Cisco
300-420
Designing Cisco Enterprise Networks (ENSLD)

Latest Version: 21.0

Question: 1

Which solution allows overlay VNs to communicate with each other in an SD-WAN Architecture?

A. External fusion routers can be used to map VNs to VRFs and selectively route traffic between VRFs.
B. GRE tunneling can be configured between fabric edges to connect one VN to another.
C. SGTs can be used to permit traffic from one VN to another.
D. Route leaking can be used on the fabric border nodes to inject routes from one VN to another.

Answer: A

Explanation:
Cisco SD-Access uses virtual networks as macro-segmentation boundaries, and those VNs are represented as VRF instances in the fabric. By design, separate VNs do not communicate directly inside the overlay unless the design introduces controlled inter-VN routing. Cisco SD-Access designs commonly use an external fusion router, firewall, or shared-services device to map fabric VNs to external VRFs and selectively exchange routes between them. That is the correct design because it preserves segmentation while allowing policy-controlled access to shared resources or selected networks. GRE tunnels between fabric edges are not the normal SD-Access inter-VN communication method and would bypass the intended fabric policy model. Security Group Tags provide microsegmentation within or across policy domains, but SGTs do not by themselves leak routes between separate virtual networks. Route leaking on fabric border nodes is not the recommended standalone answer here because inter-VN communication is normally provided through a fusion device or firewall outside the fabric. Therefore, the correct solution is external fusion routing with controlled VRF route exchange.

Question: 2

An engineer must design a VPN solution for a company that has multiple branches connecting to a main office. What are two advantages of using DMVPN instead of IPsec tunnels to accomplish this task? (Choose two.)

A. support for AES 256-bit encryption
B. greater scalability
C. support for anycast gateway
D. lower traffic overhead
E. dynamic spoke-to-spoke tunnels

Answer: B E

Explanation:
DMVPN is preferred over individually configured point-to-point IPsec tunnels when a company has many branches because it scales the overlay more efficiently. A traditional IPsec tunnel design requires manual or template-based tunnel definitions for every required site-to-site relationship. As branches increase, tunnel count, configuration complexity, and operational overhead grow quickly. Cisco DMVPN combines multipoint GRE, NHRP, and IPsec so spokes can register with the hub and dynamically discover next-hop information for other spokes. This supports a hub-and-spoke control model while allowing dynamic spoke-to-spoke data tunnels when branch-to-branch traffic is required. That is why greater scalability and dynamic spoke-to-spoke tunnel creation are the two design advantages. AES-256 encryption is not unique to DMVPN because normal IPsec can also use strong encryption. Anycast gateway is unrelated to DMVPN WAN overlay design. Lower traffic overhead is not the best answer because DMVPN adds mGRE, NHRP, and IPsec encapsulation overhead; its advantage is operational scalability and dynamic tunnel establishment.

Question: 3

Which NETCONF operation creates filtering that is specific to the session notifications?

A. <create-subscription>
B. <commit>
C. <notification>
D. <logging>

Answer: A

Explanation:
NETCONF supports event notifications through a subscription model. The operation used to establish a notification subscription is create-subscription. When a client sends this operation, it can specify the stream and optional filters that determine which notifications are delivered to that NETCONF session. This is why create-subscription is the operation associated with session-specific notification filtering. The commit operation is used with the candidate configuration datastore to apply configuration changes to the running datastore; it does not create a telemetry or event subscription. The notification element is the message sent by the server after a subscription exists, not the operation used to create one. Logging is not a NETCONF operation in the protocol operation set. In Cisco model-driven management designs, NETCONF provides structured configuration and operational access using YANG data models, while notifications allow the management station to consume specific events without relying on repeated screen scraping or broad polling. Therefore, the correct operation for creating filtering specific to session notifications is create-subscription.

Question: 4

An enterprise customer has these requirements:
end-to-end QoS for the business-critical applications and VoIP services based on CoS marking.

flexibility to offer services such as IPv6 and multicast without any reliance on the service provider.
support for full-mesh connectivity at Layer 2.
Which WAN connectivity option meets these requirements?

A. VPWS
B. MPLS VPN
C. DMVPN
D. VPLS

Answer: D

Explanation:
The requirements point to a Layer 2 multipoint WAN service. VPLS provides an emulated Ethernet LAN across a provider network, allowing multiple sites to appear as if they are connected to the same Layer 2 domain. This supports full-mesh Layer 2 connectivity and preserves customer control over higher-layer services such as IPv6, multicast, routing protocols, and QoS markings. Because the provider delivers an Ethernet multipoint service, the enterprise can retain protocol independence rather than depending on the service provider to participate in IPv6 routing or multicast routing. CoS marking is also a Layer 2 QoS mechanism, so a Layer 2 VPN service is better aligned to the stated QoS requirement. VPWS is point-to-point rather than full-mesh multipoint, so it does not meet the topology requirement by itself. MPLS Layer 3 VPN is a provider-routed service and does not give the customer full Layer 2 mesh behavior. DMVPN is an overlay routed VPN and does not provide a native Layer 2 full-mesh service. Therefore, VPLS is the correct WAN connectivity option.

Question: 5

What is a benefit of using VRRPv3 as compared to VRRPv2?

A. VRRPv3 supports IPv4 and IPv6
B. VRRPv3 supports authentication
C. VRRPv3 supports preemption
D. VRRPv3 supports stateful switchover

Answer: A

Explanation:
VRRPv3 improves protocol applicability by supporting both IPv4 and IPv6 address families. VRRPv2 is associated with IPv4 virtual router redundancy, while VRRPv3 extends the protocol so the same firsthop redundancy concept can be used for IPv6 default gateways as well. In campus and branch designs, this matters because IPv6 deployments should not require a separate redundancy design from IPv4 when a standards-based FHRP is preferred. Preemption is not a unique VRRPv3 advantage because VRRP has long supported priority-based master election and preemption behavior. Authentication is also not the correct differentiator in this comparison; VRRPv3 removed the simple protocol authentication field from the base protocol and expects security to be provided by the underlying network or IPsec where required. Stateful switchover is a platform high-availability

capability, not a VRRPv3 protocol feature. Therefore, the key benefit of VRRPv3 over VRRPv2 for enterprise design is IPv4 and IPv6 support under the same redundancy protocol model.

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer