiency, while TACACS+ is frequently chosen for its ability to separate authentication from authorization and its support for granular command-level accounting. SHA (Secure Hash Algorithm) is a cryptographic hash function used within these processes but is not an authentication protocol itself. Similarly, IPsec is a suite for securing IP communications (VPNs) and is unrelated to the administrative login AAA sequence.

NEW QUESTION: 14
You are configuring a new router and want to ensure that you can recover from future misconfigurations. In this scenario, what should you do after completing the initial configuration?
A. Update the firmware on the router.
B. Save the configuration as rollback 0.
C. Create a rescue configuration.
D. Enable automatic rollback after 10 minutes.
Answer: (SHOW ANSWER)
In the Junos OS architecture, maintaining a reliable recovery point is a critical post-installation task. While the system automatically archives previous configurations as " rollback " files every time a commit is performed, these files are transient and can eventually be rotated out of the default 50-file history as new changes are made. To ensure a permanent and reliable recovery state, a Senior Architect should manually create a rescue configuration .

The rescue configuration is a specifically designated file used to restore a device to a known-working state if it becomes unreachable or the configuration becomes corrupted. Unlike standard rollbacks, the rescue configuration is only created or updated when an administrator explicitly issues the operational mode command request system configuration rescue save. This ensures that even if several subsequent commits flush the desired initial state from the standard rollback archive, the " safe harbor " configuration remains intact on the storage media. This state can then be re-activated via the rollback rescue command in configuration mode followed by a commit. Setting a rescue configuration after the initial setup is a foundational best practice for disaster recovery and operational stability, providing a " last resort " configuration that is immune to the automated rotation of the commit history.
Reference: Operational Monitoring and Maintenance, Rescue Configuration and Recovery.

NEW QUESTION: 15
What are two fiber-optic connector types? (Choose two.)
A. LC
B. RJ-45
C. SC
D. BNC
Answer: (SHOW ANSWER)
Physical layer connectivity for Junos devices involves a variety of media types, with fiber-optic cabling being the standard for high-speed, long-distance, or high-density uplink requirements. Two of the most prevalent connector types used in these environments are the LC (Lucent Connector) and the SC (Subscriber Connector) .
The LC connector is a small-form-factor (SFF) connector that uses a 1.25 mm ferrule. Due to its compact size and " push-and-latch " mechanism, it is the primary connector type found on SFP, SFP+, and XFP transceivers used in Juniper EX, MX, and QFX series hardware. Its high-density design allows for more ports in a limited space on a line card or chassis. The SC connector , often referred to as a " square connector, " utilizes a larger 2.5 mm ferrule and a " push-pull " snapping mechanism. While it was highly common in older legacy hardware and fiber patch panels, it has largely been superseded by the LC in modern data center and enterprise switching environments.
In contrast, the RJ-45 is a standard copper Ethernet connector (typically used with Category 5e/6 cables), and the BNC (Bayonet Neill-Concelman) is a miniature quick connect/disconnect RF connector used for coaxial cable. As a Senior Architect, distinguishing between these physical interfaces is critical when specifying the correct Small Form-factor Pluggable (SFP) modules and patch cables required to bring a Junos interface into an operational up/up state.
Reference: Networking Fundamentals, Physical Layer and Media Types.

NEW QUESTION: 16
You are asked to subnet the broadcast domains but need to support 50 hosts. In this scenario, which subnet mask would satisfy this requirement?
A. /26
B. /27
C. /28
D. /29
Answer: (SHOW ANSWER)
Determining the appropriate subnet mask for a specific host requirement is a core task in designing Junos- based network infrastructures. The number of usable hosts in an IPv4 subnet is calculated using the formula

$2^n - 2$, where n represents the number of host bits remaining after the network prefix. In this scenario, the requirement is to support 50 hosts within a single broadcast domain.
Evaluating the options:
* A /29 mask provides 3 host bits ($2^3 - 2 = 6$ hosts), which is insufficient.
* A /28 mask provides 4 host bits ($2^4 - 2 = 14$ hosts), which is insufficient.
* A /27 mask provides 5 host bits ($2^5 - 2 = 30$ hosts), which still fails to meet the 50-host threshold.
* A /26 mask provides 6 host bits. Applying the formula: $2^6 - 2 = 64 - 2 = 62$ usable host addresses.
Since a /26 mask provides 62 usable addresses, it is the smallest standard subnet mask that fully satisfies the requirement of 50 hosts. Using a /26 mask allows for the 50 required hosts while providing a small buffer for future growth (12 additional addresses) without wasting the excessive address space associated with a /25 or
/24 mask. This efficient allocation of address space is a best practice for maintaining scalable and organized routing tables on Juniper devices.
Reference: Networking Fundamentals, IPv4 Subnetting, Host Requirements.

Valid JN0-106 Dumps shared by ExamDiscuss.com for Helping Passing JN0-106 Exam! ExamDiscuss.com now offer the **newest JN0-106 exam dumps**, the ExamDiscuss.com JN0-106 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com JN0-106 dumps with Test Engine here: https://www.examdiscuss.com/Juniper/exam/JN0-106/premium/ (**101** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 17
When multiple routes exist to the same destination IP address, which rule do routers use to select the next hop?
A. They choose the route with the longest prefix match.
B. They choose a route at random to balance paths.
C. They choose the route with the largest administrative distance.
D. They choose the route learned most recently.
Answer: (SHOW ANSWER)
The primary and most critical rule used by Junos OS (and routers in general) to determine the next hop for a specific packet is the Longest Prefix Match (LPM) algorithm. When the Routing Engine or Packet Forwarding Engine looks up a destination IP address in the routing or forwarding table, it may find several entries that technically encompass that address. The LPM rule dictates that the router must select the most specific route available-that is, the entry with the highest number of matching bits in its subnet mask (the longest prefix).
For example, if a router has a route for 10.1.1.0/24 and another for 10.1.1.0/28, a packet destined for 10.1.1.1 will always be forwarded according to the /28 route, as it is more specific. Longest prefix match takes precedence over all other selection criteria, including route preference (administrative distance) and metrics.
Preference and metrics are only evaluated when the router has multiple entries for the exact same prefix length (e.g., two different paths to 10.1.1.0/24). This logic ensures that traffic is guided along the most precise path defined in the network topology. Routers never choose paths at random or based on the most recent update as their primary selection mechanism, as doing so would result in non-deterministic and inefficient routing behavior. Reference: Routing Fundamentals, Routing Table and Forwarding Table Selection.

