



"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

[www.atmicnetworks .com](http://www.atmicnetworks.com)

Warning: Keep connected with our support team
for latest updates

Question: 1

What are two ways that Juniper Mist Access Assurance enforces network access control? (Choose two.)

- A. It creates a VPN using an IPsec tunnel.
- B. It monitors network traffic.
- C. It assigns specific roles to users.
- D. It groups users into network segments.

Answer: C, D

Explanation:

Juniper Mist Access Assurance is a cloud-based network access control service that provides secure wired and wireless access through identity- and policy-based mechanisms. According to the official Juniper Mist AI documentation, Access Assurance uses user and device identity to determine network access privileges dynamically.

The service enforces access policies primarily in two ways:

Assigning Specific Roles to Users:

Access Assurance dynamically assigns roles to users and devices after successful authentication.

These roles are used to apply specific network policies and permissions, defining what level of access OR network resources a user or device is allowed. Roles can be leveraged in wireless SSID configurations or switch access policies to ensure consistent enforcement across the infrastructure.

Grouping Users into Network Segments:

Access Assurance also allows grouping of users and devices into network segments using VLANs or Group-Based Policy (GBP) technology. This segmentation isolates users or devices into logical groups, ensuring security and optimized traffic handling. Policies are then applied to these groups to control communication between segments, thereby maintaining a zero-trust framework.

Options A and B are incorrect because Access Assurance does not establish VPN tunnels or passively monitor traffic as its primary method of access control. It relies instead on identity-based role assignment and segmentation to enforce network security.

Reference:

- Juniper Mist Access Assurance Data Sheet
- Juniper Mist Access Assurance Getting Started Guide
- Juniper Mist AI Cloud Documentation

Question: 2

Which statement is correct about the relationship between Juniper Mist organizations and sites?

- A. A Juniper Mist superuser login grants access to all organizations.
- B. One Juniper Mist organization can contain multiple sites.
- C. You must have one Juniper Mist superuser login for each site.
- D. One Juniper Mist site can contain multiple organizations.

Answer: B

Explanation:

According to the official Juniper Mist documentation on the configuration hierarchy, the platform uses a three-tier model: Organization → Site → Device. At the organization level, you manage administrator accounts, subscriptions, and organization-wide settings. Then:

“An organization can include one or more sites. A site can represent a physical location or a logical subdivision of your enterprise or campus.”

Also, in the simpler case explanation:

“Each customer is created as a separate organization. Within that organization multiple sites can be created.”

Mist

These statements make clear that the correct relationship is: one organization may have multiple sites under it.

The inverse — that a site might contain multiple organizations — is not supported in the documented hierarchy. Therefore option B is correct.

Question: 3

Exhibit:

Wi-Fi Roaming

Roaming Success Rate

88.2%

Roaming Failures

56

Roaming SLEs Sub-Threshold 10.6%

Roaming Classifiers

Signal Quality

WiFi Interference

Ethernet

Capacity

Referring to the exhibit, which Roaming Classifier is responsible for the sub-threshold SLEs?

- A. Signal Quality
- B. WiFi Interference
- C. Ethernet
- D. Capacity

Answer: D

Explanation:

In the Juniper Mist dashboard, Service Level Expectations (SLEs) are metrics that measure user experience in key areas such as connection, throughput, and roaming. Each SLE is composed of classifiers, which help identify the underlying cause of degraded performance or sub-threshold SCORES.

According to the Juniper Mist AI documentation, the Roaming SLE tracks client transitions between access points and evaluates the quality of those roaming events. The contributing classifiers typically include Signal Quality, Wi-Fi Interference, Ethernet, and Capacity.

In this exhibit, the bar for Capacity is the longest under the “Roaming Classifiers” section, indicating that it has the most significant impact on the Sub-Threshold SLE value (10.6%). This means roaming performance is primarily being limited by insufficient capacity — often due to AP radio congestion or a high number of concurrent clients impacting handoff efficiency.

Hence, the Capacity classifier is responsible for the sub-threshold SLEs.

Reference:

– Juniper Mist AI Service Level Expectations (SLE) Overview

– [Juniper Mist Dashboard Analytics and SLE Classifiers Guide](#)

– [Juniper Mist Wi-Fi Assurance Documentation](#)

Question: 4

How do Wireless Assurance SLEs help administrators troubleshoot?

- A. They help streamline the onboarding process.
- B. They manage Juniper Mist subscriptions.
- C. They customize the Guest User portal.
- D. They set benchmarks for network performance and user experiences.

Answer: D

Explanation:

In Juniper Mist AI, Wireless Assurance Service Level Expectations (SLEs) are designed to provide AI-driven visibility into user experience and network performance. Each SLE represents a specific aspect of the end-user journey — such as Time to Connect, Throughput, Coverage, Roaming, Capacity, and Application Experience.

According to the Juniper Mist documentation, SLEs “define measurable benchmarks for user experience and identify where deviations occur.” This allows administrators to quickly determine whether issues stem from client devices, access points, wired uplinks, or WAN connectivity. When an SLE metric falls below its threshold, Mist AI automatically highlights the affected classifier (for example, DHCP, DNS, or Wi-Fi interference) and provides root-cause correlation through AI-driven insights.

This data-driven approach enables administrators to troubleshoot proactively by focusing on user-impacting areas instead of raw device statistics. Thus, Wireless Assurance SLEs act as experience-based benchmarks that simplify troubleshooting, improve performance visibility, and shorten mean time to repair (MTTR).

Reference:

– [Juniper Mist Wireless Assurance and SLEs Overview](#)

– [Juniper Mist AI Operations and Analytics Guide](#)

Question: 5

You are asked to create a real-time visualization dashboard which displays clients on a map.

Which two Juniper Mist functions would you use in this scenario? (Choose two.)

- A. Webhooks
- B. RESTful API
- C. WebSocket
- D. Live View

Answer: C, D

Explanation:

When developing a real-time visualization dashboard that displays client locations on a map, Juniper Mist offers specific APIs and data streaming methods to support dynamic updates.

According to the Juniper Mist Developer Documentation, the WebSocket interface enables continuous, real-time streaming of client location and telemetry data directly from the Mist Cloud. This mechanism is ideal for live dashboards, as it eliminates the need for repeated REST API polling. WebSocket connections provide instant updates whenever a device moves, connects, or disconnects, ensuring the displayed map remains accurate in real time.

The Live View feature complements this functionality within the Mist Cloud and third-party integrations. It allows administrators and developers to view live location movements of Wi-Fi clients, BLE beacons, and IoT devices within a site's floor plan. It uses telemetry directly from access points, offering second-by-second updates.

In contrast, RESTful APIs and Webhooks are designed for event-based automation and configuration management rather than live visualization. REST APIs are best for historical or static data retrieval, while Webhooks are used for triggering external actions based on events.

Therefore, the correct functions for real-time map visualization are:

WebSocket (C) — for continuous live data streaming

Live View (D) — for direct map-based visualization of client activity

Reference:

- Juniper Mist Developer API and WebSocket Guide
- Juniper Mist Location Services and Live View Documentation
- Juniper Mist Cloud Architecture Overview

Question: 6

Using Juniper Mist, you want to claim multiple access points (APs) using a Web browser.

Where in the Juniper Mist Portal would you accomplish this task?

- A. Subscriptions
- B. Devices
- C. Inventory
- D. Client Onboarding

Answer: C

Explanation:

In Juniper Mist, all hardware device onboarding and claiming operations—including access points (APs), switches, and gateways—are performed under the Inventory section of the Mist Cloud Portal.

According to the Juniper Mist Cloud documentation, the Inventory page serves as the centralized location for device lifecycle management. It allows administrators to:

Claim new devices using their serial numbers or activation codes.

Batch import multiple APs via manual entry or CSV upload.

Assign claimed devices to specific sites for configuration and management.

Monitor device claim status, model type, firmware version, and cloud connectivity state.

The documentation specifies:

“To onboard or claim multiple access points in the Mist Cloud, navigate to Organization → Inventory, then click Claim Devices. Enter or paste serial numbers of the APs you want to add, and assign them to the appropriate site.”

Other options are incorrect because:

Subscriptions manages licensing and service entitlements.

Devices shows active device status per site but does not handle claiming.

Client Onboarding is used for guest access or authentication workflows, not hardware management.

Therefore, the correct answer is Inventory (C).

Reference:

- Juniper Mist Cloud Administration Guide
- Juniper Mist Access Point Onboarding and Inventory Management Documentation
- Juniper Mist AI Configuration and Setup Guide

Question: 7

Which three categories of alert types are available in Juniper Mist? (Choose three.)

