Pass2Certify.com
Prepare, Practice, & Pass.

Juniper

JN0-650

ExamName: Enterprise Routing and Switching, Professional

Exam Version: 8.2

Questions & Answers Sample PDF

(Preview content before you buy)

Check the full version using the link below.

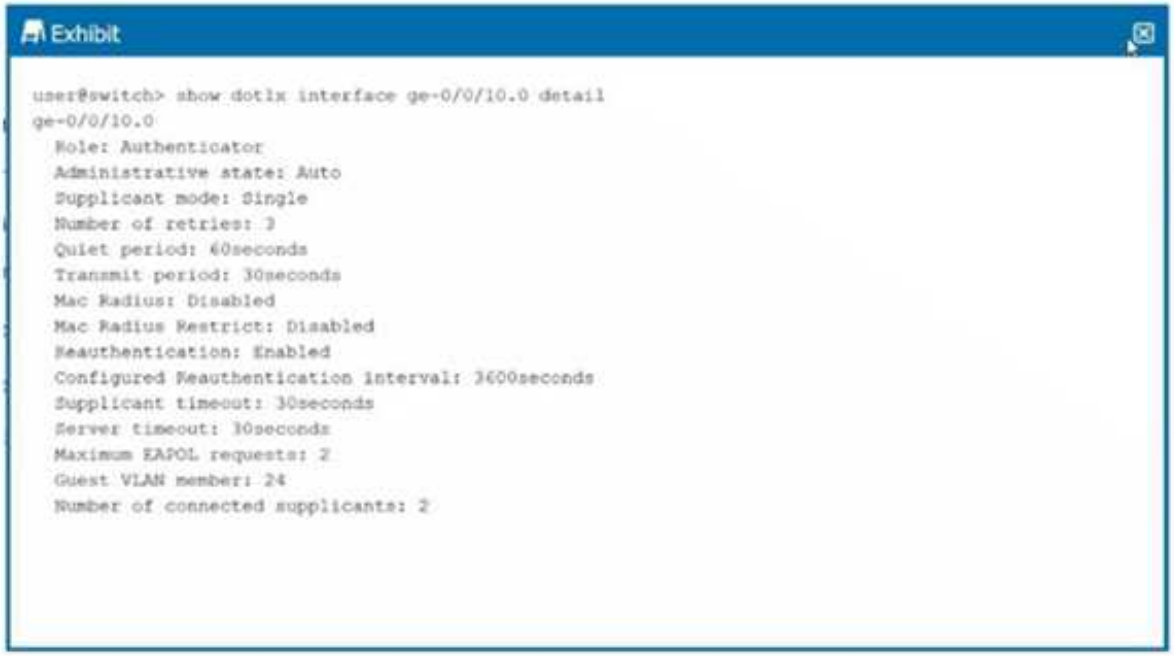
https://pass2certify.com/exam/jn0-650

Unlock Full Features:

Stay Updated: 90 days of free exam updates
Zero Risk: 30-day money-back policy
Instant Access: Download right after purchase
Always Here: 24/7 customer support team

Question 1. (Single Select)

Exhibit.



You want to limit port access to only one device at a time. Referring to the exhibit, which configuration change will accomplish this task?

A: Enable MAC RADIUS restrict.
B: Change the supplicant mode to multiple.
C: Change the supplicant mode to single-secure.
D: Change the maximum EAPOL request to l.

Answer: C

Explanation:
In Junos OS, the supplicant-mode configuration under protocols dot1x determines how the switch handles multiple MAC addresses on a single physical port. According to the exhibit, the current mode is set to Single, and the Number of connected supplicants is 2. This indicates that the port is currently allowing multiple devices, which contradicts the goal of limiting access to only one device at a time.
Here is the breakdown of why Option C is the correct solution based on Juniper's standard behavior:
Supplicant Mode: Single (Current State): In this mode, the first device to authenticate opens the port for all