NEW QUESTION: 18
Which two statements are correct regarding Layer 2 network switches? (Choose two.)

A. Switches are susceptible to traffic loops.
B. Switches flood broadcast traffic.
C. Switches do not learn MAC addresses.
D. Switches create a single collision domain.
Answer: (SHOW ANSWER)
In the Junos OS architecture and general networking standards, Layer 2 switches are designed to increase network efficiency by segmenting collision domains. Unlike legacy hubs, a switch creates a separate collision domain for each of its physical ports. This micro-segmentation allows for full-duplex communication, effectively eliminating the possibility of collisions on individual links. However, while switches segment collision domains, they maintain a single broadcast domain by default.
When a switch receives a broadcast frame, such as an ARP request, it must ensure the frame reaches all possible destinations within the local segment. Consequently, the switch floods the broadcast traffic out of all ports except the one on which it was received. This flooding behavior, while necessary for protocol discovery, makes Layer 2 networks susceptible to traffic loops. If redundant physical paths exist between switches without a loop-prevention mechanism like the Spanning Tree Protocol (STP), broadcast frames can circulate endlessly, leading to a broadcast storm that consumes all available bandwidth and processor resources on the Routing Engine. Furthermore, switches are highly active learners; they populate their Media Access Control (MAC) tables by observing the source addresses of incoming frames to ensure that subsequent unicast traffic is precisely forwarded rather than flooded. Therefore, understanding the management of broadcast domains and the risks of loops is a core competency for any Junos Associate.
Reference: Networking Fundamentals, Collision and Broadcast Domains, Layer 2 Switching Operations.

NEW QUESTION: 19
Which command would compare the candidate configuration with the active configuration before committing the changes?
A. [edit]
user@router# show | compare
B. [edit]
user@router# rollback 0
C. user@router > show configuration | compare rollback 0
D. user@router > show configuration | compare
Answer: (SHOW ANSWER)
The Junos OS operates using a candidate configuration model, where changes are made in a temporary buffer before being applied to the running system. To ensure accuracy and prevent unintended network disruptions, it is a critical best practice to review the differences between the candidate buffer and the currently active configuration. The command show | compare executed from the [edit] hierarchy level is the primary tool for this task.
When this command is issued, the CLI performs a line-by-line comparison. The output uses a " diff " format:
lines prefixed with a plus sign (+) represent new statements added to the candidate configuration, while lines prefixed with a minus sign (-) indicate statements that have been removed. This visualization allows the architect to verify exactly what will change upon execution of the commit command. Unlike operational mode commands that only show the final state, show | compare highlights the delta, making it indispensable for auditing complex policy changes or interface reconfigurations. This step acts as a final manual validation gate, reducing the risk of syntax errors or logical misconfigurations entering the production environment.
Using this command is a fundamental skill for passing the JNCIA-Junos exam and for professional day-to-day operations.
Reference: Configuration Basics, Comparing Configurations, Candidate vs. Active.

NEW QUESTION: 20

Which two operational mode commands would you use to verify CPU and memory utilization on a Junos device? (Choose two.)

Freecram.net

A. show chassis routing-engine

B. show chassis environment

C. show system processes extensive

D. show system resource-monitor summary

Answer: (SHOW ANSWER)

In the Junos OS architecture, maintaining visibility into the health of the Routing Engine (RE) is paramount for ensuring control plane stability. The command show chassis routing-engine is the primary tool for a high- level hardware status overview. It provides critical telemetry regarding the RE ' s current CPU utilization (broken down by user, background, and kernel tasks), memory usage statistics, and uptime. This command is essential for identifying if the device ' s " brain " is under significant stress due to heavy protocol processing or management tasks.

For a more granular, process-specific analysis, the show system processes extensive command is utilized.

Similar to the ' top ' utility in Unix-based systems, it lists all active software daemons (such as rpd for routing, dcd for interfaces, and mgd for management) and ranks them by their real-time CPU and memory consumption. This allows an architect to pinpoint exactly which process might be causing a performance bottleneck. While show chassis environment focuses on physical hardware health like temperatures and fan speeds, and resource-monitor provides summary data, the combination of show chassis routing-engine and show system processes extensive offers the most comprehensive diagnostic view of the device ' s internal computational resources. Reference: Operational Monitoring and Maintenance, System Health Monitoring.

NEW QUESTION: 21

You manage a Junos device with 20 interfaces. Each interface requires the same description and MTU setting.

Which configuration approach would reduce repetitive commands and ensure consistency?

A. Use the wildcard delete command to remove duplicate settings.

B. Configure each interface individually.

C. Use a configuration group.

D. Use search and replace to apply settings across interfaces.

Answer: (SHOW ANSWER)

In the Junos OS architecture, configuration groups (defined under the [edit groups] hierarchy) provide a powerful mechanism for template-based management. This approach is specifically designed to handle scenarios where multiple configuration objects, such as twenty different Ethernet interfaces, require identical parameters like a specific description or MTU value. By defining these common settings once within a group, an administrator can then apply that group to multiple interfaces using the apply-groups statement.

