DUMPSBOSS.

Mist AI WirelessSpecialist (JNCIS-MistAI-Wireless)

Juniper JN0-452

Version Demo

Total Demo Questions: 13

Total Premium Questions: 139

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Wireless Fundamentals	43
Topic 2, WLAN Design	5
Topic 3, WLAN Implementation	27
Topic 4, WLAN Operations	29
Topic 5, Mist AI	35
Total	139

QUESTION NO: 1

Referring to the exhibit, what does the security alert indicate?

A. An AP that is not part of the Mist Org is connected to the same wired network as the Mist APs.

B. An AP that is not part of the Mist Org is launching a DDoS attack on the Mist APs.

C. An AP that is not part of the Mist Org is advertising the same SSIDs as the Mist APs.

D. An AP that is not part of the Mist Org is operating in the same RF channel as the nearby Mist AP.

ANSWER: C

Explanation:

An AP that is not part of the Mist Org is advertising the same SSIDs as the Mist APs. This security alert identifies a rogue AP presenting an SSID that matches one configured and broadcast by managed APs in the organization. Mist classifies this situation as a honeypot or evil-twin-style condition because an unauthorized nearby device can imitate the legitimate wireless network name and potentially entice clients to associate with it. Detecting this requires Mist APs to scan the RF environment and compare the SSIDs observed in beacon and probe-response frames with the SSIDs configured in the Mist organization. The alert gives administrators visibility into potential wireless impersonation so they can investigate the device's location, ownership, security configuration, and any risk to users who may attempt to join the familiar-looking network. This indication concerns the unauthorized AP's SSID advertisement, rather than proving that it is physically connected to the organization's wired network. Juniper's Mist documentation describes rogue, neighbor, and honeypot AP detection, including honeypots that advertise organization SSIDs, at Rogue, Neighbor, and Honeypot APs. Additional details on the alerting framework are available in the Mist Security Alerts documentation.

QUESTION NO: 2

You have deployed location services at a site and have installed an application which includes the Mist SDK on Bluetooth-only mobile client devices. The devices with the SDK-enabled app have Bluetooth enabled, but the devices do not appear in the Mist GUI under Clients/App Clients.

What is causing this problem?

A. There is BLE and Wi-Fi co-channel interference.

B. The clients are connected to the wrong WLAN.

C. The AP BLE radios do not hear the SDK-enabled client's BLE beacons.

D. The client devices are not connected to Wi-Fi or to a cellular data plan.

ANSWER: D

Explanation:

The correct answer is **"The client devices are not connected to Wi-Fi or to a cellular data plan."** The Mist SDK uses Bluetooth Low Energy to scan and use signals from the Mist AP infrastructure for location-related functionality, but the mobile application must also have an IP data connection to communicate its SDK data and application-client information with the Mist cloud. Bluetooth capability by itself does not provide the Internet connectivity needed for the SDK-enabled application to send telemetry or location updates to the cloud portal. Consequently, a device that is Bluetooth-only can participate in local BLE scanning, but it cannot be represented as an App Client in the Mist GUI unless it has a working Wi-Fi or cellular connection through which the app can reach Mist cloud services. Ensure the device can access the Internet, that the application is permitted to use network data, and that any firewall or proxy policy permits the required cloud communication. Juniper's Mist SDK documentation describes the SDK's role in enabling mobile-app location experiences and its integration with Mist cloud services: Mist SDK Overview. For additional deployment and SDK resources, see the Juniper Mist Documentation.

QUESTION NO: 3

Juniper Mist events are filtered into which three categories? (Choose three.)

A. organization

B. AP

C. security

D. client

E. site

ANSWER: B D E

Explanation:

Juniper Mist operational events are organized and filtered by the affected scope of the wireless environment: **AP**, **client**, and **site**. AP events identify activity and state changes associated with an access point, such as connectivity, reboot, radio, or configuration-related operational records. Client events follow events associated with an individual wireless endpoint, providing useful context for connection and service-delivery troubleshooting. Site events represent events with site-level context, allowing an administrator to review conditions and changes relevant to the broader location rather than a single AP or endpoint. These scopes make the Events view practical for narrowing investigations: an administrator can begin at the site level for environmental or infrastructure context, inspect AP-level records when an issue appears device-specific, or focus on the client event history to investigate an individual user experience. This event organization is part of Mist's operational monitoring workflow and complements the dashboard's broader AI-driven visibility and troubleshooting capabilities. Juniper's Mist documentation portal provides the product documentation and monitoring guidance at Juniper Mist Wi-Fi Documentation; the Mist documentation library is also available at Mist Documentation.