subsequent devices. As long as the first device remains authenticated, other devices can send traffic through the port without individual authentication. This is why the exhibit shows 2 connected supplicants despite the mode being "Single."
Supplicant Mode: Single-Secure (The Solution): This mode strictly limits the port to only one MAC address. Once a device successfully authenticates via 802.1X, the switch drops any traffic coming from any other MAC address on that port. If the authenticated device logs off or the session times out, the port becomes available for a new device, but never more than one simultaneously. * Supplicant Mode: Multiple (Option B): This mode allows multiple supplicants to authenticate individually. Each MAC address must go through its own authentication process. This would allow more than one device, which is the opposite of the user's requirement.
MAC RADIUS Restrict (Option A): This feature is used to force MAC-based authentication and does not inherently limit the number of devices to one in the same way that changing the supplicant mode does.
Maximum EAPOL requests (Option D): This parameter defines how many times the switch will send an EAP-Request/Identity frame to a supplicant before giving up. Changing this to 1 does not restrict the number of devices allowed on the port; it only changes the retry logic for a single authentication attempt.
Configuration Example for Junos OS 24.4: To implement this change, you would use the following command: set protocols dot1x edit interface ge-0/0/10.0 supplicant-mode single-secure

Question 2. (Multi Select)

Your OSPF network consists of a mix of 1GbE and 10GbE interfaces. By default, all interfaces have the same cost in your OSPF network. You are asked to ensure that the 10GbE interfaces are more preferred when available

In this scenario, which two statements would accomplish this behavior? (Choose two.)

A: You should define the reference bandwidth as 10G. which will assign the 1GbE interfaces a higher cost
B: You should manually assign the interface metric for each 10GbE interface to be higher than the 1GbE interfaces in your OSPF network.
C: You should define the reference bandwidth as 1G. which will assign the 1GbE interfaces a higher cost.
D: You should manually assign the interface metric for each 1GbE interface to be higher than the 10GbE interfaces in your OSPF network.

Answer: A, D

Explanation:

OSPF determines the best path to a destination by calculating the metric (cost) of each link. By default, Junos OS uses a reference bandwidth of 100 Mbps to calculate this cost using the formula:

$$Cost = \frac{\text{Reference Bandwidth}}{\text{Interface Bandwidth}}.$$

When the reference bandwidth is left at the default 100 Mbps, any interface with a speed of 100 Mbps or higher (including 1 GbE and 10 GbE) is assigned a cost of 1 because the minimum OSPF cost is 1. This results in equal-cost paths, preventing the router from preferring the faster 10 GbE link. To ensure 10 GbE interfaces are preferred, you must create a cost differential: Option A (Reference Bandwidth): By increasing the reference bandwidth to 10G (or higher), the calculation changes. For a 10 GbE link, the cost becomes $10,000 / 10,000 = 1$. For a 1 GbE link, the cost becomes $10,000 / 1,000 = 10$. Since OSPF prefers the path with the lowest cumulative cost, the 10 GbE link is now preferred. Option D (Manual Metric): You can manually override the automatic cost calculation by assigning a higher metric specifically to the 1 GbE interfaces. If a 1 GbE interface is manually set to a cost of 50 and the 10 GbE interface remains at 1 (or is set to a lower value), the router will prioritize the 10 GbE path. Option B is incorrect because a higher metric makes a path less preferred. Option C is incorrect because a 1G reference bandwidth would still result in both 1 GbE and 10 GbE interfaces having a cost of 1.

Question 3. (Multi Select)

Which two statements correctly describe how EX Series switches use captive portal for Layer 2 authentication? (Choose two.)

A: The captive portal is the default Layer 2 authentication method that is applied before other methods such as 802 1X or MAC RADIUS.
B: The captive portal authentication allowlist works for devices that do not have HTTP capabilities.
C: The captive portal is configured on Layer 3 interfaces and does not participate in Layer 2 authentication on EX Series switches.
D: The captive portal is used as a fallback mechanism for clients that fail 802.1X or MAC RADIUS authentication.

Answer: B, D

Explanation:

In Junos OS 24.4, Captive Portal is used as a web-based authentication method for Layer 2 network access control, often in environments where 802.1X is not feasible for all users.

Fallback Mechanism (Option D): On EX Series switches, Juniper supports a flexible authentication order. By default, the switch attempts authentication in the order of 802.1X, then MAC RADIUS, and finally Captive Portal. If a client fails both 802.1X and MAC RADIUS, the switch can fall back to Captive Portal to redirect the user to a login page.