- A. Users
- B. Site
- C. Security
- D. Infrastructure
- E. Marvis

Answer: CDE

Explanation:

Alerts represent network and device issues that are ongoing. Juniper Mist™ categorizes them as follows:

Infrastructure Alerts—Repeated events involving servers and protocols that can potentially affect a

large number of clients. For example, an event during which a Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), or RADIUS server is unreachable can affect many clients.

Similarly, if a power supply on a switch is in alarm state, a large number of clients and a large amount of traffic could be affected.

Marvis Alerts—Repeated events that Marvis tracks on the Marvis Actions dashboard. For example, if an access point (AP) regularly fails health checks, you'll see a Marvis alert for it.

Security Alerts—Repeated events that could dramatically affect network security. For example, these alerts appear if a rogue AP is detected and clients start connecting to it.

Certificate Alerts—Notification for expired, and soon-to-expire, user-added digital certificates. These include RadSec (configured at Organization > Settings > RadSec Certificates and AP RadSec certificate), SSO (configured at Organization > Settings > Single Sign-On), and PSK Portal IDP certificates (configured at Organization > Client Onboarding). Certificate alerts appear on the Alerts page and begin 30 days before the certificate's expiry date, then the notification repeats 15, 7, 3, and 1 day before expiration unless the certificate is renewed. .

<https://www.juniper.net/documentation/us/en/software/mist/mist-aiops/topics/concept/alerts-overview.html>

Question: 8

Exhibit:

Subscriptions

Service	Purchased	Onboarded	Start Date	End Date
Marvis for Wireless	103	82	Feb. 21, 2022	Feb. 2025

Mist Wireless Assurance -
Standard

61

61

Jul. 2, 2021

Jul. 1, 2024

Mist Premium Analytics for
Wireless

24

24

Feb. 21, 2022

Feb. 20, 2025

Referring to the exhibit, how many Marvis for Wireless subscriptions have been purchased and onboarded?

- A. 103
- B. 82
- C. 24
- D. 61

Answer: B

Explanation:

In the Juniper Mist Cloud Portal, the Subscriptions page provides a summary of all service entitlements associated with an organization, including the number of licenses purchased and onboarded for each Mist Cloud service.

According to the official Juniper Mist Cloud Administration Guide, this section displays key fields such as Service Name, Purchased, Onboarded, Start Date, and End Date. The Purchased column indicates the total number of subscriptions bought, while the Onboarded column represents how many of those have been actively assigned and deployed within the organization's network.

In the exhibit, the entry for Marvis for Wireless shows 103 purchased and 82 onboarded, meaning that while 103 licenses were obtained, only 82 have been claimed and are in use within the system.

Therefore, the correct number of onboarded Marvis for Wireless subscriptions is 82.

Reference:

- Juniper Mist Cloud Administration Guide
- Juniper Mist Licensing and Subscription Management Documentation

Question: 9

Marvis has notified you that you have a bad cable.

What additional information does the Marvis Actions dashboard provide to help you solve the issue?

- A. If the port or cable is at fault.
- B. The switch port to which the cable is connected.
- C. Which of the eight Ethernet wires are broken.
- D. The category rating of the cable.

Answer: A

Explanation:

The Marvis Virtual Network Assistant (VNA) in Juniper Mist AI uses real-time telemetry and AI-driven correlation to identify hardware and connectivity issues, including bad cable conditions. When a “Bad Cable” alert is raised, Marvis analyzes physical link metrics from the switch and AP—such as CRC errors, FCS drops, and link flaps—to isolate the root cause.

According to the Juniper Mist AI Operations Guide, the Marvis Actions dashboard provides

contextual insights into the issue, showing whether the fault lies in the physical cable itself or the switch port it is connected to. Specifically, the dashboard highlights:

The affected device and port.

Whether the degradation originates from the port hardware or the cabling.

Suggested corrective action (e.g., replace the cable or check switch hardware).

Marvis uses its AI-driven root cause analysis engine to distinguish between cable integrity problems and port failures by examining electrical signature anomalies and historical telemetry.

Options B, C, and D are incorrect because Marvis does not display cable category ratings or identify individual broken Ethernet pairs—it focuses on identifying and isolating the fault domain.

Therefore, the correct answer is A. If the port or cable is at fault.

Reference:

- Juniper Mist Marvis Virtual Network Assistant User Guide
- Juniper Mist AI Operations and Troubleshooting Documentation
- Juniper Mist Actions and Insights Dashboard Overview

Question: 10

Which two statements are true about switch configurations at the site level? (Choose two.)

- A. Organizational-level templates override site-level switch configurations.
- B. Switch configurations at the site level are required to manually configure individual switches.
- C. Switch configurations at the site level are an additional way to apply a switch template to a specific site.
- D. Site-level switch configurations override org-level templates.

Answer: C, D

Explanation:

In the Juniper Mist Cloud architecture, configuration hierarchy and inheritance are key design principles for managing EX Series and QFX Series switches under Wired Assurance. Configuration settings can be applied at both the organization level and the site level, with clearly defined precedence rules.

According to the Juniper Mist Wired Assurance Configuration Guide, the organization level defines global configuration templates that apply across multiple sites, while the site level provides customization options specific to a particular location or environment.

The documentation states:

“Site-level configuration overrides any global or organizational template configurations for switches within that site.”

and further clarifies:

“Administrators can create or modify switch templates at the site level to apply custom settings to specific deployments without affecting other sites under the same organization.”

Thus:

Statement C is correct — site-level configurations are an additional method to apply templates for a specific site.

Statement D is correct — site-level configurations take precedence over org-level templates.

Statement A is incorrect because org-level templates do not override site-level configurations; the reverse is true.

Statement B is incorrect because site-level configuration is not required for manual switch setup—it is an optional, more efficient method of template application.

Reference:

- Juniper Mist Wired Assurance Configuration and Template Management Guide
- Juniper Mist Cloud Administration Guide
- Juniper Mist Site and Organization Configuration Hierarchy Documentation

Question: 11

What is required for Marvis Minis to operate?

- A. WAN Assurance subscription
- B. Premium Analytics subscription
- C. Minimum AP firmware
- D. WLAN template

Answer: C

Explanation:

Marvis Minis is an advanced feature within the Juniper Mist AI ecosystem designed to perform autonomous, synthetic network testing. It uses Mist Access Points (APs) to simulate client behavior— such as association, authentication, DHCP,

DNS, and application reachability—to proactively detect service issues before real users are affected.

According to the Juniper Mist Marvis Minis Deployment Guide and Marvis AI documentation, the key requirement for enabling Marvis Minis is that all participating access points must be running a minimum supported firmware version that includes the Minis agent functionality.

The documentation specifies:

“Marvis Minis requires APs running the minimum firmware version that supports synthetic testing. APs on earlier versions will not be capable of running Minis tests or reporting results to the Mist Cloud.”

Additional subscriptions such as WAN Assurance, Premium Analytics, or WLAN templates are not prerequisites for operation. While Marvis licensing must be active, the feature itself relies primarily on compatible firmware within the Mist-managed APs.

Therefore, the correct answer is C. Minimum AP firmware — ensuring the APs are on a supported firmware release is essential for Marvis Minis functionality.

Reference:

- Juniper Mist Marvis Minis Deployment and Configuration Guide
- Juniper Mist AI Operations and Troubleshooting Documentation
- Juniper Mist Wireless Assurance and Firmware Management Guide

Question: 12

Which two statements are correct about the Juniper Mist vBLE Asset Visibility mode? (Choose two.)

- A. The vBLE antenna is in the receive mode.
- B. The vBLE antenna tracks chirps from BLE tags.
- C. The vBLE antenna communicates with mobile devices running the Juniper Mist location SDK.
- D. The vBLE antenna is in the transmit mode.

Answer: A, B

Explanation:

Juniper Mist's virtual Bluetooth Low Energy (vBLE) technology is designed to deliver precise indoor location services using cloud-managed access points equipped with integrated BLE antenna arrays. The system supports multiple operational modes, including Engagement Mode (for mobile app interactions) and Asset Visibility Mode (for BLE tag tracking).

According to the Juniper Mist Location Services Documentation, in Asset Visibility Mode, the vBLE antenna functions primarily in receive mode to detect and process signals emitted from BLE asset tags. These tags periodically transmit Bluetooth "chirps" that are received by multiple APs. Mist Cloud then uses angle-of-arrival (AoA) and RSSI triangulation algorithms to determine the exact location of the asset within the facility.

The documentation specifies:

"In Asset Visibility Mode, the vBLE antenna operates in receive mode and listens for BLE tag beacons (chirps). The system triangulates these signals to calculate the real-time location of tracked assets."

Conversely, Engagement Mode is the configuration in which vBLE operates in transmit mode to

interact with mobile devices running the Mist SDK — which corresponds to location-based engagement or proximity notifications.