QUESTION NO: 4

Once a client discovers an access point, what is the correct order of steps for successful 802.1X authentication?

A. Open System Authentication - > 802.1X Authentication - > Association

B. Association - > 802.1X Authentication - > Open System Authentication

C. Association - > Open System Authentication - > 802.1X Authentication

D. Open System Authentication - > Association - > 802.1X Authentication

ANSWER: D

Explanation:

Open System Authentication - > Association - > 802.1X Authentication is the correct sequence because a station must first establish its basic IEEE 802.11 relationship with the access point before port-based network access control can begin. After discovering a suitable AP, the client performs Open System authentication, which is the initial 802.11 authentication exchange used by modern WPA/WPA2/WPA3 enterprise WLANs. The client then sends an association request and, once associated, has a controlled port through which EAP over LAN (EAPOL) traffic can be exchanged. The 802.1X process then starts: the client acts as the supplicant, the AP acts as the authenticator, and the authentication server—commonly RADIUS—validates the client's EAP credentials. Until that exchange succeeds, ordinary user data is not permitted through the controlled port. On a Mist WLAN configured for Enterprise security, this sequence enables the AP to broker EAP authentication to the configured RADIUS service and apply access policy after successful authentication. Juniper's WLAN security documentation describes Enterprise authentication and RADIUS integration at Juniper Mist WLAN Security. Juniper's 802.1X overview also describes the supplicant, authenticator, and authentication-server roles: Juniper 802.1X Authentication.

QUESTION NO: 5

What are two ways to access Marvis? (Choose two.)

A. Use the conversational assistant.

B. Use Actions.

C. Use Insights.

D. Use config templates.

ANSWER: A B

Explanation:

Marvis can be accessed through the conversational assistant and through Actions. The conversational assistant provides an interactive, natural-language interface in which an administrator can ask operational questions about the environment and receive AI-driven responses, troubleshooting guidance, and relevant network context. This interface is intended to make investigation faster by allowing users to express a problem or question directly rather than manually navigating through numerous dashboards and data views.

Actions provides the second access method. Marvis Actions presents proactively identified network issues, their scope, likely root cause, and recommended remediation steps. Administrators use Actions to review and prioritize problems surfaced by Marvis, such as client-connectivity, wireless, switching, WAN, or application experience issues. Together, these interfaces support both reactive investigation through conversational queries and proactive operations through AI-generated action items. Juniper describes Marvis AI as its AI-native virtual network assistant and identifies Marvis Actions as a core mechanism for delivering actionable network insights. See Juniper Marvis AI and Marvis Actions documentation.

QUESTION NO: 6

A packet capture is taken while a client obtains an IPv4 address through the normal DHCP DORA exchange.

Which two DHCP messages are originated by the client? (Choose two.)

A. DHCP Discover

B. DHCP Offer

C. DHCP Request

D. DHCP ACK

ANSWER: A C

Explanation:

The client originates the **DHCP Discover** message to locate available DHCP servers and the **DHCP Request** message to request the offered address and configuration. These are the first and third messages in the normal DORA sequence.

The DHCP server originates the Offer and ACK messages. Examining which side transmits each message helps identify whether a failure is occurring at the client, relay path, or DHCP server.

QUESTION NO: 7

Mist WLAN objects are configurable at which two levels? (Choose two.)

A. site group

B. organization

C. site

D. access point

ANSWER: A C

Explanation:

Mist WLAN objects are configured at the **site group** and **site** levels. A site group provides a reusable configuration scope for sites that share common wireless requirements. Administrators can define WLAN settings once in the site group and apply that configuration consistently to its member sites. This approach is particularly useful for standardizing SSIDs, authentication methods, VLAN assignments, and other WLAN policies across similar locations while reducing repeated administrative work.