This methodology drastically reduces the number of repetitive commands required and, more importantly, ensures strict consistency across the device. If the MTU needs to be adjusted in the future, the change is made in a single location-within the configuration group-and is automatically inherited by all interfaces to which the group is applied. This inheritance model prevents " configuration drift " where individual interfaces might otherwise end up with mismatched settings due to manual entry errors. Using configuration groups is considered a best practice for Senior Architects managing high-density platforms, as it simplifies the candidate configuration file and makes the management of bulk interface settings both scalable and error- resistant.

Reference: Configuration Basics, Junos Configuration Groups, apply-groups.

NEW QUESTION: 22

Which two characteristics describe Junos OS software? (Choose two.)
A. Junos OS is a monolithic code base.
B. Junos OS supports automation features.
C. Junos OS runs only on routers.
D. Junos OS uses a modular architecture with independent processes.
Answer: (SHOW ANSWER)
Junos OS is distinguished from legacy network operating systems by its modern, modular architecture .
Unlike a monolithic system where a single failure can crash the entire kernel, Junos runs various software functions-such as the routing protocol process (rpd), the interface process (dcd), and the management daemon (mgd)-as independent processes in their own protected memory spaces. This modularity ensures high availability; if one daemon encounters an error, it can be restarted without impacting the overall system stability or traffic forwarding.
Furthermore, Junos OS is a leader in automation features . It was built with a programmable foundation, utilizing an XML-based configuration database and supporting NETCONF for standardized remote management. This allows network architects to utilize modern DevOps tools like Ansible, Python (PyEZ), and SaltStack to automate complex configuration tasks, perform bulk upgrades, and enforce state compliance.
By treating the network as code, Junos enables high-velocity operations that reduce human error. While Junos originally powered routers, it now runs across a vast portfolio including EX/QFX switches and SRX firewalls, proving its versatility far beyond just routing platforms.
Reference: Junos OS Fundamentals, Software Architecture, Modularization.

NEW QUESTION: 23
Which statement is correct about traffic flow in the network shown in the exhibit?

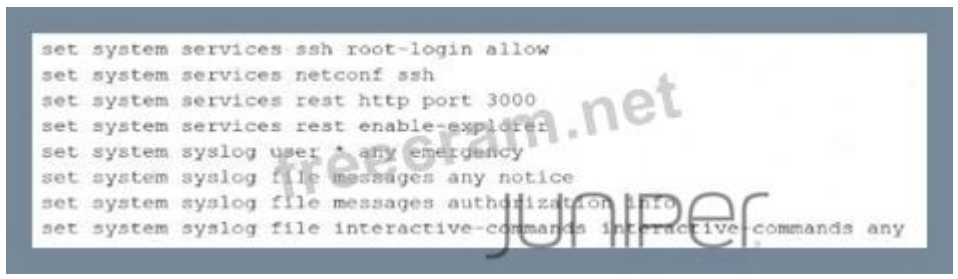


freecram.net
juniper NETWORKS

A. A routing loop can occur if one of the users sends packets to 10.1.99.1.
B. Only User A can reach destinations beyond Router R1.
C. Router R2 will drop packets destined for user B and user C.
D. Router R1 will discard all packets from all three users.
Answer: (SHOW ANSWER)
The configuration exhibit demonstrates a classic scenario where mismatched static routing leads to a routing loop . Router R1 is configured with a default route (0.0.0.0/0) pointing to R2 as its next hop. Conversely, R2 is configured with a broad static route for 10.1.0.0/16 pointing back to R1 .
If a user sends a packet to an unassigned IP address such as 10.1.99.1 , the following sequence occurs:

* R1 receives the packet and consults its routing table. Finding no specific match for the 10.1.99.1 host, it uses the default route and forwards the packet to R2 .
* R2 receives the packet and identifies that 10.1.99.1 falls within its defined static route for 10.1.0.0/16 .
* Following its configuration, R2 forwards the packet back to R1 . This process repeats indefinitely-or until the packet ' s Time to Live (TTL) reaches zero-because the broad summary on R2 encompasses addresses that R1 does not actually have a local path for. This illustrates the critical importance of ensuring that summary routes or default routes do not overlap in a way that creates circular forwarding paths for non-existent destinations. Reference: Routing Fundamentals, Static Route Configuration, Routing Loops and TTL.

NEW QUESTION: 24
Click the Exhibit button.



Which command displays the output in the format shown in the exhibit?
A. show configuration | display inheritance
B. show configuration | display set
C. show configuration
D. show configuration | display detail
Answer: (SHOW ANSWER)
The exhibit illustrates a Junos configuration rendered as a sequence of flat, executable lines that each begin with the set keyword. This is commonly referred to as the " set format. " By default, Junos OS displays the configuration in a hierarchical, brace-delimited format (often called " staza " or " curly brace " format). While the default format is excellent for visualizing the structural relationship between different configuration objects, the set format is often preferred for documentation, scripting, or copying specific configuration snippets between different devices.
To produce the output seen in the exhibit, an administrator must append the pipe filter | display set to the show configuration command. This filter instructs the CLI parser to flatten the hierarchical structure and prepend the necessary context to every individual leaf statement. These lines are highly functional because they can be pasted directly into the CLI of another device while in configuration mode to recreate the exact settings. In contrast, display inheritance is used to reveal hidden settings applied via configuration groups, and display detail provides additional technical metadata about the objects. Neither of those options would transform the output into the discrete set command lines shown in the exhibit. Understanding how to toggle between these display formats is a fundamental skill for any architect managing Junos infrastructures through the Command Line Interface.
Reference: User Interfaces, Configuration Display Options, display set.