Thus, the correct answers are:

- A . The vBLE antenna is in the receive mode
- B . The vBLE antenna tracks chirps from BLE tags

Reference:

- Juniper Mist Location-Based Services Configuration Guide
- Juniper Mist vBLE Architecture and Operation Modes Documentation
- Juniper Mist Cloud Location Services Technical Overview

Question: 13

Which statement about Marvis Minis is correct?

- A. Marvis Minis is Juniper's onsite technical support team that troubleshoots enterprise access points.
- B. Marvis is an LLM that designs network infrastructure.
- C. Marvis provides Marvis Actions to simulate user connections.
- D. Marvis Minis works with Juniper Mist AI to validate network configuration to optimize user experiences.

Answer: D

Explanation:

Marvis Minis is a component of the Marvis Virtual Network Assistant (VNA) within the Juniper Mist AI ecosystem. It is designed to proactively ensure optimal network performance and user experience

by running synthetic network tests using Mist-managed access points.

According to the Juniper Mist Marvis Minis Technical Overview, this feature allows APs to act as virtual clients that automatically simulate user connection flows, including authentication, DHCP, DNS, and application reachability. These tests validate that the network configuration and services are functioning as expected, even before real users experience issues.

The documentation states:

“Marvis Minis operates in conjunction with Mist AI to continuously validate network configurations and optimize user experience by identifying potential problems proactively.”

“Using Mist APs, Marvis Minis performs synthetic transactions to verify the performance of wireless, wired, and WAN segments without requiring external devices.”

Hence, Marvis Minis is not a support team (A), not a design AI model (B), and Marvis Actions (C) is a different feature for identifying and resolving live issues. The accurate description is that Marvis Minis collaborates with Mist AI to validate configurations and optimize user experiences.

Reference:

- Juniper Mist Marvis Minis Overview and Deployment Guide
- Juniper Mist AI Operations and Monitoring Guide
- Juniper Mist Marvis Virtual Network Assistant Documentation

Question: 14

Which two statements describe SLEs? (Choose two.)

- A. SLEs use machine learning to provide a proactive approach to understanding the end-user experience.

-
- B. SLEs use data science to troubleshoot network issues on an ad hoc basis.
 - C. The metrics analyzed to meet specific SLE goals are categorized into classifiers.
 - D. SLEs display a detailed list of Wi-Fi clients who have connected to the network.

Answer: A, C

Explanation:

In Juniper Mist AI, Service Level Expectations (SLEs) form the foundation of Wireless Assurance and Wired Assurance. They provide a data-driven, proactive method to measure and maintain the quality of user experience, going beyond traditional device-centric monitoring.

According to the Juniper Mist AI Operations Guide and Wireless Assurance Documentation, SLEs:

“Leverage machine learning and data science to deliver a proactive understanding of end-user experience and identify root causes of performance issues.”

Each SLE (such as Time to Connect, Roaming, Throughput, Coverage, and Capacity) is composed of classifiers, which break down performance metrics into measurable, root-cause categories. Examples include DHCP, DNS, Authentication, and Signal Quality classifiers.

This classifier-based structure enables Mist AI to automatically correlate problems and highlight the most probable cause of degradation—eliminating the need for manual troubleshooting or reactive analysis.

Options B and D are incorrect because SLEs are not ad hoc tools for manual troubleshooting and do not simply list connected clients. Instead, they provide intelligent, AI-driven insights into user experience across the network.

Therefore, the correct statements are:

- A . SLEs use machine learning to provide a proactive approach to understanding the end-user experience.
- C . The metrics analyzed to meet specific SLE goals are categorized into classifiers.

Reference:

- Juniper Mist Wireless Assurance and SLE Overview
 - Juniper Mist AI Operations and Analytics Guide
 - Juniper Mist Cloud Monitoring and SLE Classifier Documentation
-

Question: 15

What are two ways to claim an Access Point with Juniper Mist? (Choose two.)

- A. Activation code
- B. Claim code
- C. MAC address
- D. Serial number

Answer: A, B

Explanation:

From Juniper's official guide:

"You'll need either a claim code or an activation code to claim an AP. With either, you can claim an AP by using one of the following methods:

Mist AI Mobile App

A Web browser

You can claim either a single AP using a claim code or multiple APs using an activation code. You can use any of these methods to claim an AP:

To claim a single AP, use the claim/QR code located on the rear of the AP.

To claim multiple APs, you'll need to use an activation code. When you purchase multiple APs, we provide you with an activation code along with your PO information."

From the Mist documentation:

"APs can be claimed to any organization by using either the activation code, claim code or QR code.

Activation Code: Whenever you order APs, our Sales Operations team will send you an activation code which can be used for claiming the APs and subscriptions as per the order. ...

AP Claim Code: You can individually claim APs to your organization by navigating to Organization > Inventory > Claim

APs and entering in the claim code found on the back of each AP.

AP QR Code: Using our Mist AI mobile app you can scan the QR code printed on the back of our APs to claim APs to your organization.”

Summary:

The Juniper Mist platform allows you to claim an Access Point using:

Activation code (provided for bulk purchases, via PO)

Claim code (unique per AP, on the rear label)

QR code (scanned with the Mist AI mobile app, also encoded as the claim code)

These extracts are direct from Juniper’s own documentation and confirm the methods for AP onboarding in the Mist platform.

Question: 16

Which two protocols does Marvis Minis automatically validate? (Choose two.)

- A. Simple Network Management Protocol (SNMP)
- B. Dynamic Host Configuration Protocol (DHCP)
- C. Network Time Protocol (NTP)
- D. Address Resolution Protocol (ARP)

Answer: B, D

Explanation:

Marvis Minis is a feature within Marvis Virtual Network Assistant (VNA) that proactively tests and validates network performance by simulating user connections. Instead of waiting for user complaints, it performs synthetic client transactions to confirm the functionality of critical network services.

According to the Juniper Mist Marvis Minis Technical Overview and Marvis AI Operations Guide, Minis validates several network functions automatically, including:

Dynamic Host Configuration Protocol (DHCP): Ensures clients can obtain IP addresses properly from DHCP servers, validating end-to-end DHCP exchange success and response time.

Address Resolution Protocol (ARP): Verifies correct IP-to-MAC address resolution, confirming that clients can reach devices on the same subnet and that ARP tables are updated correctly.

Marvis Minis also performs checks on DNS resolution, authentication, and application reachability, but not on SNMP or NTP. Those protocols are used for management and time synchronization, not end-user connectivity validation.

Thus, the correct answers are B (DHCP) and D (ARP).

Reference:

- Juniper Mist Marvis Minis Deployment and Operations Guide
- Juniper Mist AI Assurance and Troubleshooting Documentation
- Juniper Mist Cloud Synthetic Testing Overview

Question: 17

What does the Predictive Analytics and Correlation Engine (PACE) of Mist AI use to understand the end-user experience?

- A. Machine learning
- B. User feedback
- C. Network monitoring tools
- D. Manual analysis

Answer: A

Explanation:

The Predictive Analytics and Correlation Engine (PACE) is the core AI engine that powers the Juniper Mist Cloud. It is

designed to continuously learn from real-time telemetry and user interactions across wireless, wired, and WAN networks to proactively identify anomalies and predict performance issues.

According to the Juniper Mist AI Cloud and PACE Architecture Documentation, PACE:

“Leverages machine learning and advanced analytics to correlate data across millions of network sessions, automatically identifying patterns that affect user experience.”

The engine continuously evaluates key Service Level Expectations (SLEs), such as Time to Connect, Throughput, and Roaming, to establish performance baselines and detect deviations before users notice them.

PACE does not rely on manual analysis or user feedback, and it integrates telemetry rather than external monitoring tools to maintain a closed-loop feedback system for self-correction and optimization.

Therefore, PACE uses machine learning (A) to understand, predict, and improve end-user experience across Juniper Mist-managed networks.

Reference:

- Juniper Mist AI Cloud Architecture and PACE Overview
- Juniper Mist AI Operations and Analytics Guide
- Juniper Mist Assurance and Machine Learning Documentation

Question: 18

Which two statements describe port profiles? (Choose two.)

- A. They can be assigned to multiple ports.
- B. They include a set of interface configurations.
- C. They must be assigned to only one port.
- D. They include a set of routing configurations.

Answer: A, B

Explanation:

Port profiles in Juniper Mist Wired Assurance are reusable configuration templates that define how switch ports behave. They streamline switch provisioning and ensure consistent configurations across **multiple ports and devices within a site or organization.**

According to the Juniper Mist Wired Assurance Configuration Guide, port profiles are defined as:

“A collection of interface-level settings that can be applied to one or more switch ports to simplify configuration and ensure uniform policy enforcement.”

Key characteristics include:

Reusable templates: Port profiles can be assigned to multiple ports on one or more switches, allowing rapid deployment and consistent port behavior (e.g., access, trunk, voice VLAN).

