DUMPSARENA

DesignAssociate (JNCIA-Design)

Juniper JN0-1103

Version Demo

Total Demo Questions: 8

Total Premium Questions: 85

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Design Methodology	8
Topic 2, Network Design Fundamentals	24
Topic 3, Network Design	25
Topic 4, Juniper Networks Design	28
Total	85

QUESTION NO: 1

As a network architect, in which three areas would you add MX Series routers? (Choose three.)

A. mobile device

B. data center network

C. service provider

D. edge network

ANSWER: B C D

Explanation:

MX Series routers are designed for high-capacity routing roles at major network aggregation and interconnection points. A data center network is an appropriate deployment area because MX platforms provide high-density interfaces, scalable routing, and data center interconnect capabilities for connecting facilities and cloud environments. Service provider networks commonly use MX routers in access, aggregation, edge, and core roles; the family supports carrier-grade routing, MPLS, segment routing, broadband subscriber services, and extensive peering capacity. An edge network is also a strong fit because MX routers can apply routing policy, traffic engineering, services, and secure connectivity where customer, branch, access, or external networks meet the wider WAN or Internet. These roles benefit from the MX family's scale, high availability, and broad transport support. Juniper describes the MX Series as a portfolio for service-provider, cloud, and enterprise WAN deployments, with applications spanning edge, core, and data center environments. See the Juniper MX Series routers overview and the MX Series overview documentation.

QUESTION NO: 2

Your organization is adopting SaaS applications for remote and branch users. The security design must block access to inappropriate Web destinations and prevent sensitive corporate information from being uploaded to unsanctioned cloud applications.

Which two security capabilities should be included in the design? (Choose two.)

A. Cloud Access Security Broker

B. WAN optimization

C. Secure Web Gateway

D. OSPF authentication

ANSWER: A C

Explanation:

Secure Web Gateway provides policy enforcement for Internet and Web access. It can apply URL and content controls to prevent users from reaching prohibited or risky destinations.

Cloud Access Security Broker provides visibility and policy control for cloud-service use. CASB capabilities can identify cloud applications and help enforce data-protection policies for sensitive information accessed or shared through SaaS services. A WAN optimization service improves application delivery but does not provide the required Web and cloud-data security controls, while a routing protocol does not enforce user-security policy.

QUESTION NO: 3

You are preparing a brownfield network redesign. The customer requires that existing business services remain available during the migration.

Which two activities should be completed before selecting the target architecture? (Choose two.)

A. Document the existing topology and service dependencies.

B. Select the target platforms before reviewing the current environment.

C. Identify maintenance windows and rollback requirements.

D. Remove legacy services before determining their dependencies.

E. Validate the design only after the complete migration.

ANSWER: A C

Explanation:

Documenting the existing topology and dependencies is necessary because a brownfield design must account for current connectivity, routing relationships, security policies, applications, and service dependencies. Without this information, a proposed change can unintentionally disconnect a required service.

Identifying maintenance windows and rollback requirements is also necessary because service continuity constrains how the new design can be introduced. A sound migration plan defines when disruptive work can occur, how each phase will be validated, and how service can be restored if a change does not perform as intended.

Selecting platforms before discovery can lead to a design that does not meet existing constraints. Removing legacy services before understanding their dependencies is risky, and delaying validation until after migration does not protect production services.

QUESTION NO: 4

Where are path selections made for an SD-WAN router?

A. physical interface card

B. local packet forwarding engine

C. local routing engine

D. centralized controller

ANSWER: C

Explanation:

local routing engine is correct because an SD-WAN router makes its forwarding-path decisions locally, using the routing, application, and SLA policy information that it has received from the centralized management and control infrastructure. The controller centrally defines and distributes policy, while each router evaluates locally available paths and current path characteristics, such as loss, latency, and jitter, to steer traffic according to that policy. This local decision process is essential to SD-WAN operation: it allows the router to react quickly to changing WAN conditions without needing to query a controller for every traffic flow or packet. In Juniper SD-WAN designs, centralized components provide orchestration, configuration, and policy distribution, but the branch or edge router performs the real-time path selection needed for resilient application delivery. This distributed intelligence also preserves forwarding continuity when connectivity to centralized management is temporarily unavailable. Juniper describes its Session Smart routing architecture as using routers that make intelligent forwarding decisions based on policy and network conditions. See Juniper Session Smart Router and Juniper Session Smart Router Documentation.

QUESTION NO: 5

You are designing a campus network for a financial-services organization. The customer requires access-layer connectivity to remain available if a single distribution switch fails.