NEW QUESTION: 25
When troubleshooting a problem, you issue the following commands in sequence:
* show chassis alarms
* show chassis fpc
* show chassis fpc detail
* show chassis errors fpc-slot 0

In this scenario, what happens when you press the up arrow key twice at the prompt?
A. The show chassis fpc command is displayed at the prompt.
B. The show chassis errors fpc-slot 0 command is displayed at the prompt.
C. The show chassis alarms command is displayed at the prompt.
D. The show chassis fpc detail command is displayed at the prompt.
Answer: (SHOW ANSWER)
The Junos OS Command Line Interface (CLI) utilizes an advanced command-line editing environment influenced by standard Emacs and Unix terminal behaviors. One of the most critical features for operational efficiency is the command history buffer. This buffer automatically records a sequence of previously executed commands, allowing administrators to recall, modify, and re-execute them without manual re-entry.
The navigation of this history buffer is strictly chronological and operates as a stack. When the up arrow key is pressed once, the CLI retrieves the most recent command that was successfully entered-in this scenario, show chassis errors fpc-slot 0. Pressing the up arrow key a second time moves the cursor one step further back into the history stack to the command that preceded the most recent one. Following the provided sequence, the command executed prior to the " errors " check was show chassis fpc detail. Consequently, the second press of the up arrow key will display show chassis fpc detail at the prompt. This mechanism is essential for architects during intensive troubleshooting sessions, enabling them to cycle through relevant diagnostic commands rapidly while maintaining focus on the hardware output rather than syntax repetition.
Reference:
User Interfaces, CLI Editing Features, Command History.

NEW QUESTION: 26
Your system administrator notified the infrastructure team that all server NICs will be moving to jumbo frames. All of the NICs used by servers are 1 gigabit. The starting frame size will be 4K. The exact frame size may change depending on testing results. In this scenario, which choice would provide a flexible solution?
A. Create a group that adjusts MTU size on 1 gigabit interfaces and apply at the interfaces level.
B. Apply the MTU to each interface family for each 1 gigabit interface.
C. Set the app-engine compute-cluster Ethernet MTU size for the Junos VM.
D. Use the system internet-options path-mtu-discovery to dynamically adjust MTU.
Answer: A (LEAVE A REPLY)
In large-scale Junos deployments, efficiency and flexibility are achieved through the use of configuration groups . When faced with a requirement like moving all 1-gigabit interfaces to jumbo frames-with the caveat that the exact MTU value (e.g., 4000 bytes) might change after testing-manually editing every interface is both tedious and prone to error.
By creating a configuration group under the [edit groups] hierarchy, you can define the MTU parameter once.
You then use the apply-groups statement at the [edit interfaces] level or on specific interface ranges. This creates a " template " effect. The flexibility comes into play during the testing phase: if results indicate that a
9000-byte MTU is preferable to 4000 bytes, the architect only needs to modify the value in the group definition. The Junos OS inheritance mechanism automatically propagates this update to every interface associated with that group.
Applying MTU at the family level (Option B) is less efficient and doesn ' t handle the physical Layer 2 MTU requirements of jumbo frames as effectively. Path-MTU discovery (Option D) is a protocol-level function for avoiding fragmentation but does not configure the local interface ' s hardware capability to accept larger frames. Thus, groups represent the best practice for centralized, scalable management.
Reference: Configuration Basics, Junos Groups, Interface MTU Configuration.

NEW QUESTION: 27

You power on a new MX Series router for the first time and connect to the console. You notice that no transit interfaces are passing traffic. In this scenario, which statement is correct?

A. All interfaces are enabled with DHCP client enabled.

B. All interfaces are enabled and have an IP address of 10.0.0.1.

C. The interfaces are configured as Layer 2 trunk ports.

D. The interfaces are not configured.

Answer: (SHOW ANSWER)

When you initially unbox and power on a Juniper MX Series router, it loads a factory-default configuration

. Unlike some consumer-grade or lower-end enterprise switches that might have all ports active in a default VLAN, high-performance routers like the MX Series prioritize security and intentionality. In the factory- default state, the transit interfaces are not configured .

While the physical hardware interfaces (such as ge-0/0/0 or xe-0/1/0) are detected by the Junos kernel, they lack any logical unit or protocol family definitions (like family inet or family inet6). Without a logical unit- even a simple unit 0-the Packet Forwarding Engine (PFE) will not accept or forward any traffic arriving on those ports. Furthermore, as discussed in previous questions, the device is essentially in a " locked " state; you cannot even commit new changes to enable these interfaces until you have defined a root-authentication password. This " blank slate " approach ensures that no traffic accidentally flows through a newly installed provider-edge device until an architect has explicitly defined the routing policies, firewall filters, and interface parameters required for the specific network environment. To begin passing traffic, you must manually define the logical units and assign the appropriate IP addresses or switching parameters to each interface.

Reference: Configuration Basics, Initial Configuration, Factory Default Settings.

NEW QUESTION: 28

How many usable hosts are in a /24 subnet mask?

A. 250

B. 254

C. 255

D. 256

Answer: (SHOW ANSWER)

In the IPv4 addressing architecture, a /24 prefix length (standard Class C subnet mask of 255.255.255.0) signifies that the first 24 bits of the 32-bit address are reserved for the network portion, leaving 8 bits for the host portion. To calculate the total number of available IP addresses within this range, the formula 2^n is applied, where n represents the number of host bits. For a /24 mask, 2^8 results in 256 total addresses. However, standard networking conventions-which Junos OS adheres to for interface configuration and routing-require the reservation of two specific addresses within any given subnet. The first address in the range is the network address (where all host bits are 0), used to identify the subnet itself in the routing table.

