Juniper

JN0-106

Junos, Associate (OS 21.2)

Questions & Answers (Demo)

Version: 4.0

Question: 1

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: 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.

Reference: Routing Fundamentals, Route Preference Selection.

Question: 2

What is the purpose of an ARP packet?

A. to determine the MPLS label of a given IP address

B. to determine the IP address of a given URL

C. to determine the MAC address of a given IP address

D. to determine the IP address of a given MAC address

Answer: C

Explanation:

The Address Resolution Protocol (ARP) is a fundamental Layer 2 utility used within the IPv4 suite to resolve a known network-layer (Layer 3) address to its corresponding physical media access control (MAC) or hardware address (Layer 2). In a typical Ethernet environment, when a Junos device needs to forward a packet to a next-hop on a local subnet, the Packet Forwarding Engine (PFE) requires the destination MAC address to properly encapsulate the frame.

The process begins with an ARP Request, which is broadcast to all hosts on the segment asking, "Who owns this IP address?" The host assigned that specific IP responds with an ARP Reply containing its MAC address. The Junos device then stores this mapping in its ARP cache (viewable via the show arp command) to avoid repeated broadcasts for subsequent packets. This resolution is essential because while IP addresses facilitate end-to-end logical routing, the actual delivery of data across a physical wire or switch fabric relies entirely on hardware addresses. Without successful ARP resolution, the device cannot complete the Layer 2 header, and the traffic will be dropped as "encapsulation failed."

Reference: Networking Fundamentals, Ethernet and Address Resolution Protocol.

Question: 3

Which protocol provides secure remote CLI access to a Junos device?

A. FTP

B. SNMP

C. Telnet

D. SSH

Answer: D

Explanation:

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.

Question: 4

You want to automatically back up your Junos device configuration to an external server every time you commit a configuration change. In this scenario, which command would accomplish this task?

A. set system commit synchronize

B. set system archival configuration transfer-interval

C. set system archival configuration transfer-on-commit

D. set system archival configuration archive-sites

Answer: C

Explanation:

Junos OS provides robust automation features for configuration management, specifically through the system archival utility. When an administrator needs to ensure that every successful configuration change is mirrored to an off-box repository for disaster recovery or auditing, the transfer-on-commit statement is the appropriate tool. This command instructs the Junos device to initiate an automated upload process immediately following the validation and activation of a commit command.

To fully implement this, the administrator must also define the archive-sites, which specify the destination URIs (using protocols such as FTP, SCP, or HTTP) and the necessary credentials for the external server. While transfer-interval can be used to back up configurations on a chronological schedule (e.g., every 60 minutes), transfer-on-commit is superior for tracking specific change events as they happen. This ensures that the external backup is always synchronized with the current active configuration on the device. Once configured, the device handles the background transfer, allowing

the administrator to maintain a historical record of configuration states without manual intervention, which is essential for large-scale operational environments.

Reference: Configuration Basics, Managing Configurations, System Archival.

Question: 5

Which statement describes the primary purpose of a routing policy in Junos OS?

A. It controls which routes are accepted or advertised by a routing protocol. B. It determines the physical interface used for forwarding traffic. C. It sets the maximum number of routes in the routing table. D. It enables automatic rollback of routing changes.

Answer: A

Explanation:

In Junos OS, a routing policy is a powerful tool used to manage the flow of routing information between the Routing Information Base (RIB) and routing protocols. Unlike forwarding decisions, which are handled by the Packet Forwarding Engine, routing policies function within the control plane on the Routing Engine. Their primary purpose is to define specific criteria for importing routes into the routing table from neighbors or exporting routes from the routing table to neighbors.

Routing policies consist of terms containing from (match) and then (action) statements. They allow administrators to filter prefixes (e.g., denying specific BGP routes), modify route attributes (e.g., changing OSPF metrics or BGP communities), and manipulate path selection behavior. For example, an export policy might be used to ensure that only specific internal subnets are advertised to an ISP via BGP, preventing the accidental leakage of private infrastructure addresses. By default, Junos applies "default policies" for each protocol (such as OSPF accepting all OSPF routes), but custom policies allow for granular control over how the device interacts with the rest of the network. This ensures that the routing table contains only the desired paths for optimal traffic engineering.

Reference: Routing Policy and Firewall Filters, Policy Framework.