The site level provides the local configuration scope for a specific physical location. It supports WLAN configuration tailored to that site's operational requirements and allows a site to receive the WLAN configuration associated with its applicable site group. Together, these levels provide both scalable, centralized policy reuse and site-specific wireless administration. Juniper's Mist documentation describes the hierarchy and configuration concepts used to manage wireless settings across organizations, site groups, and sites. See the Juniper Mist Documentation and the Juniper Technical Documentation portal for current Mist Wi-Fi configuration guidance.

QUESTION NO: 8

The customer wants to broadcast a WLAN at a certain time and day of the week.

Which statement is correct in this scenario?

A. Third-party integration is required to achieve this requirement.

B. Mist supports this function with an additional subscription.

C. APs need to be upgraded for this feature.

D. SSID scheduling should be configured.

ANSWER: D

Explanation:

SSID scheduling should be configured. Mist SSID scheduling lets an administrator define when an SSID is advertised, using a schedule that specifies the applicable days of the week and start/end times. This directly satisfies a requirement to make a WLAN available only during designated periods, such as business hours, school hours, or for a temporary guest network. The schedule is configured in the Mist dashboard as part of the WLAN/SSID configuration and is then applied to the access points in the relevant site or sites. When the scheduled window is active, the APs broadcast the SSID; outside that window, the WLAN is not advertised according to the configured schedule. This capability enables organizations to limit wireless-network visibility and access availability in alignment with operational policies without requiring manual daily configuration changes. Juniper documents SSID scheduling as a WLAN configuration capability and describes setting the days and time ranges during which an SSID is broadcast. See the Juniper Mist SSID Scheduling documentation and the Juniper Mist WLAN configuration documentation for configuration details.

QUESTION NO: 9

What happens first when a client requests to join a WLAN?

A. 802. 11 authentication

B. ARP request

C. 802.11 association

D. DHCP discovery

ANSWER: A

Explanation:

802. 11 authentication occurs first in the traditional IEEE 802.11 join sequence. After a station discovers an access point and selects the WLAN it wants to join, it performs an 802.11 authentication exchange with that access point before it can establish an association. This initial MAC-layer exchange establishes that the access point will proceed with the client's request to join the basic service set. In an open-system WLAN, the authentication transaction is normally a simple request and successful response; in shared-key implementations, it historically involved a challenge-response process. Once this 802.11 authentication step succeeds, the client can send an association request and the access point can allocate association state and return an association response. For enterprise WLANs, the subsequently associated client may then complete access control through 802.1X/EAP and obtain network configuration such as an IP address. Keeping these stages distinct is important: 802.11 authentication is the initial link-layer admission exchange, whereas later authentication and authorization mechanisms determine access to protected network resources. Cisco's overview of the 802.11 security process describes authentication as preceding association: Cisco 802.11 Network Security. The IEEE 802.11 working group maintains the WLAN standard family governing these MAC procedures: IEEE 802.11 Working Group.

QUESTION NO: 10

Click the Exhibit button.

Referring to the exhibit, which statement is correct about the Post-Install user's role?

A. It is used for help desk monitoring and workflow for all sites.

B. It has access limited to installing APs and switches at all sites.

C. It has read-only access to all sites.

D. It has full access to all sites.

ANSWER: B

Explanation:

It has access limited to installing APs and switches at all sites. The Post-Install role, also called the Installer role in Mist, is intended for personnel performing the initial physical deployment and onboarding of network devices. Its permissions are deliberately limited to the installation workflow rather than ongoing network administration. An installer can claim access points and switches into the organization, assign or unassign devices to sites, and assist with placing access points on maps as part of bringing a site online. This role supports efficient handoff from field installation teams to network operations teams while protecting the organization from unintended configuration or inventory changes.

Although the role can perform installation tasks across the organization, access to individual sites and their access points may be governed by a timed grace period or by explicit site-level access. This model gives installers the access needed to complete deployment without granting broad administrative authority. In particular, the role is designed for adding and staging devices, not for permanently removing organizational inventory or making unrestricted site configuration changes. Juniper's Mist Mobile App documentation describes the Installer/Post-Install workflow and the permissions associated with device installation: Mist AI Mobile App documentation.