The last address in the range is the directed broadcast address (where all host bits are 1), utilized to communicate with all hosts on that segment simultaneously. Therefore, the number of " usable " hosts that can be assigned to device interfaces, such as ge-0/0/0.0 or a workstation, is calculated as $2^n - 2$. In this instance, $256 - 2 = 254$. Understanding this calculation is fundamental for an architect when performing IP address management (IPAM) and ensuring that the Packet Forwarding Engine is configured with valid, assignable host addresses within a defined broadcast domain.

Reference: Networking Fundamentals, IPv4 Subnetting and CIDR.

NEW QUESTION: 29

Which two statements about prefix lists in Junos are correct? (Choose two.)

A. Prefix lists can be re-used in multiple routing policies.
B. Prefix lists can be used in both firewall filters and routing policies.
C. Prefix lists cannot be used in routing policies.
D. Prefix lists cannot be used in firewall filters.
Answer: (SHOW ANSWER)
Prefix lists in Junos OS are named collections of IP addresses or network prefixes defined under the [edit policy-options] hierarchy. One of their most powerful features is their versatility and reusability. Because they are defined as independent objects, a single prefix list can be referenced in multiple different routing policies across the device. This modularity ensures consistency; for instance, if a set of " internal " prefixes changes, an administrator only needs to update the list in one location for those changes to propagate to every policy that utilizes it.
Furthermore, prefix lists are designed to be used across different functional areas of the Junos architecture.
They are equally valid for use in routing policies (to control the import or export of routes between protocols like BGP or OSPF) and in firewall filters (to match source or destination addresses for transit or management traffic). When used in a routing policy, the prefix list typically performs an exact match on the prefix length unless modified by a match type like orlonger. In a firewall filter, it acts as a high-speed lookup table for the Packet Forwarding Engine. This dual-purpose capability makes prefix lists a foundational tool for architects seeking to implement scalable, automated security and routing logic within a unified configuration framework.

NEW QUESTION: 30
A network administrator must set up the initial configuration of the out-of-band management interface on a new Juniper router to ensure management traffic is isolated from the default routing table (inet.0). In this scenario, which configuration step is required to accomplish this task in Junos OS?
Freecram.net
A. Configure an IP address on interface ge-0/0/0.0 and enable ethernet-switching family.
B. Configure the lo0.0 loopback interface with a management IP and apply it to the [edit system services] hierarchy.
C. Assign an IP address to the me0.0 interface and set the routing-options to instance-type virtual-router.
D. Assign an IP address to interface fxp0.0 or em0.0 and use the command set system management- instance to enable the management routing instance.
Answer: (SHOW ANSWER)
In modern Junos OS versions, the most efficient and standard way to isolate Out-of-Band (OOB) management traffic from transit traffic is by utilizing the management-instance . Historically, management interfaces like fxp0 (on M/MX/T series) or me0 (on EX/QFX series) shared the global routing table (inet.0), which could lead to routing conflicts if management subnets overlapped with production data.
To resolve this, Junos introduced the set system management-instance command. When this is enabled, the OS automatically creates a dedicated routing instance named mgmt_junos. The physical management interface (be it fxp0, em0, or me0) and its associated logical unit are moved into this private instance. This creates a complete separation: management protocols like SSH, SNMP, and NTP operate within mgmt_junos, while BGP, OSPF, and customer data remain in inet.0. This architecture ensures that even a massive routing loop or table exhaustion in the production plane will not prevent an administrator from accessing the device via the OOB port. Furthermore, it simplifies the configuration of default gateways for management traffic, as the mgmt_junos instance maintains its own independent routing table (mgmt_junos.inet.0), preventing management routes from ever being leaked into the provider core.
Reference: Operational Monitoring and Maintenance, Management Instance, OOB Management.

NEW QUESTION: 31
Which statement accurately describes the purpose of route preference in Junos OS?
A. It sets the metric for forwarding traffic through the Packet Forwarding Engine.

B. It determines which route is selected as active when multiple routes to the same destination exist.
C. It controls the redistribution of routes between routing instances.
D. It determines the maximum number of routes that can be installed in the routing table.
Answer: (SHOW ANSWER)
In the Junos OS architecture, the routing table often receives prefix information from various sources, including direct connections, static configurations, and multiple dynamic interior and exterior gateway protocols. Route preference, frequently referred to as administrative distance in other vendor environments, serves as the primary tie-breaking mechanism used by the Routing Engine to select a single " active " route when multiple entries for the exact same destination prefix exist from different protocol sources. Each routing source is assigned a default numerical value, where a lower numerical value indicates a more preferred or " trustworthy " source. For instance, a direct route typically carries a preference of 0, while OSPF internal routes default to 10 and BGP routes default to 170.
The selection process evaluates these values; the route with the lowest preference is installed in the forwarding table and used for transit traffic. If preferences are equal, Junos secondary tie-breakers like local preference or metric are considered. Understanding this hierarchy is critical for traffic engineering and ensuring predictable routing behavior across the fabric. Modification of these default values via routing policy allows administrators to influence path selection without altering the underlying protocol metrics themselves.
Reference: Routing Fundamentals, Route Preference Selection.