Interface-level parameters: They include settings such as VLAN assignments, PoE configuration, speed, duplex, and LLDP options.

Port profiles do not include routing configurations (those are defined at the Layer 3 interface or VLAN interface level) and are not limited to a single port.

Therefore, the correct answers are:

A . They can be assigned to multiple ports.

B . They include a set of interface configurations.

Reference:

E. Juniper Mist Wired Assurance Configuration and Templates Guide

F. Juniper Mist Cloud Switch Management Documentation

G. Juniper EX Series Switch Wired Assurance Overview

Question: 19

Where do reminders about subscription expiration appear in the Juniper Mist portal?

A. In a banner message at the top of the Juniper Mist portal

B. In the dashboard alerts

C. In Marvis Actions

D. In the device's insights section

Answer: A

Explanation:

Juniper Mist Cloud provides visual and automated notifications to alert administrators about subscription status and expiration for services such as Wireless Assurance, Wired Assurance, WAN Assurance, Premium Analytics, and Marvis AI.

According to the Juniper Mist Cloud Administration and Licensing Guide, the system:

“Displays subscription and license expiration warnings in a banner across the top of the Mist portal interface when licenses are within their renewal window.”

This banner typically appears in yellow or red, depending on urgency, and includes direct links to the Subscriptions page for renewal actions.

While subscription status information can also be viewed manually under Organization → Subscriptions, the real-time reminders and notifications appear as banner messages at the top of the Mist Portal.

Options B, C, and D are incorrect because:

Dashboard alerts focus on network events, not licensing.

Marvis Actions highlights operational or performance issues.

Device insights report performance metrics, not subscription data.

Therefore, the correct answer is A. In a banner message at the top of the Juniper Mist portal.

Reference:

- Juniper Mist Cloud Licensing and Subscription Management Guide
- Juniper Mist Administration and Portal User Interface Overview
- Juniper Mist Cloud Operations and Renewal Notifications Documentation

Question: 20

Which Juniper Mist dashboard feature uses the ROAMINGOF element?

A. Conversational Assistant

B. Marvis Query Language

C. Marvis Minis

D. Wireless SLE

Answer: B

Explanation:

The ROAMINGOF element is part of the Marvis Query Language (MQL), which is the structured query syntax used by Marvis, Juniper's Virtual Network Assistant (VNA).

According to the Juniper Mist Marvis and MQL Technical Reference, Marvis Query Language provides advanced data query and automation capabilities that go beyond the conversational interface. It allows administrators to directly extract analytical insights, run network diagnostics, and perform queries related to user experience metrics and Service Level Expectations (SLEs).

The documentation specifies:

"MQL is the analytical engine of Marvis that uses elements such as ROAMINGOF, CONNECTIVITYOF, and PERFORMANCEOF to query Mist data and retrieve SLE metrics, performance trends, and device events."

The ROAMINGOF element specifically relates to the Wireless Roaming SLE category, enabling Marvis

to evaluate client roaming performance across access points, identify failed transitions, and correlate signal quality or capacity-related issues.

While the Conversational Assistant (A) uses natural language queries, it translates them internally into MQL commands.

Marvis Minis (C) runs synthetic tests, and Wireless SLE (D) displays performance metrics but does not directly use MQL syntax elements.

Thus, the correct answer is B. Marvis Query Language.

Reference:

– Juniper Mist Marvis Query Language (MQL) Reference Guide

– Juniper Mist Marvis Virtual Network Assistant Technical Overview

Question: 21

In the context of Juniper Mist, which two statements describe a bad user minute? (Choose two.)

- A. A metric that tracks how many minutes a user is connected to a network.
- B. A way to normalize a user's negative network experience.
- C. The number of minutes a device is down multiplied by the number of users affected.
- D. The number of affected users multiplied by the number of minutes they are affected.

Answer: B, D

Explanation:

In Juniper Mist AI, the concept of a Bad User Minute (BUM) is a core metric used within Service Level Expectations (SLEs) and the AI-driven analytics engine to quantify negative user experience.

According to the Juniper Mist AI Operations and SLE Analytics Guide, a “bad user minute” is defined as:

“A normalized measure that represents one minute of degraded user experience for one user.”

Mist AI calculates this by multiplying the number of affected users by the number of minutes they experience poor performance. This allows administrators to understand the impact of network issues not just in duration, but in terms of total user experience degradation.

For example, if ten users experience poor connectivity for one minute, the system records 10 bad user minutes. This normalization helps Juniper Mist prioritize incidents based on impact, rather than duration alone, allowing administrators to focus on issues that affect the greatest number of users.

Therefore:

B is correct — it's a way to normalize a user's negative experience.

D is correct — it's calculated as number of affected users × number of minutes affected.

Reference:

- Juniper Mist AI Operations and Analytics Guide
- Juniper Mist Wireless Assurance and SLE Overview
- Juniper Mist AI Insight Metrics and KPI Definitions

Question: 22

How often does Marvis Minis execute automatic validations?

- A. Every 30 minutes
- B. Every hour
- C. Every week
- D. Every day

Answer: B

Explanation:

Marvis Minis continuously validates the health of network services by performing synthetic tests at predefined intervals without requiring user intervention. These tests simulate real client interactions — such as authentication, DHCP, DNS, and application reachability — to detect network issues **proactively**.

According to the Juniper Mist Marvis Minis Technical Overview, the feature performs:

“Automated validations every hour to ensure wireless, wired, and WAN network services are operating as expected.”

Each validation cycle allows the Minis agent (running on Mist Access Points) to verify connectivity and performance parameters across key stages of the client experience. If any issues are detected, they are automatically surfaced in the

Marvis Actions dashboard for further analysis.

While administrators can trigger additional manual tests, automatic validations occur every hour by default across all enabled sites.

Therefore, the correct answer is B. Every hour.

Reference:

– Juniper Mist Marvis Minis Operations and Validation Guide

Question: 23

Which two configuration elements are available in a WLAN template? (Choose two.)

- A. Radio management
- B. Template policies
- C. Organizations
- D. WLANs

Answer: A, D

Explanation:

In the Juniper Mist Cloud, a WLAN template is used to standardize and simplify the configuration of wireless networks across multiple sites. Templates define common wireless parameters, ensuring consistent deployment and easier scalability while reducing configuration errors.

According to the Juniper Mist Wireless Assurance Configuration Guide, WLAN templates contain several configurable elements that define how the wireless network operates, including:

Radio Management (A)

This element controls RF parameters such as transmit power, channel width, and radio band assignments (2.4 GHz / 5 GHz / 6 GHz). It leverages Mist's AI-driven Radio Resource Management (RRM) to optimize RF performance across APs dynamically.

WLANs (D)

The template includes WLAN definitions (SSIDs) with associated settings such as authentication type, VLAN assignment, access control policies, and bandwidth limitations. WLANs can be linked to specific sites through these templates for unified management.

The other options are incorrect:

Template Policies (B) are not a defined component within WLAN templates—they refer to higher-level configuration management.

Organizations (C) exist at the top hierarchy level in Mist Cloud (above sites and templates) and are not configured within a WLAN template.

Therefore, the two correct configuration elements available in a WLAN template are:

A . Radio management

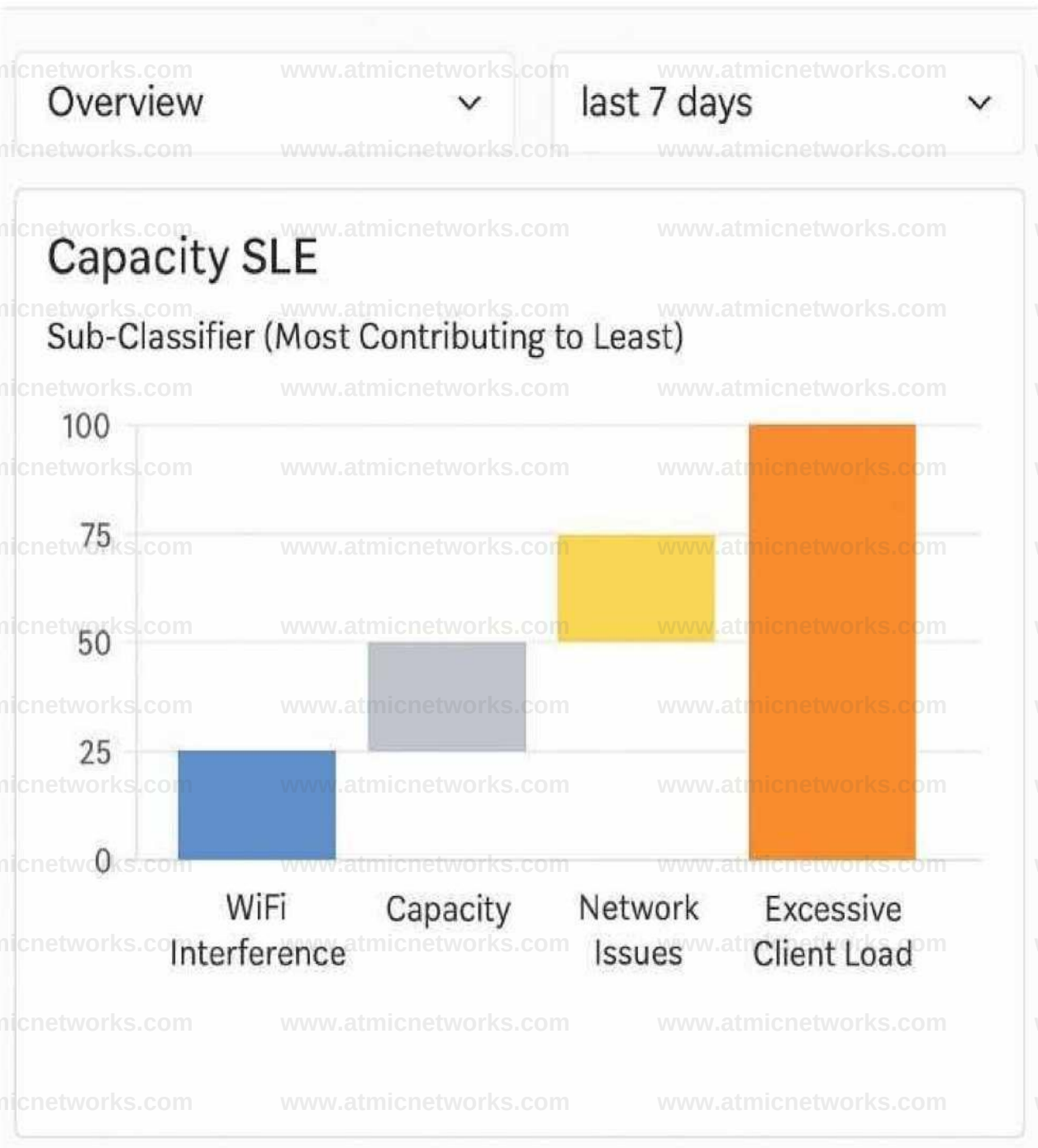
D . WLANs

Reference:

- Juniper Mist Wireless Assurance Configuration and Deployment Guide
 - Juniper Mist Cloud WLAN Template Management Documentation
 - Juniper Mist AI Configuration Hierarchy and Template Overview
-

Question:
24

Exhibit:



Referring to the exhibit, which sub-classifier contributed the most to capacity issues?

- A. WiFi Interference
- B. Capacity
- C. Network ISSUES
- D. Excessive Client Load

Answer: D

Explanation:

In the Juniper Mist Wireless Assurance dashboard, each Service Level Expectation (SLE) is broken down into sub-classifiers to identify the specific causes of degraded user experience. For the Capacity SLE, Mist AI analyzes performance indicators related to access point utilization, airtime availability, client density, and radio congestion.

According to the Juniper Mist Wireless Assurance Analytics Guide, sub-classifiers within the Capacity SLE may include:

WiFi Interference – measures co-channel and adjacent-channel interference.

Capacity – monitors total bandwidth and airtime utilization.

Network Issues – highlights backend transport or switching congestion.

Excessive Client Load – indicates when too many clients are associated with a single access point or radio, leading to reduced throughput and contention.

In the exhibit, the Excessive Client Load bar clearly shows the highest contribution to the Capacity SLE degradation. This means that the majority of capacity issues were caused by an overloaded access point or radio channel handling more clients than optimal.

Therefore, the correct answer is D. Excessive Client Load.

Reference:

- Juniper Mist Wireless Assurance SLE and Classifier Documentation
- Juniper Mist AI Operations and Analytics Guide

Question: 25

Which two statements about webhooks and APIs are correct? (Choose two.)

- A. Webhooks are a push from Juniper Mist, and APIs are a pull by the client.
- B. There is an hourly limit to the number of API calls that an organization can have.
- C. There is an hourly limit to the number of webhooks that an organization can have.
- D. 100% of all Juniper Mist objects are configurable using webhooks.

Answer: A, B

Explanation:

In the Juniper Mist Cloud architecture, both webhooks and APIs are key interfaces for automation, integration, and data exchange with third-party systems. While they both facilitate communication between Mist and external applications, they operate in opposite directions and serve distinct purposes.

According to the Juniper Mist API and Webhook Developer Guide:

Webhooks are push-based notifications initiated by the Juniper Mist Cloud. When specific events occur (such as device disconnection, client onboarding, or alert generation), Mist sends structured JSON payloads to a preconfigured external URL endpoint.

APIs (Application Programming Interfaces) are pull-based queries where an external client polls the Mist Cloud to retrieve or update data (e.g., inventory, configuration, or metrics).

Additionally, the Mist Cloud enforces rate limits on API calls to ensure platform stability and fair usage:

“API rate limits are applied on a per-organization basis to prevent excessive polling and to maintain consistent performance.”

In contrast, webhooks do not have a strict hourly quota because they are event-triggered rather than continuous requests.

Therefore:

A is correct — Webhooks push, APIs pull.

B is correct — There is an hourly API rate limit per organization.

Options C and D are incorrect because webhooks are event-based (not rate-limited hourly) and do not configure Mist objects directly—they only send notifications.

Reference:

- [Juniper Mist API and Webhook Developer Documentation](#)
- [Juniper Mist Cloud Automation and Integration Guide](#)
- [Juniper Mist Platform Architecture Overview](#)

Question: 26

What does the AI-driven RRM in Juniper Mist Wireless Assurance optimize?

- A. Band steering
- B. Radio resource settings
- C. SSID naming conventions
- D. User interfaces

Answer: B

Explanation:

The AI-driven Radio Resource Management (RRM) feature in Juniper Mist Wireless Assurance dynamically optimizes radio resource settings across all managed access points (APs) to ensure optimal wireless coverage, capacity, and performance.

According to the Juniper Mist Wireless Assurance and RRM Guide, RRM continuously analyzes live network telemetry, including metrics such as signal strength, interference, channel utilization, and client distribution, to make intelligent adjustments in real time.

It automatically optimizes parameters such as:

Channel selection (to minimize co-channel and adjacent-channel interference).

Transmit power levels (to balance coverage and minimize contention).

Channel width (to optimize throughput based on RF conditions).

The documentation specifies:

“AI-driven RRM in Mist Cloud continuously learns and adapts radio configurations based on environmental and client behavior patterns, improving network stability and overall user experience.”

Options A, C, and D are incorrect because:

Band steering is a specific feature handled separately within WLAN settings.

SSID naming conventions and user interfaces are administrative, not RRM-controlled.

Therefore, the correct answer is B. Radio resource settings.

Reference:

- Juniper Mist Wireless Assurance and AI-driven RRM Documentation
- Juniper Mist AI Cloud Operations Guide
- Juniper Mist Access Point Configuration and Optimization Guide

Question: 27

What are device-specific WAN Edge templates used for in an SD-WAN configuration?

- A. To automate the WLAN template process
 - B. To automatically generate configuration elements specific to device models
 - C. To perform traffic inspection for WAN edge devices
 - D. To monitor network events and stop attacks
-

Answer: B

Explanation:

In the Juniper Mist SD-WAN solution, device-specific WAN Edge templates are used to streamline the deployment and configuration of Juniper SRX or SSR (Session Smart Router) devices serving as WAN Edge nodes. These templates ensure consistent and accurate configurations across a distributed WAN environment while accounting for differences in hardware models and interface types.

According to the Juniper Mist WAN Assurance and SD-WAN Configuration Guide, device-specific templates:

“Automatically generate configuration elements tailored to the hardware platform, including interfaces, ports, and device capabilities.”

They are part of Mist's cloud-managed SD-WAN automation framework, which combines WAN Assurance and AI-driven insights to manage branch connectivity. The templates simplify provisioning by populating device-level parameters such as:

Interface naming and mapping based on the device model.

Hardware-specific configurations like tunnel endpoints, IP addressing, and routing settings.

Security and performance policies consistent with the organization's SD-WAN design.

Options A, C, and D are incorrect because:

A (WLAN template automation) pertains to wireless network configuration, not WAN edge devices.

C (traffic inspection) relates to firewall or security policies handled by SRX's UTM features, not templates.

D (monitoring and attack prevention) falls under Mist's security or analytics capabilities, not the template function.

Therefore, the correct answer is B. To automatically generate configuration elements specific to device models.

Reference:

- Juniper Mist WAN Assurance and SD-WAN Configuration Guide
 - Juniper Mist Cloud Device Template Management Documentation
 - Juniper Mist AI-Driven SD-WAN Deployment Overview
-

Question: 28

You are creating a new site in the UI.

What are three required configuration settings in this scenario? (Choose three.)

- A. Country
- B. Location
- C. RF Template
- D. Active Hours
- E. Site Name

Answer: A, B, E

Explanation:

When creating a new site in the Juniper Mist User Interface, the three required configuration settings are Site Name, Country, and Location. According to Juniper Mist's official configuration guides: "At a minimum, enter the name, time zone, and location..." The 'Information' section of site setup requires the Site Name (a descriptive name to identify the site), Country (which sets regulatory and RF domain requirements), and Location (address or geo-coordinates for the site). These form the basis of the site identity in the Mist cloud and are mandatory for dashboard visibility, compliance, and baseline RF configuration. An RF Template, though critical for wireless tuning, is optional and can be assigned post-site creation. Active Hours are not required for the default site setup and are related to scheduling analytics or location-based services, not to the core creation workflow.

Reference:

Juniper Mist Configure a Site , Site Configuration Settings Guide , Mist Management Guide

Question: 29

Which Juniper Mist feature provides application forwarding path details?

-
- A. Router Insights
 - B. WAN Edge Insights
 - C. Forwarding Insights
 - D. Platform Insights

Answer: C

Explanation:

In the Juniper Mist WAN Assurance and SD-WAN framework, Forwarding Insights is the feature responsible for providing application forwarding path visibility. It delivers detailed analytics on how application traffic is being routed across the WAN, enabling network administrators to understand and optimize application performance across multiple WAN links or paths.

According to the Juniper Mist WAN Assurance and Insights Documentation, Forwarding Insights:

“Provides visibility into the application forwarding path by showing which WAN link or tunnel is used for a specific flow, including health metrics such as latency, loss, and jitter.”

It integrates with Marvis and the AI-driven WAN Assurance engine to automatically correlate user experience with network transport behavior. Administrators can use Forwarding Insights to:

Identify which path (primary, secondary, or backup) an application flow takes.

View real-time performance metrics such as round-trip delay and packet loss per path.

Understand why path selection decisions were made, based on policy or link health.

Other options are incorrect:

A . Router Insights focuses on routing and device-level performance, not per-application path details.

B . WAN Edge Insights provides device health and site connectivity data, not application-level forwarding analytics.

D . Platform Insights covers cloud infrastructure performance, not WAN traffic analysis.

Thus, the correct answer is C. Forwarding Insights.

Reference:

-
- Juniper Mist WAN Assurance and Forwarding Insights Technical Guide
 - Juniper Mist AI-Driven SD-WAN Operations Documentation
 - Juniper Mist Cloud Analytics and Insights Overview

Question: 30

Your organization currently uses Access Assurance for 802.1X authentication of wireless users using user certificates. All users are currently placed in the same VLAN after authentication.

There are multiple VLANs at your sites.

In this scenario, how would you configure Access Assurance to make the network more secure?

- A. Configure MAC Authentication Bypass (MAB) and assign WxLAN roles based on groups of MAC addresses.
- B. Configure user authentication using EAP-TTLS and assign WxLAN roles based on AD user group.
- C. Configure host (machine) authentication using EAP-TLS and assign WxLAN roles based on AD user group.
- D. Configure user authentication using EAP-TLS and assign WxLAN roles based on AD user group.

Answer: D

Explanation:

Juniper Mist Access Assurance provides cloud-based network access control (NAC) by integrating RADIUS, identity-based policy enforcement, and WxLAN role-based segmentation. It allows administrators to assign users and devices to specific VLANs or network segments dynamically based on authentication attributes, thereby improving both security and policy granularity.

According to the Juniper Mist Access Assurance Configuration Guide, to enhance network security in a multi-VLAN environment, you should:

“Use EAP-TLS (certificate-based authentication) for secure user identification, and dynamically assign WxLAN roles or VLANs based on Active Directory (AD) group membership.”

Here's why D is correct:

EAP-TLS ensures mutual authentication between client and RADIUS server using digital certificates — preventing credential theft or spoofing.

Integrating with Active Directory allows role-based access control (RBAC), enabling dynamic VLAN or WxLAN assignment. This ensures users from different groups (e.g., staff, contractors, guests) are automatically segmented into appropriate network zones.

Option breakdown:

A (MAB): Used for non-802.1X devices (e.g., printers), less secure for user authentication.

B (EAP-TTLS): Username/password-based and less secure than certificate-based EAP-TLS.

C (Host authentication): Verifies devices only, not user identity—insufficient for user-level control.

Therefore, the most secure and scalable configuration is:

☒ D. Configure user authentication using EAP-TLS and assign WxLAN roles based on AD user group.

Reference:

- Juniper Mist Access Assurance Deployment and Configuration Guide
- Juniper Mist Cloud NAC and 802.1X Authentication Documentation
- Juniper Mist Secure Access and WxLAN Role-Based Policy Guide

Question: 31

Which two statements are correct about Juniper Mist subscriptions? (Choose two.)

- ☐ A. Subscriptions are not associated with a specific device serial number.
- ☐ B. If a device fails and is removed from the network, you must manually transfer the subscription to the new device before installing.
- ☐ C. Subscriptions are associated with a specific device serial number.
- ☐ D. If a device fails and is removed from the network, the subscription will automatically apply to the new device when added.

Answer: A, D

Explanation:

In the Juniper Mist Cloud licensing model, subscriptions represent service entitlements that enable specific features such as Wireless Assurance, Wired Assurance, WAN Assurance, Marvis Virtual Network Assistant, and Premium

Analytics. These subscriptions are managed at the organization level and are not permanently tied to individual hardware units.

According to the Juniper Mist Licensing and Subscription Management Guide, subscriptions are:

“Cloud-based entitlements associated with an organization, not bound to specific device serial numbers. Devices draw from the subscription pool dynamically.”

This design allows flexibility and simplifies device replacement or scaling:

When a new device (for example, an access point or switch) is added to the organization, the subscription is automatically assigned to it from the available pool.

If a device is removed or fails, the subscription is automatically released and reassigned to a replacement unit—no manual transfer is required.

Therefore:

A is correct because subscriptions are not linked to a single device’s serial number.

D is correct because subscriptions automatically reapply when replacement devices are onboarded.

Options B and C are incorrect because Juniper Mist subscriptions are organization-based, not hardware-bound, and require no manual reassignment after device failure or replacement.

Reference:

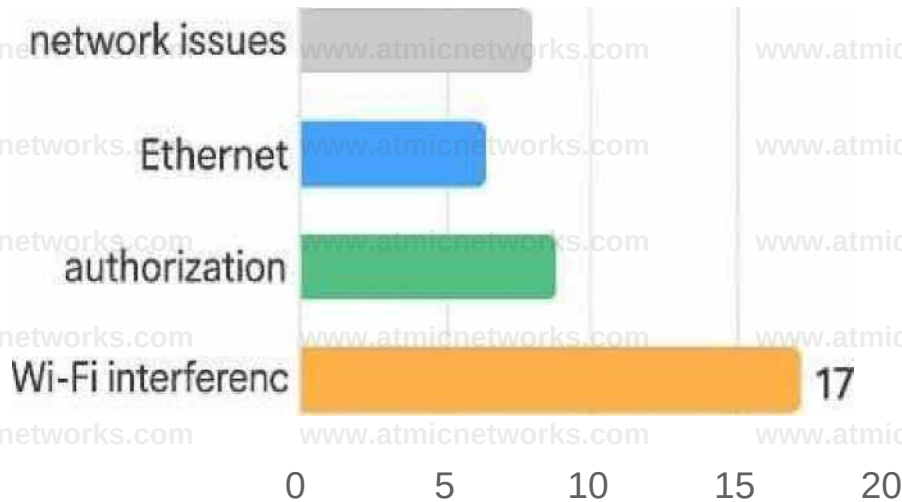
- Juniper Mist Cloud Licensing and Subscription Management Guide
 - Juniper Mist Organization and Device Lifecycle Documentation
 - Juniper Mist Cloud Operations and Entitlement Management Overview
-

Question: 32

Exhibit:

Capacity (last 7 days)

17%



Referring to the exhibit, which classifier was the largest contributor to 17% of the capacity issues?

- A. Network Issues
- B. Ethernet
- C. Authorization
- D. Wi-Fi Interference

Answer: D

Explanation:

Within the Juniper Mist Wireless Assurance dashboard, the Capacity SLE (Service Level Expectation) provides visibility into how well the network can handle concurrent users and traffic loads. It identifies the contributing factors, or classifiers, responsible for degraded capacity performance such as Wi-Fi interference, network issues, Ethernet problems, or authorization delays.

According to the Juniper Mist AI Operations and SLE Analytics Guide, the platform:

“Uses classifiers to break down SLE metrics and identify which network factors most heavily contribute to sub-threshold performance.”

In the exhibit, the Wi-Fi interference classifier has the longest bar reaching the full 17%, clearly showing it as the largest contributor to capacity degradation. Wi-Fi interference occurs when multiple APs or nearby wireless networks overlap on the same channel, resulting in increased contention, collisions, and reduced airtime availability — all of which impact overall capacity.

Therefore, the correct answer is D. Wi-Fi Interference.

Reference:

- Juniper Mist Wireless Assurance SLE and Classifier Documentation
- Juniper Mist AI Operations and Analytics Guide
- Juniper Mist Dashboard and Troubleshooting Insights Overview

Question: 33

Which statement is correct about the Super User account role?

- A. The Super User role has limited read/write capabilities.
- B. The Super User role is restricted to the specific sites that are defined when creating the user account.
- C. You must use the Super User role to claim an organization's new AP.
- D. You must use the Super User role to add administrators to an organization.

Answer: D

Explanation:

In the Juniper Mist Cloud platform, user roles define the scope of permissions that determine what administrative functions an individual can perform within an organization. The Super User role represents the highest level of administrative authority within a Juniper Mist organization and carries full control over both organization-wide and site-specific configurations.

According to the Juniper Mist Cloud Administration and User Management documentation, the Super User role is described as:

“The Super User role provides full read and write access across the entire organization. Only Super Users can manage organization-level settings, add or remove other administrators, and assign **privileges** to users.”

This means that only a Super User can add new administrators, manage subscription entitlements, configure organization-level policies, and perform full lifecycle device management. Unlike site administrators, Super Users are not restricted to specific locations—they have unrestricted visibility and control across all sites within the organization.

Therefore, the correct answer is D, since the Super User role is explicitly required to add administrators to an organization and perform top-level management operations.

Reference:

- Juniper Mist Cloud Administration and User Management Guide
- Juniper Mist Organization and Role-Based Access Control Documentation
- Juniper Mist Cloud Fundamentals and User Roles Study Guide

Question: 34

Mist AI collects and integrates data from multiple sources, including the data science and customer success teams and the domain experts. This process improves ML/AI accuracy. What is this process called?

- A. Anomaly detection
 - B. Mist AI efficacy loop
 - C. Bayesian inference
-

D. Marvis Actions

Answer: B

Explanation:

The Mist AI Efficacy Loop is a key concept within the Juniper Mist AI architecture that ensures continuous improvement of its machine learning (ML) and artificial intelligence (AI) models. This process combines feedback and data collected from multiple sources — including real-world network telemetry, customer success feedback, domain experts, and the Mist data science team — to refine the AI algorithms and enhance prediction accuracy.

According to the Juniper Mist AI Operations and Architecture Guide, the process is described as follows:

“The Mist AI efficacy loop is a closed-loop feedback system that continuously collects data from the field, correlates it with expert knowledge and support insights, and uses it to retrain and improve AI models for greater accuracy and reliability.”

This iterative learning cycle allows Mist AI to:

Improve anomaly detection precision.

Reduce false positives in network issue detection.

Enhance Marvis’s ability to accurately identify root causes and recommend corrective actions.

The efficacy loop is what differentiates Mist AI from static analytics platforms, as it creates a selflearning system that evolves with every deployment and customer interaction.

Therefore, the correct answer is B. Mist AI efficacy loop.

Reference:

- Juniper Mist AI Operations and Architecture Guide
 - Juniper Mist AI Cloud Fundamentals Documentation
 - Juniper Mist AI and Machine Learning Study Guide
-

Question: 35

Which two statements are correct about the switch configuration hierarchy in Juniper Mist? (Choose two.)

- A. The switch configuration cannot be managed at the organization level.
- B. The switch templates exist at the organization level.
- C. The switch templates exist at the site level.
- D. The switch-specific configuration cannot override switch templates.

Answer: B, C

Explanation:

The Juniper Mist Wired Assurance platform uses a hierarchical configuration model to manage switch settings efficiently across organizations and sites. This hierarchy provides flexibility by allowing administrators to apply global configurations through templates at the organization level, while also permitting site-specific customizations.

According to the Juniper Mist Wired Assurance Configuration and Template Management Guide, the configuration hierarchy functions as follows:

“Switch templates can be created at both the organization and site levels. Organization-level templates define global configurations, while site-level templates provide location-specific customization that overrides the organization-level settings where applicable.”

This structure enables consistent policy deployment while preserving site autonomy for unique configurations. For example, global VLAN or QoS configurations can be managed at the organization level, and local templates can adjust settings for switch ports or device groups at specific sites.

Switch-specific overrides are allowed within the hierarchy, ensuring flexibility in cases where unique port or feature configurations are required.

Therefore:

B is correct because switch templates exist at the organization level for global use.

C is correct because switch templates also exist at the site level for localized adjustments.

Reference:

- Juniper Mist Wired Assurance Configuration and Template Management Guide
- Juniper Mist Cloud Hierarchical Configuration Documentation
- Juniper Mist Wired Assurance and EX/QFX Management Overview

Question: 36

What are the principal types of machine learning for AI agents?

- A. Supervised, unsupervised, dynamic programming, and Q-learning
- B. Supervised, unsupervised, Markov decision process, and Bellman equation
- C. Supervised, unsupervised, clustering, and association rules
- D. Supervised, unsupervised, reinforcement, and deep learning

Answer: D

Explanation:

In the Juniper Mist AI ecosystem, the intelligence behind Mist's automation and insight generation is driven by machine learning (ML) and artificial intelligence (AI) models. These models enable Mist AI to identify trends, predict network issues, and automate remediation through the Marvis Virtual Network Assistant (VNA).

According to the Juniper Mist AI and Machine Learning Overview, Mist AI utilizes several core ML paradigms:

"Mist AI leverages supervised, unsupervised, reinforcement, and deep learning models to interpret telemetry data, recognize behavioral patterns, and make predictive adjustments for network optimization."

Supervised Learning – Uses labeled data for training, allowing Mist AI to identify known issues (e.g., DHCP failures or high latency).

Unsupervised Learning – Detects anomalies or patterns in unlabeled datasets (e.g., identifying abnormal client behavior).

Reinforcement Learning – Continuously improves network performance by using feedback from outcomes of previous actions.

Deep Learning – Employs neural network models for complex pattern recognition and predictive analytics.

These combined learning approaches enable Mist AI to evolve autonomously and maintain accuracy through its AI efficacy loop.

Therefore, the correct answer is D. Supervised, unsupervised, reinforcement, and deep learning.

Reference:

- Juniper Mist AI and Machine Learning Overview
- Juniper Mist AI Cloud Architecture and Predictive Analytics Guide
- Juniper Mist Marvis Virtual Network Assistant Technical Documentation

Question: 37

Which statement is true about Radio Resource Management (RRM)?

- A. The RRM event-driven system automatically runs once a day.
- B. The RRM global optimization system automatically runs every hour.
- C. The RRM event-driven system automatically runs every hour.
- D. The RRM global optimization system automatically runs once a day.

Answer: D

Explanation:

Radio Resource Management (RRM) is a key feature of Juniper Mist Wireless Assurance that uses AI-driven automation to dynamically adjust radio settings across access points (APs) for optimal wireless performance. The RRM engine ensures proper channel assignment, transmit power control, and interference management across the network.

According to the Juniper Mist Wireless Assurance and AI-Driven RRM Guide, RRM operates in two modes:

Event-Driven RRM:

This mode reacts immediately to real-time changes in the RF environment, such as new access points, interference spikes, or client density changes.

Global Optimization RRM:

This process runs as a scheduled, system-wide optimization once per day to evaluate the overall RF environment and redistribute channels and power settings network-wide for the best balance of coverage and capacity.

The documentation states:

“The RRM global optimization algorithm automatically executes once daily to ensure optimal channel and power planning across all APs.”

Thus, the correct answer is D – The RRM global optimization system automatically runs once a day.

Reference:

- Juniper Mist Wireless Assurance and RRM Configuration Guide
- Juniper Mist AI-Driven Radio Resource Optimization Documentation
- Juniper Mist Cloud Operations and RF Management Overview

Question: 38

Which Juniper device is used in Routing Assurance?

- A. MX Series
 - B. EX Series Switches
 - C. Session Smart Routers
 - D. SRX Series Firewalls
-

Answer: C

Explanation:

Routing Assurance is a feature of the Juniper Mist WAN Assurance solution, providing AI-driven visibility, analytics, and troubleshooting for Juniper Session Smart Routers (SSR) deployed in SD-WAN environments. The system monitors routing performance, link health, and application traffic to ensure reliable WAN connectivity and performance.

