



Juniper JN0-106 JNCIA-Junos Practice Questions

Shared by Rice on 19-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

Refer to the exhibit.

Click the Exhibit button.

```
user@router> show route 192.168.100.100
inet.0: 16 destinations, 19 routes (16 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
192.168.100.100/32 * [Static/5] 00:12:52
    > to 192.168.0.2 via xe-0/0/0.0
      [OSPF/10] 00:01:01, metric 100
    > to 192.168.1.2 via xe-0/1/2.0
      [IS-IS/15] 00:01:08, metric 10
    > to 192.168.3.2 via xe-0/1/3.0
      [BGP/170] 00:00:06, localpref 100
        AS path: 65002 I, validation-state: unverified
    > to 192.168.4.2 via xe-0/1/4.0
```

Referring to the exhibit using the show route 192.168.100.100 command output, over which interface will the traffic be forwarded?

Options:

- A- xe-0/1/3.0
- B- xe-0/0/0.0
- C- xe-0/1/4.0
- D- xe-0/1/2.0

Answer:

B

Explanation:

In the Junos OS architecture, the Routing Engine (RE) manages path selection by evaluating multiple potential routes to a specific destination found within the Routing Information Base (RIB). When multiple routing sources (such as static configuration, OSPF, IS-IS, and BGP) provide information for the exact same destination prefix---in this case, 192.168.100.100/32---the device utilizes route preference as the primary tie-breaker to determine which entry becomes the 'active' route.

The provided exhibit displays the default preference values for each protocol: Static is 5, OSPF is 10, IS-IS is 15, and BGP is 170. Junos OS follows a 'lower is better' logic for preference; therefore, the Static route is selected as the most trustworthy path. In the command output, the active route is explicitly identified by the asterisk (*) and plus sign (+) symbols located next to

the [Static/5] entry. Looking at the specific next-hop information for this active static route, the output indicates the traffic is sent to 192.168.0.2 via xe-0/0/0.0. Consequently, the Packet Forwarding Engine (PFE) will install this specific path into the forwarding table, causing all traffic destined for 192.168.100.100 to be egressed over the xe-0/0/0.0 interface.

Question 2

Question Type: MultipleChoice

Which two functions are performed by the PFE? (Choose two.)

Options:

- A- It maintains the routing table.
- B- It implements firewall filters.
- C- It selects active routes.
- D- It forwards transit traffic.

Answer:

B, D

Explanation:

The Packet Forwarding Engine (PFE) represents the data plane of a Junos device, responsible for the high-speed processing and movement of packets through the system. Its primary role is to forward transit traffic---data that enters one interface and exits another---at wire speed using specialized hardware such as Application-Specific Integrated Circuits (ASICs). To accomplish this, the PFE utilizes a local copy of the Forwarding Information Base (FIB) provided by the Routing Engine, ensuring that forwarding decisions are made locally without requiring the main CPU's intervention for every packet.

In addition to pure forwarding, the PFE is the functional component that implements and executes firewall filters and policing. Because firewall filters must be applied to transit traffic at line rate to prevent bottlenecks, the PFE evaluates incoming and outgoing packets against configured filter terms in hardware. This ensures that security policies and traffic shaping are applied with minimal latency. It is critical to note that the PFE does not maintain the master routing table (RIB) or perform route selection; those 'intelligent' control plane functions are strictly the domain of the Routing Engine. By offloading the repetitive tasks of packet inspection and hardware forwarding to the PFE, Junos OS maintains consistent performance even under heavy traffic loads or complex security configurations. Reference: Junos OS Fundamentals, Packet Forwarding Engine Architecture.

Question 3

Question Type: MultipleChoice

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

Options:

- 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:

A, B

Explanation:

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.

Question 4

Question Type: MultipleChoice

Which command is used to view real-time traffic statistics for all interfaces?

Options:

- A- show interfaces extensive
- B- monitor interface traffic
- C- monitor traffic interface all
- D- show interfaces statistics

Answer:

B

Explanation:

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.

Question 5

Question Type: MultipleChoice

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?

Options:

- 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:

D

Explanation:

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.

Question 6

Question Type: MultipleChoice

What information would you find using the CLI help command?

Options:

- A- a URL for accessing the technical documentation
- B- message of the day
- C- hyperlinks for remediation actions
- D- an explanation for specific system log error messages

Answer:

D

Explanation:

The Junos OS CLI is engineered with an extensive, self-contained help subsystem designed to provide immediate technical guidance without requiring constant reference to external manuals. The help command is a versatile tool that operates through several key sub-commands: topic, reference, and log. While help topic provides conceptual overviews and help reference displays specific configuration syntax and hierarchical requirements, the help log command is specifically tailored for system maintenance and troubleshooting.

The primary purpose of help log is to provide a detailed explanation for specific system log error messages generated by the device. When a Junos daemon or process writes an entry to the syslog, it includes a unique message identifier or 'tag.' By executing help log <message-tag>, an architect can retrieve a clinical breakdown of why the message was generated, the severity of the event, and often the recommended action to resolve the underlying issue. This capability is vital for rapid interpretation of complex system events in real-time. It ensures that administrators have authoritative, context-aware information directly at the terminal, effectively bridging the gap between raw diagnostic output and actionable technical intelligence within the Junos environment. Reference: User Interfaces, CLI Help Facilities, help log.

Question 7

Question Type: MultipleChoice

Which Junos tool should you use to identify the path that packets take through the network to a destination?

Options:

- A- monitor interface traffic
- B- traceroute
- C- SNMP
- D- ping

Answer:

B

Explanation:

When you need to visualize the hop-by-hop journey of a packet across a multi-vendor or Junos-based network, traceroute is the definitive operational tool. Unlike ping, which merely confirms end-to-end reachability by eliciting an Echo Reply, traceroute provides a clinical breakdown of every Layer 3 device (router or switch) in the path.

The mechanics of this tool are quite clever: it sends out a sequence of packets (usually UDP or ICMP) with an increasing Time-to-Live (TTL) value, starting at 1. When the first router receives the packet, it decrements the TTL to 0, discards the packet, and sends an ICMP 'Time Exceeded' message back to the source. This informs your Junos device of the first hop's identity. This process repeats, incrementing the TTL each time, until the packet reaches the final destination. This path discovery is vital for identifying where traffic might be diverted by a misconfigured routing policy or where latency is being introduced in the network fabric. While monitor interface traffic gives you real-time throughput on a local port and SNMP provides historical telemetry to a management station, neither can map the external topological path like traceroute. In the Junos CLI, you can even specify the source address or bypass the routing table to test specific egress paths.

Question 8

Question Type: MultipleChoice

How are the Routing Engine and the Packet Forwarding Engine components connected?

Options:

- A- They use shared memory access.
- B- They use external breakout cables.
- C- They use an MPLS connection.
- D- They use an internal Ethernet link.

Answer:

D

Explanation:

The fundamental architecture of Junos OS is built upon the clean separation of the Control Plane (Routing Engine or RE) and the Forwarding Plane (Packet Forwarding Engine or PFE). While these two components perform vastly different tasks, they must maintain a high-speed, reliable communication channel to synchronize the state of the device. This connection is achieved through an internal Ethernet link.

This internal link serves several critical functions. First, it allows the Routing Engine to 'push' the distilled forwarding table (FIB) to the PFE, ensuring that the hardware knows exactly how to handle incoming transit traffic at wire speed. Second, it acts as a conduit for exception traffic. If the PFE receives a packet that it cannot handle alone---such as an OSPF hello, a BGP update, or an ICMP 'Time Exceeded' message---it sends that packet over the internal Ethernet link to the RE for processing. This link is carefully policed by built-in rate limiters to ensure that a flood of transit-related exception traffic cannot overwhelm the Routing Engine's CPU, a mechanism known as control plane protection. By using a standard Ethernet-based internal fabric, Junos ensures a scalable and modular design where the RE can focus on complex protocol calculations while the PFE focuses on the heavy lifting of packet switching.

Question 9

Question Type: MultipleChoice

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



```
[edit firewall]
user@router# show
family inet {
    filter mgmt_fill {
        term t1 {
            from {
                destination-port ssh;
            }
            then count c1;
        }
        term t2 {
            then accept;
        }
    }
}
[edit interfaces]
user@router# show
me0 {
    unit 0 {
        family inet {
            filter {
```

Options:

- 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:

A, C

Explanation:

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.

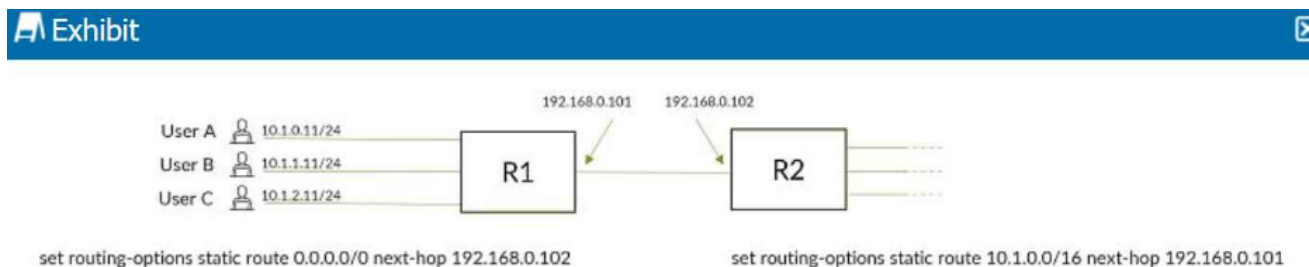
The second true statement is that the filter evaluates SSH packets egressing from the management interface. In the provided snippet, term t1 specifically matches the destination-port ssh, and the filter is applied to the interface unit. When a filter is applied to an interface, it can monitor traffic 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.



Question 10

Question Type: MultipleChoice

Which statement is correct about traffic flow in the network shown in the exhibit?



Options:

- 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:

A

Explanation:

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.

Question 11

Question Type: MultipleChoice

Which statement about class of service (CoS) in a network is correct?

Options:

- 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

Explanation:

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.



Question 12

Question Type: MultipleChoice

Which statement accurately describes the purpose of route preference in Junos OS?

Options:

- 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:

B

Explanation:

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.



To Get Premium Files for JN0-106 Visit

<https://www.p2pexams.com/products/jn0-106>

For More Free Questions Visit

<https://www.p2pexams.com/juniper/pdf/jn0-106>

20%
DISCOUNT

P2P
exams