QUESTION NO: 11

Your organization has recently purchased new VoIP handsets. All of the VoIP handsets fail to connect to the corporate WLAN. However, all other devices connect successfully. You expect that there might be a bug with the new handsets. The vendor asks you to provide a pcap file of the handsets' connection attempts.

Which Juniper Mist feature will provide this file?

A. Dynamic Packet Capture

B. Service Level Expectations

C. Clients Insights

D. Alerts dashboard

ANSWER: A

Explanation:

Dynamic Packet Capture is the Juniper Mist feature used to collect packets associated with a wireless client and produce a packet-capture file for troubleshooting. An administrator can initiate a targeted capture for an affected VoIP handset, typically using its client MAC address and the relevant access point, rather than collecting unrelated traffic across the WLAN. The resulting capture can be downloaded in standard PCAP format and examined with protocol-analysis tools such as Wireshark or supplied directly to the handset vendor. This is particularly useful when clients fail during association, authentication, DHCP, or other connection stages, because the capture provides evidence of the exchanges occurring during the attempted join. Mist's packet-capture capability is designed to make this collection available from the cloud-managed wireless workflow, reducing the need to reproduce the issue while physically connected to an AP or deploy a separate sniffer. Juniper's Mist documentation portal provides product documentation and operational guidance for Mist-managed wireless environments at Juniper Mist Documentation. Juniper also describes the Mist AI Wireless solution and its cloud-managed operational capabilities at Juniper Mist AI Wireless.

QUESTION NO: 12

Which two SLEs measure the amount of time that it takes for a process to complete? (Choose two.)

A. roaming

B. AP uptime

C. throughput

D. time to connect

ANSWER: A D

Explanation:

roaming and **time to connect** are duration-based Service Level Expectations (SLEs) in Juniper Mist Wi-Fi Assurance. The roaming SLE measures the time involved in a client's transition between access points. This lets administrators identify whether client mobility is occurring quickly enough to support a continuous user experience as a device moves through the wireless environment. Mist evaluates the roaming event and presents performance information that helps isolate delays associated with the transition process.

The time to connect SLE measures the elapsed time for a client to become usable on the network after it begins connecting. It covers the connection workflow, including key stages such as association, authentication, DHCP, and DNS. Measuring this end-to-end duration is valuable because a client can eventually connect successfully while still delivering an unacceptable user experience if one stage takes too long. Both SLEs therefore express process completion time rather than availability or capacity. Juniper describes Mist's AI-driven SLE framework and user-experience monitoring in its Mist AI wireless overview and provides product documentation through the Juniper documentation portal.

QUESTION NO: 13

Regarding the seven layer OSI networking model, which two layers are different between Ethernet and Wi-Fi? (Choose two.)

A. media access control (MAC) sub-layer

B. network layer

C. logical link control (LLC) sub-layer

D. physical layer

ANSWER: A D

Explanation:

The **media access control (MAC) sub-layer** and the **physical layer** are the two OSI-related layers that differ between Ethernet and Wi-Fi. Both technologies operate at the bottom two OSI layers, but their MAC mechanisms are designed for fundamentally different media. Ethernet MAC operation was designed for a wired LAN medium, whereas IEEE 802.11 Wi-Fi MAC operation coordinates access to a shared radio channel and includes wireless-specific functions such as association, authentication, acknowledgments, retransmissions, and contention-based channel access. These functions allow multiple stations to communicate reliably despite variable RF conditions and the inability to detect all simultaneous transmissions directly.

The physical layer is also different because Ethernet transmits electrical or optical signals through copper or fiber cabling, while Wi-Fi uses modulated radio-frequency signals sent and received through antennas. Their PHY specifications consequently define different signaling, modulation, channelization, coding, transmission rates, and media characteristics. IEEE maintains distinct 802.3 Ethernet and 802.11 wireless LAN standard families, reflecting these separate MAC and PHY implementations. See the IEEE 802.3 Ethernet working group and the IEEE 802.11 wireless LAN working group for the respective technology families.