Valid JN0-106 Dumps shared by ExamDiscuss.com for Helping Passing JN0-106 Exam! ExamDiscuss.com now offer the **newest JN0-106 exam dumps**, the ExamDiscuss.com JN0-106 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com JN0-106 dumps with Test Engine here: https://www.examdiscuss.com/Juniper/exam/JN0-106/premium/ (**101** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 32
An administrator configures the timezone on a Junos device. Which two actions must the administrator perform to ensure the device uses the correct local time? (Choose two.)
A. Configure an NTP server.
B. Configure a DNS server.
C. Set the date and time setting manually.
D. Reboot the device.
Answer: (SHOW ANSWER)
In Junos OS, configuring the time-zone (such as America/LosAngeles) within the [edit system] hierarchy establishes the offset from Coordinated Universal Time (UTC) and governs how the device displays timestamps for logs and system events. However, simply setting the timezone does not adjust the underlying system hardware clock; it only dictates how that clock ' s data is interpreted and presented. To ensure the device reflects the correct local time, the administrator must either synchronize the system with an external reference or manually input the current date and time.
Configuring a Network Time Protocol (NTP) server is the preferred professional method, as it allows the device to automatically synchronize its clock with a reliable stratum source, ensuring long-term accuracy and consistency across the network. Alternatively, the set date operational mode command can be used to manually define the current year, month, day, hour, and minute. While a DNS server is necessary for resolving the hostnames of NTP servers, it does not provide time data itself. Furthermore, rebooting the device will not correct a fundamentally unset or

drifting clock. Therefore, combining the correct timezone with either NTP synchronization or a manual date setting is the standard procedure for establishing temporal accuracy on a Junos platform. Reference: Operational Monitoring and Maintenance, System Time and NTP.

NEW QUESTION: 33
You must add a large hierarchical configuration to your Junos device. You also want to completely replace the existing candidate configuration with a new configuration file. Which command would allow you to accomplish these tasks?
A. load merge terminal
B. load override terminal
C. load factory default
D. load set terminal
Answer: (SHOW ANSWER)
The load command in Junos OS provides several operational methods for importing configuration data into the candidate buffer. When an administrator needs to perform a " clean slate " update-where the objective is to completely replace the existing candidate configuration with a new hierarchical file-the override option is the correct tool. Unlike load merge, which blends new data with the existing configuration, or load replace, which only updates specifically tagged sections, load override discards every statement currently in the candidate configuration and substitutes it entirely with the new content.
Using the terminal keyword in conjunction with override allows the architect to paste a large hierarchical configuration directly into the Command Line Interface (CLI). This is the most efficient method for applying validated templates, restoring full system backups, or migrating configurations between devices without having to manually delete existing parameters. After the data is pasted and the process is finalized (typically with a Ctrl +D sequence), the Junos OS kernel validates the new candidate configuration against the device ' s hardware and software capabilities. To make these changes active and operational, a subsequent commit command must be executed. This comprehensive replacement mechanism ensures configuration integrity by eliminating any potential remnants of previous, unwanted settings that might conflict with the new deployment.
Reference: Configuration Basics, Loading and Managing Configurations.

NEW QUESTION: 34
Which protocol is used to discover the Layer 2 (MAC) address of a next hop for IPv6 hosts?
A. DHCP
B. ARP
C. NDP
D. DNS
Answer: (SHOW ANSWER)
In the IPv6 protocol suite, the traditional Address Resolution Protocol (ARP) used in IPv4 has been deprecated and replaced by the Neighbor Discovery Protocol (NDP). NDP is a multifaceted protocol built upon the Internet Control Message Protocol version 6 (ICMPv6). Its primary purpose is to allow a host or router to determine the Layer 2 hardware (MAC) address of a neighbor on the same local link when only the neighbor ' s IPv6 address is known.
This specific process is known as Neighbor Solicitation and Neighbor Advertisement. When a Junos device needs to resolve a MAC address for an IPv6 next hop, it sends a Neighbor Solicitation (ICMPv6 Type 135) message to the solicited-node multicast address. The target host responds with a Neighbor Advertisement (ICMPv6 Type 136) containing its physical MAC address. Beyond address resolution, NDP also handles Router Discovery, Prefix Discovery, and Duplicate Address Detection (DAD). Unlike ARP, which relies on broadcasts that can impact all hosts on a segment, NDP utilizes efficient multicast communication.

Understanding NDP is critical for Junos architects, as it is the foundational mechanism that facilitates logical- to-physical address mapping in modern IPv6 environments, ensuring that the Packet Forwarding Engine can properly encapsulate frames for local delivery.
Reference: Networking Fundamentals, IPv6 Neighbor Discovery Protocol.

NEW QUESTION: 35
Which two tasks should be performed when creating a new user account on a Junos device? (Choose two.)
A. Assign the user to a login class.
B. Enable SSH for the user explicitly.
C. Configure a password for the user.
D. Configure the user to bypass authentication.
Answer: (SHOW ANSWER)
Creating a new user account in Junos OS involves several specific steps within the [edit system login] configuration hierarchy. To establish a functional and secure user account, an administrator must first define the username and assign that user to a login class. Login classes are essential because they define the permissions and access levels for the user, such as super-user, read-only, or operator. Without a login class, a user would have no permissions to perform tasks within the CLI.
The second mandatory task is to configure an authentication method for the user, most commonly a password.
This is typically done using the authentication plain-text-password command, which prompts the administrator to enter and confirm the secret string that the system then hashes and stores. While Junos also supports public-key authentication for SSH, a local password remains the standard for basic access control. It is important to note that SSH access is generally controlled at the system level under [edit system services] and does not need to be enabled on a per-user basis individually. Furthermore, allowing a user to bypass authentication is contrary to the Junos security model and is not a standard task in user account creation.
Reference: User Interfaces, User Management, Login Classes.

NEW QUESTION: 36
Which statement is correct when Router R1 receives a packet from User A destined for User B as shown in the exhibit?


A. Router R1 replaces the destination IP address in the packet with the IP address of Router R2.
B. Router R1 leaves the packet unchanged.
C. Router R1 replaces the destination MAC address in the packet with the MAC address of Router R2.
D. Router R1 replaces the destination MAC address in the packet with the MAC address of User B.
Answer: (SHOW ANSWER)
Comprehensive and Detailed 150 to 250 words of Explanation From: In a routed environment like the one shown in the exhibit, traffic forwarding involves a constant interaction between Layer 3 (Network) and Layer
2 (Data Link) addressing. When User A generates a packet destined for User B, the source and destination IP addresses remain static throughout the entire journey across the network (assuming no Network Address Translation is performed). However, the Layer 2 Ethernet headers must be rewritten at every hop because MAC addresses have only local significance on a physical segment.
As Router R1 receives the packet from User A, it performs a lookup in its Forwarding Information Base (FIB) and identifies that the path to User B requires forwarding the packet to Router R2. R1 decapsulates the incoming frame, stripping away the original Ethernet header that contained

User A ' s source MAC and R1 ' s own destination MAC. To forward the packet to the next hop, R1 creates a new Ethernet header. The source MAC address becomes the MAC address of R1's egress interface, and the destination MAC address is replaced with the MAC address of Router R2 . R1 cannot use User B ' s MAC address at this point because User B is not on a directly connected segment. This hop-by-hop MAC address replacement is essential for the Packet Forwarding Engine to successfully deliver the frame to the next Layer 3 device in the path. Reference: Networking Fundamentals, Packet Forwarding, Layer 2 and Layer 3 Addressing.

NEW QUESTION: 37
Which statement about class of service (CoS) in a network is correct?
A. CoS encrypts traffic to secure data across the network.
B. CoS prioritizes certain types of traffic during congestion.
C. CoS assigns IP addresses dynamically to optimize routing.
D. CoS prevents broadcast storms by segmenting VLANs.
Answer: B (LEAVE A REPLY)
Class of Service (CoS) is a fundamental suite of features in Junos OS designed to manage traffic patterns during periods of network congestion. Rather than treating all packets equally, CoS allows the Packet Forwarding Engine (PFE) to differentiate between various types of traffic-such as latency-sensitive Voice over IP (VoIP), critical routing protocol updates, and standard " best-effort " internet traffic-and prioritize them accordingly. When egress interface buffers become saturated, the CoS mechanism uses defined schedulers and queues to ensure that high-priority packets are transmitted first, while less critical traffic may be delayed or dropped.
It is important to distinguish CoS from security or addressing functions. CoS does not provide encryption services (which is the role of IPsec or MACsec), nor does it manage IP address allocation or VLAN segmentation. Instead, it focuses entirely on the intelligent allocation of bandwidth and buffer resources. By implementing CoS, network architects can guarantee a specific level of performance for mission-critical applications, effectively minimizing jitter and packet loss for the most important data streams. This deterministic behavior is vital for modern converged networks where multiple traffic types compete for limited hardware resources across the switch fabric or WAN links. Reference: Junos OS Fundamentals, Class of Service (CoS) Overview.

NEW QUESTION: 38
Which two statements accurately describe the relationship between the routing table and the forwarding table on a Junos device? (Choose two.)
A. The routing table resides in the data plane for fast lookups.
B. The routing table selects the best route based on routing information.
C. The forwarding table is built from the routing table.
D. The routing table is built from the forwarding table.
Answer: (SHOW ANSWER)
The relationship between the routing table (Routing Information Base or RIB) and the forwarding table (Forwarding Information Base or FIB) is the cornerstone of the Junos OS architectural separation between the control and data planes. The routing table resides in the control plane on the Routing Engine (RE). Its primary role is to aggregate all reachability information from every configured protocol and select the best route for each destination prefix based on criteria like preference and metrics.
Once the Routing Engine has identified the single " active " best path for a destination, it distills this complex routing data into a simplified, streamlined version called the forwarding table . The forwarding table contains only the essential information needed to move a packet: the destination prefix, the egress interface, and the Layer 2 next-hop MAC address. The RE then " pushes " this forwarding table to the Packet Forwarding Engine (PFE) in the data plane. By having the PFE use a table built from the routing table , Junos ensures that transit traffic can be processed at wire speed without the overhead of complex routing logic. This one-way flow-from the comprehensive RIB on the RE to the

optimized FIB on the PFE-allows the device to maintain high performance even while routing protocols are recalculating or the management plane is under heavy load.

NEW QUESTION: 39

Click the Exhibit button.

```
[edit routing-options]
user@router# show
static {
    route 10.10.10.0/24 next-hop 10.1.1.1;
}
```

freecram.net

Referring to the exhibit, you are configuring a Junos router to provide connectivity to a building across town on the network 10.10.10.0/24. The next-hop router is at 10.10.1.1, which is reachable using interface ge-0/0/1.
After committing the configuration in the exhibit, users report they still cannot reach the 10.10.10.0/24 network, and the route does not appear as active in the routing table. In this scenario, which statement is correct?

A. The next-hop address 10.1.1.1 is not directly connected or reachable through another route.

B. Static routes must include the outgoing interface as the next hop.

C. The static route requires a preference value to be specified or it will not install.

D. The static route requires the retain keyword to remain active in the routing table.

Answer: (SHOW ANSWER)

In Junos OS, the Routing Engine (RE) performs a validation check on every entry in the Routing Information Base (RIB). For a static route to be considered valid and transition to an active state in the inet.0 table, its designated next hop must be resolvable . A next-hop address is resolvable only if the router has an existing route (typically a directly connected route) to that specific IP address.
According to the exhibit, the static route for 10.10.10.0/24 has been configured with a next hop of 10.1.1.1 .
However, the scenario states that the actual gateway router is located at 10.10.1.1 . If the local interface (ge-0 /0/1) is configured with an IP in the 10.10.1.0/x subnet, the router will have a direct route to 10.10.1.1, but it will likely have no path to the 10.1.1.1 address provided in the exhibit.
Because the router cannot resolve the next hop 10.1.1.1 , the static route is placed in an " inactive " or " hidden " state. It will not be installed in the forwarding table pushed to the Packet Forwarding Engine (PFE), and standard show route commands will not display it unless specific flags like hidden or all are used. This logic ensures that the router does not attempt to forward packets into a " black hole " where the gateway is logically unreachable. To fix this, the administrator must modify the configuration to point to the correct, reachable next-hop address of 10.10.1.1.
Reference: Routing Fundamentals, Static Route Resolution, and Troubleshooting Routing Tables.

