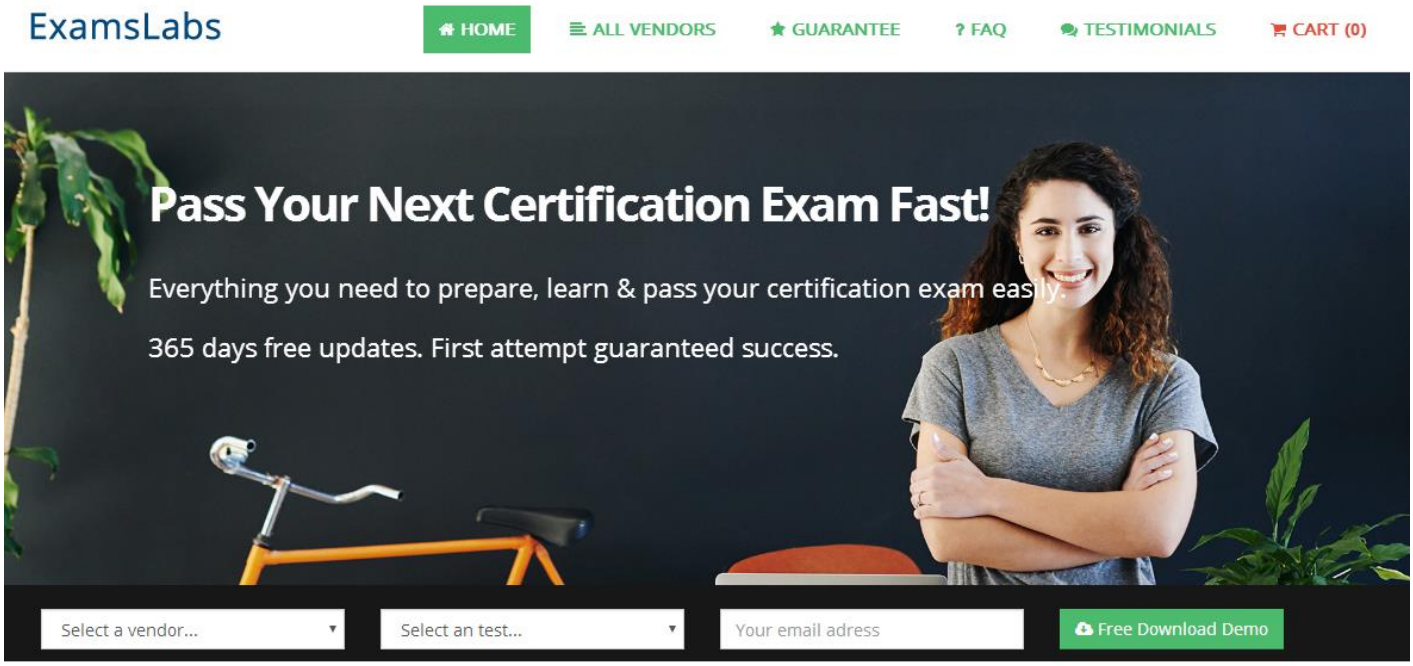
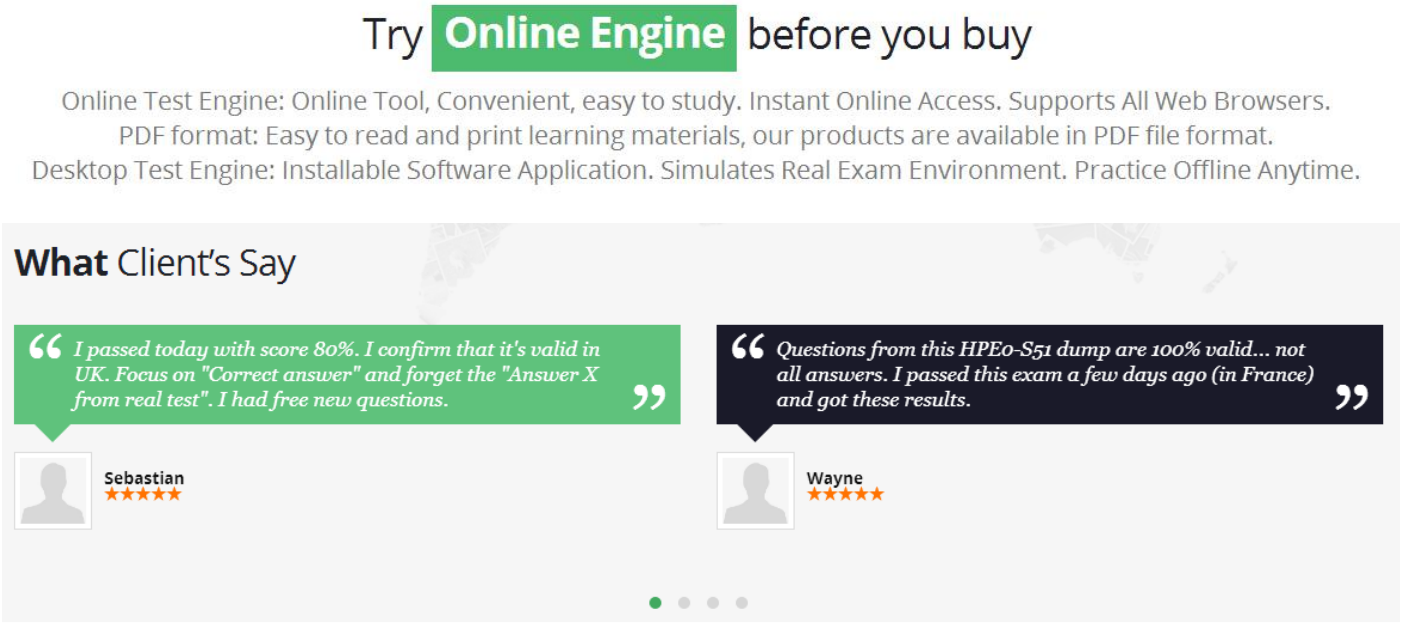
ExamsLabs





http://www.examslabs.com/

Latest Study Materials, Valid Dumps - ExamsLabs

Exam : **JN0-650**

Title : Enterprise Routing and Switching, Professional (JNCIP-ENT)

Vendor : Juniper

Version : DEMO

NO.1 Your Layer 2 network uses 802.1X to authenticate user devices connecting to the network. You are asked to include a new Layer 2 interface connection from the conference room in your network. You must ensure that only a single device is allowed to authenticate on this port at one time to avoid users from being able to plug in a rogue switch to this port.
In this scenario, which 802.1X method would you use for the new interface?

A. single-secure supplicant mode

B. multiple supplicant mode

C. single supplicant mode

D. MAC-RADIUS

Answer: A

Explanation:
This question focuses on port security and preventing " rogue switches " or multiple devices from accessing a single physical port simultaneously.
Single-Secure Supplicant Mode (Option A): This is the most restrictive 802.1X mode in Junos OS. It allows exactly one MAC address to be authenticated on the port at a time. If a device successfully authenticates, the switch will drop any traffic coming from any other MAC address on that same physical interface. If a user tries to plug in a switch, only the first device that authenticates will have access; all other devices behind that switch will be blocked.
Single Supplicant Mode (Option C): This mode allows the first authenticated user to " open " the port for all other users. This would actually allow a rogue switch to function once the first device is authorized.
Multiple Supplicant Mode (Option B): This allows multiple devices to connect, provided each one authenticates individually. While secure, it does not prevent a user from connecting multiple devices to the port, which violates the requirement to allow only one.
MAC-RADIUS (Option D): This is an authentication method, not a port-access mode that limits the number of supplicants.

NO.2 You want to implement a system in your network to simplify VLAN management that can also dynamically create and prune VLANs. How would you accomplish this task?

A. Enable GVRP on access interfaces.

B. Enable MVRP on access interfaces.

C. Enable MVRP and GVRP on all interfaces.

D. Enable MVRP on trunk interfaces.

Answer: D

NO.3 Which two statements are correct about OSPFv2 and OSPFv3? (Choose two.)

A. OSPFv3 is processed per subnet.

B. OSPFv2 and OSPFv3 require an Area 0.

C. OSPFv2 carries prefix information in LSAs

D. OSPFv3 carries flooding scope in LSAs.

Answer: B,D

NO.4 Exhibit.

Referring to the exhibit, you see that the 0.0.0.0/0 route is coming from AS 64512.
What is the command to achieve this task?

A. show route receive-protocol bgp < peer ip >

B. show route protocol bgp source-gateway < peer ip >

C. show route protocol bgp next-hop < peer ip >

D. show route receive-protocol bgp < peer ip > hidden

Answer: D

Explanation:

The exhibit shows a BGP routing process where an Import Policy is being applied to routes received in the RIB-IN. Specifically, Policy 1 states: " Reject 0.0.0.0/0 from AS 64512. " In Junos OS, when a routing policy rejects a route, that route is not placed in the main routing table (inet.0) for active use. Instead, it becomes a hidden route. To verify that a specific peer is actually sending a route that is subsequently being rejected by your policy, you must use specific diagnostic commands:

Understanding " Hidden " Routes: When a BGP route is received but fails to meet policy requirements (or has an unreachable next-hop), Junos keeps it in the BGP RIB-IN but marks it as " hidden. " It will not appear in a standard show route command.

Command Logic (Option D): The command show route receive-protocol bgp < peer ip > hidden allows an administrator to view all routes received from a specific neighbor, including those that were rejected by import policies.

show route receive-protocol bgp < peer ip > : Shows only the routes that passed the import policy and were accepted into the table. Since the 0.0.0.0/0 route from AS 64512 is explicitly rejected in the exhibit, it would not show up here.

Adding the hidden keyword is the essential step to see the rejected default route and verify that AS 64512 is indeed sending it before the policy drops it.

Other Options:

Option A is incorrect because it only shows accepted routes.

Option B and C are used to filter the existing active routing table based on gateway or next-hop attributes, but they cannot show routes that have been rejected and excluded from that table.

NO.5 Your existing enterprise network uses OSPFv3 on Juniper devices. You need to extend the networking into a new building, and it needs to be in its own OSPF area. Your team is debating about making the area a stub Which two statements are correct in this scenario? (Choose two.)

A. Stub areas can have an ASBR

B. Stub areas can also be not-so-stubby areas.

C. Stub areas do not support virtual links.

D. Stub areas can be converted into totally stubby areas.

Answer: C D

Explanation:

OSPF stub areas are used to reduce the size of the Link-State Database (LSDB) in routers with limited resources by restricting the flooding of external routes.

Virtual Links (Option C): According to OSPF standards (both v2 and v3), virtual links cannot pass through stub areas. A virtual link must transit a " transit area, " which must be a standard (non-stub) area with a full routing table.

Totally Stubby Areas (Option D): A stub area (which blocks Type 5 External LSAs) can be further restricted into a totally stubby area. In Junos OS, this is done by adding the no-summaries statement to the stub configuration. This blocks both Type 5 and Type 3 (Inter-area) LSAs, replacing them with a single default route.

Incorrect Statements: Option A is incorrect because standard stub areas cannot contain an ASBR; only Not-So- Stubby Areas (NSSA) allow for an ASBR. Option B is incorrect because an area is either a Stub or an NSSA; they are mutually exclusive configurations for the same area.

NO.6 When configuring Q-in-Q tunneling, which type of tunneling involves the swapping of S-VLANs with C- VLANs?

A. L2PT

B. many-to-many

C. VLAN rewrites

D. all-in-one

Answer: C

Explanation:

In a Juniper Q-in-Q (Layer 2 tunneling) environment, VLAN rewrites (specifically the swap operation) provide the most granular control over how customer traffic (C-VLANs) is mapped to service provider traffic (S-VLANs).

* VLAN Rewrites (The Swap Operation): This method involves replacing the incoming customer VLAN tag with a service provider tag as the frame enters the tunnel. This is technically a " swap " because the original C-VLAN tag is removed and the S-VLAN tag is written in its place. At the egress of the tunnel, the S-VLAN tag is swapped back for the original C-VLAN tag. This is often used when different customers use the same C-VLAN IDs and the provider needs to keep them unique within their core.
* Many-to-Many: This is a mapping style where multiple customer VLANs are mapped to multiple service provider VLANs, but it typically relies on the " push " (stacking) operation rather than a literal " swap " of the tag itself.
* All-in-One: This is the simplest form of Q-in-Q where all traffic entering an interface is " pushed " into a single S-VLAN tag, regardless of any existing C-VLAN tags. No swapping occurs; the original tags are simply buried under the new provider tag.
* L2PT (Layer 2 Protocol Tunneling): This is a feature used to tunnel Layer 2 control protocols (like STP, CDP, or LLDP) across a provider network by encapsulating them or changing their destination MAC addresses. It does not involve the swapping of VLAN tags.

NO.7 You are configuring CoS throughout your enterprise network using DSCP. You have configured

MF classification on your edge devices and are using BA classifiers throughout the core You are using the EZQoS template provided on your EX Series switches that are acting as your edge devices. You have loaded the configuration group and applied it to the appropriate interfaces. Classification and scheduling are working properly on your edge devices; however, traffic is not being classified correctly when it reaches your core devices In this scenario, which statement is correct about solving this problem?

A. You should configure and apply a policer to the edge devices ' egress interfaces toward the core.

B. You must configure the core devices using the EZQoS template as well

C. You should configure and apply rewrite rules on the edge devices ' egress interfaces toward the core

D. You must configure the edge devices to use BA classifiers instead of MF classifiers

Answer: C

Explanation:

In an end-to-end CoS (Class of Service) design, there is a clear distinction between classification at the ingress and rewrite rules at the egress.

The Problem: Your edge devices are successfully classifying traffic (assigning packets to internal forwarding classes). However, the core devices-which use BA (Behavior Aggregate) classifiers-are not classifying correctly. BA classifiers look at the bits in the packet header (like DSCP or 802.1p) to determine priority.

The Missing Link (Option C): When a packet leaves the edge device, its internal forwarding class and loss priority must be " written " back into the packet header so that the next-hop (the core device) can see it. By default, Junos may not preserve or set these bits correctly on egress. You must apply rewrite rules on the edge switches ' egress interfaces facing the core. These rules ensure the DSCP values in the headers match the forwarding class determined by the edge ' s MF classifier, allowing the core ' s BA classifier to function properly.

Other Options: Option A (policer) handles rate limiting, not classification. Option B is incorrect because core devices often have different hardware or scaling needs than edge switches, and standard BA configuration is preferred over templates in the core. Option D is incorrect because MF classifiers are standard for edge devices where deep packet inspection is needed to identify traffic types.