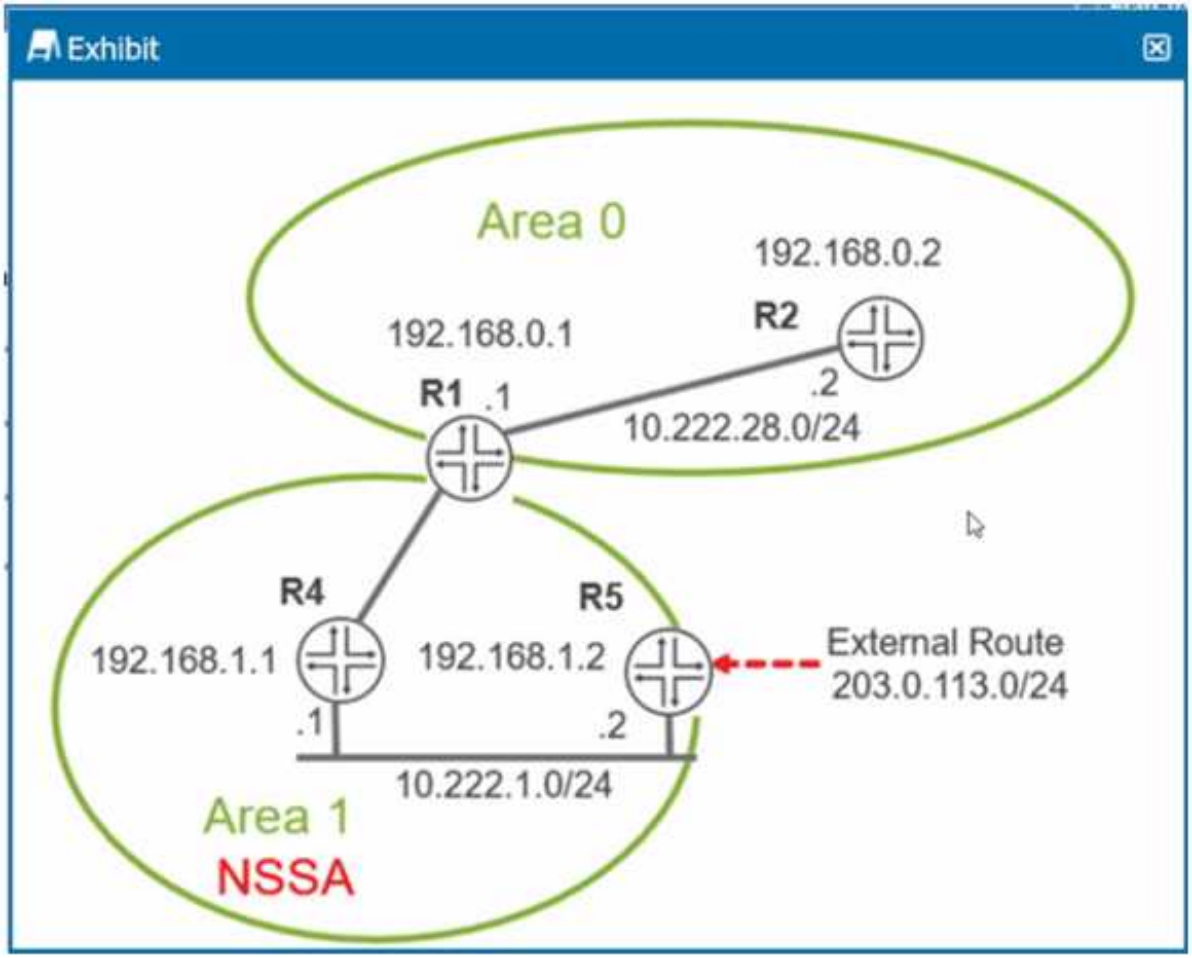
MAC Allowlist (Option B): Captive Portal relies on intercepting HTTP/HTTPS traffic to redirect users. However, "headless" devices like printers or cameras lack web browsers and cannot interact with the portal. To accommodate these, Junos allows administrators to configure an authentication allowlist (or whitelist), which identifies these devices by their MAC addresses and permits them to bypass the portal entirely.

Precedence (Option A): This is incorrect because Captive Portal is generally the last method in the default sequence, not the first.

Layer 2 Participation (Option C): While Captive Portal requires a Layer 3 interface (RVI/IRB) for the redirection process, it is explicitly used to control Layer 2 access on EX Series switches.

Question 4. (Multi Select)

Exhibit.



Referring to the exhibit, which two statements are correct? (Choose two.)

A: R1 will advertise the 203 0.113.0724 route as an OSPF Type 7 LSA into Area 0.
B: R5 will advertise the 203 0.113 0/24 route as an OSPF Type 5 LSA into Area 1.
C: R1 will advertise the 203 0.113.0/24 route as an OSPF Type 5 LSA into Area 0
D: R5 will advertise the 203 0.113.0/24 route as an OSPF Type 7 LSA into Area 1.

Answer: C, D

Explanation:

The exhibit shows an OSPF network where Area 1 is configured as a Not-So-Stubby Area (NSSA). R5 is an Autonomous System Boundary Router (ASBR) injecting an External Route (203.0.113.0/24) into this area.

NSSA ASBR Behavior (Option D): Within an OSPF NSSA, external routes cannot be advertised as standard Type 5 LSAs because stubby areas do not support them. Instead, the ASBR (R5) advertises the external prefix using a Type 7 LSA (NSSA External LSA). This LSA is flooded throughout Area 1.

ABR Translation Behavior (Option C): When the Type 7 LSA reaches the Area Border Router (R1), the ABR

is responsible for translating it into a Type 5 LSA (AS External LSA). This allows the external route to be propagated into the backbone (Area 0) and subsequently to the rest of the OSPF domain.
Incorrect Statements (A & B): Option A is incorrect because Type 7 LSAs are local to the NSSA and are never advertised into Area 0. Option B is incorrect because Type 5 LSAs are strictly prohibited within an NSSA.

Question 5. (Multi Select)

You are deploying a new campus switching environment using EX Series switches. This new environment includes IP phones requiring Power over Ethernet (PoE) and end-user client PCs attached to a single switch port that will be configured with 802.1X authentication.

Considering the default configuration on an EX Series access switch and the configuration requirements to support this deployment, which two statements are correct? (Choose two.)

A: Configuration for the voice VLAN for all relevant access ports must be added.
B: Configuration for PoE on all relevant access ports must be added
C: Configuration for LLDP and LLDP-MED on all relevant access ports must be added.
D: Configuration for 802.1X on all relevant access ports must be added.

Answer: A, D

Explanation:
In a standard campus deployment on Juniper EX Series switches involving VoIP phones and 802.1X authentication, understanding the default behavior of Junos OS 24.4 is critical:
Voice VLAN (Option A): By default, an access port belongs to a single VLAN (the native or data VLAN). For an IP phone to operate correctly on the same physical port as a PC, a Voice VLAN must be explicitly configured and associated with the interface. This allows the switch to segregate voice traffic (usually tagged) from data traffic (untagged).
802.1X Configuration (Option D): Access ports do not have 802.1X authentication enabled by default. To enforce network access control for the client PCs, you must manually enable and configure the dot1x protocol on all relevant interfaces.
PoE Default (Option B): On EX Series switches that support PoE (like P or MP models), PoE is enabled by default on all PoE-capable ports. Therefore, additional configuration is generally not required unless you need to change power priorities or management modes.

LLDP Default (Option C): Standard LLDP is typically enabled by default in the factory configuration of most EX Series switches to facilitate neighbor discovery. While LLDP-MED is used for VoIP, the core requirement for "deploying" the described environment highlights the manual steps of VLAN and security setup rather than protocol discovery which often runs out-of-the-box.

Need more info? Check the link below:

https://pass2certify.com/exam/jn0-650

Thanks for Being a Valued Pass2Certify User!

Guaranteed Success Pass Every Exam with Pass2Certify.

Save $15 instantly with promo code

SAVEFAST

Sales: sales@pass2certify.com

Support: support@pass2certify.com