Which design choice best satisfies this requirement?

A. Connect each access switch to two distribution switches.

B. Connect each access switch to a larger distribution switch.

C. Increase the bandwidth of each access-to-distribution uplink.

D. Add additional access switches in each wiring closet.

ANSWER: A

Explanation:

Connecting each access switch redundantly to two distribution switches is the best design choice. This removes the distribution switch as a single point of failure and permits the access layer to retain an upstream path when one distribution device is unavailable. The design must also use an appropriate redundancy mechanism and routing or switching design to ensure that the surviving path can forward traffic.

Adding more access switches increases port density but does not protect an existing access switch from loss of its only distribution uplink. A larger distribution switch may provide additional capacity, but it remains a single failure domain. Using a single higher-bandwidth uplink improves performance but does not provide device or path redundancy.

QUESTION NO: 6

You are asked to design an enterprise network.

In this scenario, which two product families are appropriate to deploy in the distribution layer according to Juniper Networks? (Choose two.)

A. QFX

B. SRX

C. ACX

D. EX

ANSWER: A D

Explanation:

QFX and **EX** are appropriate product families for an enterprise distribution layer. This layer aggregates access-layer connections, provides high-capacity switching, and commonly supplies Layer 3 gateway and routing functions for multiple VLANs or subnets. QFX switches are designed for high-performance, scalable Ethernet switching and can be deployed where the distribution tier requires substantial port density, uplink bandwidth, resilient architectures, or virtual-chassis and fabric-based designs. EX switches provide enterprise-class access and aggregation capabilities, including Layer 2 and Layer 3 switching, routing, and redundancy features that make them suitable for distribution deployments of varying sizes. Both families run Junos OS, supporting consistent operational practices and policy implementation across the campus design. Juniper's campus guidance positions switching platforms in the EX and QFX portfolios for building campus access, aggregation, and core connectivity, with the precise platform selected according to scale, interface requirements, and resiliency objectives. See Juniper's switching portfolio overview and the enterprise campus networking overview for platform roles and campus design context.

QUESTION NO: 7

Which aspect of network design facilitates future growth and troubleshooting efforts?

A. business continuity

B. high availability

C. modularity

D. security

ANSWER: C

Explanation:

modularity is correct because it organizes a network into smaller, clearly defined functional building blocks with well-understood roles and interfaces. A modular design lets an organization expand capacity or introduce services by modifying or adding the relevant module rather than redesigning the entire network. This supports future growth in a controlled, repeatable way and limits the operational impact of changes.

Modularity also makes troubleshooting more efficient. Because functions and boundaries are deliberately separated, engineers can isolate a fault domain, verify behavior at module interfaces, and focus diagnostic work on the affected portion of the design. Standardized modules encourage consistent configurations, documentation, and operational procedures, which further reduces the time needed to identify and remediate issues. These characteristics are central to scalable network architecture: growth can occur incrementally, and failures can be contained and investigated without unnecessary disruption to unrelated services. Juniper's design certification track emphasizes the design skills used to create scalable, resilient network solutions; see the Juniper Networks Design certification track. For additional Juniper design and architecture resources, see Juniper enterprise networking solutions.

QUESTION NO: 8

Which VPN protocol has the highest overhead?

A. GRE over MPLS

B. IPsec with NAT Traversal

C. Secure Vector Routing

D. IPsec without NAT Traversal

ANSWER: B

Explanation:

IPsec with NAT Traversal is correct because NAT-T adds a UDP encapsulation layer to an IPsec ESP packet so that the protected traffic can traverse devices performing network address translation. In tunnel mode, IPsec already adds an outer IP header plus ESP-related fields, including an ESP header, initialization vector or nonce as required by the selected encryption algorithm, padding, trailer, and integrity data when used. NAT-T adds a UDP header outside ESP, and packets normally use UDP destination port 4500. This additional encapsulation increases the per-packet byte overhead beyond IPsec ESP without NAT-T. The practical design consequence is a reduced effective payload size for a given physical MTU. Designers should account for this reduction when choosing tunnel MTUs and TCP MSS-clamping values, especially where fragmentation, path-MTU discovery limitations, or applications that send near-MTU packets may be present. Juniper documents NAT traversal as UDP encapsulation of IPsec traffic to support communication through NAT devices. The UDP encapsulation format and use of port 4500 are standardized in RFC 3948; Juniper's implementation guidance is available in the IPsec NAT Traversal documentation.