NEW QUESTION: 40

Which statement about collision domains and broadcast domains is correct?

A. A router separates collision domains but forwards all broadcast traffic between its interfaces.

B. VLANs on a switch reduce collision domains but have no effect on broadcast domains.

C. A switch creates a separate collision domain for each port, but all ports remain in the same broadcast domain by default.

D. Broadcast domains are only relevant in IPv4 networks and are not used in IPv6 networks.

Answer: (SHOW ANSWER)

Understanding the distinction between collision and broadcast domains is fundamental to Layer 2 and Layer 3 networking. In a modern Ethernet switching environment, a switch effectively eliminates collisions by creating a separate collision domain for each of its physical ports. This is

achieved through micro- segmentation and the support of full-duplex communication, which allows for simultaneous transmission and reception of data on a per-port basis.
However, while a switch segments collision domains, it does not inherently segment broadcast domains. By default, all ports on a switch reside within the same broadcast domain, meaning that a broadcast frame (such as an ARP request) received on one port will be flooded to all other ports within that specific VLAN or bridge domain. Segmenting broadcast domains requires either the configuration of Virtual LANs (VLANs) or the use of a Layer 3 device like a router, which does not forward broadcast traffic by default between its interfaces. It is a common misconception that broadcast domains are absent in IPv6; while IPv6 utilizes multicast (via NDP) instead of traditional Layer 2 broadcasts, the concept of the " link-local " scope where these packets are distributed remains functionally equivalent to a broadcast domain. For the JNCIA-Junos standard, the core takeaway is that switches provide per-port collision isolation while maintaining a unified broadcast environment unless explicitly partitioned.
Reference: Networking Fundamentals, Collision and Broadcast Domains.

NEW QUESTION: 41
You want to redeploy a Junos device by clearing the existing configuration and resetting it to factory defaults.
In this scenario, which command would help to accomplish this task?
A. show system storage
B. request system storage cleanup dry-run
C. request system zeroize
D. request system storage cleanup
Answer: (SHOW ANSWER)
When a network architect needs to completely sanitize a Junos device for redeployment or decommissioning, the request system zeroize command is the most thorough tool available. Unlike simply loading the factory default configuration, which only resets the configuration database, the zeroize command performs a deep wipe of the system.
Specifically, this command removes all user-created data, including all configuration files (active and rollback), log files, license keys, and any locally stored files in the /var/tmp or /home directories. It essentially restores the device to its " pristine " out-of-box state. Once the command is initiated, the device reboots and goes through a sanitization process. This is a critical security measure to ensure that sensitive information- such as encrypted passwords, proprietary routing policies, or SNMP community strings-does not leave the organization when hardware is transferred.
In contrast, the request system storage cleanup command is a maintenance utility used to delete temporary files and old log entries to free up disk space, but it does not affect the running configuration or user accounts.
Therefore, for a total system reset that includes configuration deletion, zeroize is the mandatory operational command.
Reference: Operational Monitoring and Maintenance, System Sanitization, request system zeroize.

NEW QUESTION: 42
Which two statements are true about the firewall filter configuration shown in the exhibit? (Choose two.)



freecram.net

A. It applies the filter to a physical interface.

B. It counts the number of SSH packets that egress from the source SSH interface.

C. It evaluates SSH packets egressing from the management interface.

D. It sends filtered data to a syslog file.

Answer: (SHOW ANSWER)

The exhibit illustrates the configuration of a firewall filter named mgmt_fill and its subsequent application to an interface. The first true statement is that the filter is applied to a physical interface . The configuration shows the filter attached to me0 , which in Junos nomenclature represents the Management Ethernet port-a dedicated physical port for out-of-band management traffic. This is separate from logical or virtual interfaces, as me0 provides the physical link for administrative access.

The second true statement is that the filter evaluates SSH packets egressing from the management interface . In the provided snippet, term t1 specifically matches the destination-port ssh , and the filter is applied to the interface unit. When a filter is applied to an interface, it can monitor traffic entering or leaving the device. Furthermore, the filter utilizes a count action (count c1), which is a non-terminating action used to provide telemetry on specific traffic types passing through that physical port. There is no mention of a syslog or log action in the configuration, meaning that while packets are counted, they are not being written to the system log files. This configuration is a standard method for hardening the management plane and tracking administrative session activity on the Routing Engine. Reference: Routing Policy and Firewall Filters, Firewall Filter Actions, Management Interfaces.

NEW QUESTION: 43

Your team alerts you that users connected to ge-0/0/5 are experiencing intermittent slowness. You log in to the switch and want to see live, real-time traffic updates for that interface to determine whether the link is being over-utilized. Which monitoring command should you use in this scenario?

A. show interfaces ge-0/0/5 extensive

B. monitor interface ge-0/0/5
C. show interfaces terse
D. show chassis hardware
Answer: (SHOW ANSWER)

Valid JN0-106 Dumps shared by ExamDiscuss.com for Helping Passing JN0-106 Exam! ExamDiscuss.com now offer the **newest JN0-106 exam dumps**, the ExamDiscuss.com JN0-106 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com JN0-106 dumps with Test Engine here: https://www.examdiscuss.com/Juniper/exam/JN0-106/premium/ (**101** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)