According to the Juniper Mist WAN Assurance and Routing Assurance Guide, the feature is described as:

“Routing Assurance provides continuous monitoring of routing operations and path decisions for Juniper Session Smart Routers, offering AI-driven insights into application routing behavior and WAN path health.”

The Session Smart Router (SSR) platform—powered by 128 Technology (acquired by Juniper Networks)—is specifically designed for AI-driven, session-aware routing. It integrates seamlessly with Mist Cloud to:

Track routing changes and path selection decisions.

Correlate application experience with routing behavior.

Identify and remediate path-related issues automatically through Marvis AI.

Other devices serve different functions:

MX Series – Carrier-grade routing, not used in Mist Routing Assurance.

EX Series – Switches used for Wired Assurance.

SRX Series – Firewalls supporting WAN Assurance and security but not Routing Assurance.

Therefore, the correct answer is C. Session Smart Routers.

Reference:

– Juniper Mist WAN Assurance and Routing Assurance Guide

– Juniper Mist Cloud SD-WAN Operations Documentation

– Juniper Session Smart Router Technical Overview

Question: 39

Which two statements are correct when considering Juniper Mist clouds? (Choose two.)

- A. Users created in a specific regional cloud can manage organizations in other clouds.
- B. Users created in a specific regional cloud can only manage organizations in that cloud.
- C. Creating a new user enables the user only for the cloud in which it was created.
- D. Creating a new user enables the user across all clouds.

Answer: B, C

Explanation:

The Juniper Mist Cloud operates as a regionally distributed cloud infrastructure, where each geographic region (for example, US, EU, APAC) hosts its own isolated Mist Cloud instance. This design ensures compliance with regional data privacy regulations, improves network performance, and enhances scalability and reliability.

According to the Juniper Mist Cloud Administration and Operations Guide, user accounts and organizations are region-specific, meaning:

“Users and organizations exist within specific regional Mist Clouds. A user account created in one regional cloud is valid only within that region and cannot be used to access organizations hosted in another cloud.”

This structure ensures data sovereignty and security while maintaining logical separation between regions. When administrators create a new user, that user’s credentials and access privileges apply only to the Mist Cloud region in which the user was created.

Therefore:

B is correct because users created in a regional cloud can only manage organizations within that same cloud.

C is correct because a newly created user is enabled only for the regional cloud where it was registered.

Options A and D are incorrect because Mist Clouds are isolated — cross-region user or organization access is

not supported.

Reference:

- Juniper Mist Cloud Administration and Operations Guide
- Juniper Mist Cloud Regional Deployment and Data Residency Documentation
- Juniper Mist Cloud Fundamentals and Architecture Study Guide

Question: 40

Exhibit:

Coverage

Successful:
79%

Unsuccessful
21%

Referring to the exhibit, which percentage of Coverage was unsuccessful?

- A. 9%
- B. 21%
- C. 79%
- D. 15%

Answer: B

Explanation:

In Juniper Mist Wireless Assurance, the Coverage SLE (Service Level Expectation) measures the quality and consistency of Wi-Fi signal coverage across an organization's wireless infrastructure. It provides insight into how well clients can connect to access points with sufficient signal strength and quality.

According to the Juniper Mist AI Operations and Analytics Guide, the Coverage SLE is defined as:

"The percentage of client connections that meet the minimum signal strength threshold required for satisfactory performance. Sub-threshold values represent areas where coverage is inadequate or inconsistent."

In the exhibit, the SLE visualization shows 79% successful coverage and 21% unsuccessful coverage, meaning that 21% of connection attempts or client areas did not meet the desired signal strength threshold. These failures may be caused by factors such as:

Insufficient AP density or placement.

RF interference from neighboring devices.

Physical obstructions impacting signal propagation.

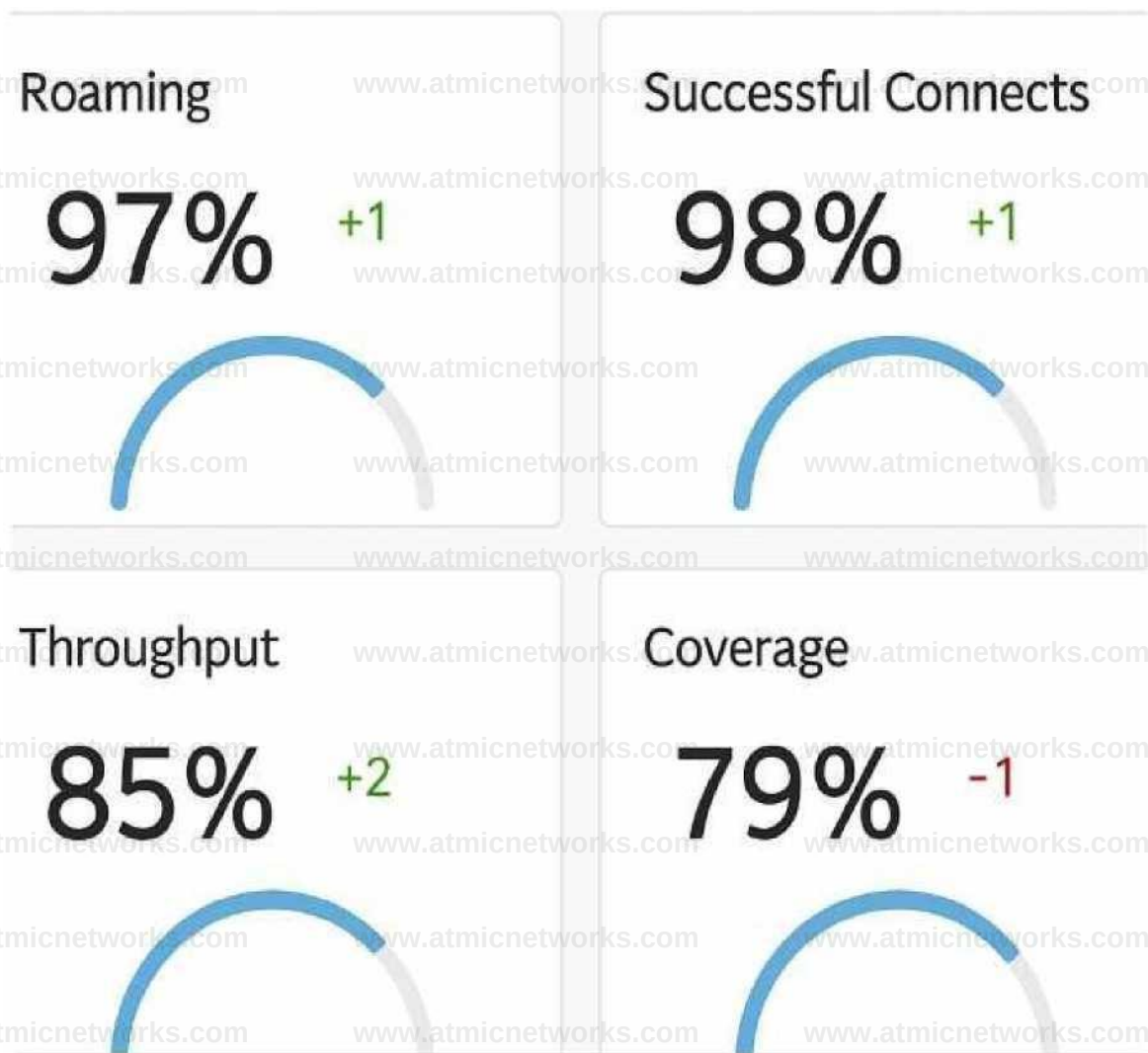
Thus, the unsuccessful coverage percentage is 21%, indicating potential areas where additional APs or configuration optimization may be needed to improve user experience.

Reference:

- Juniper Mist Wireless Assurance and SLE Documentation
- Juniper Mist AI Operations and Troubleshooting Guide
- Juniper Mist Cloud Analytics and Coverage Metrics Overview

Question: 41

Exhibit:



Referring to the exhibit, which SLE would an administrator investigate to troubleshoot weak signal issues?

- A. Roaming
- B. Successful Connects
- C. Throughput
- D. Coverage

Answer: D

Explanation:

In Juniper Mist Wireless Assurance, Service Level Expectations (SLEs) are key metrics that measure different aspects of the end-user experience. Each SLE focuses on a distinct area of network performance such as Connection, Roaming, Throughput, and Coverage.

The Coverage SLE specifically measures whether wireless clients are receiving adequate signal strength (RSSI) and signal quality (SNR) from access points. According to the Juniper Mist AI Operations and SLE Analytics Guide, this metric is defined as:

“The Coverage SLE quantifies the percentage of client sessions that meet the required signal strength and quality thresholds. Low coverage indicates areas with weak or inconsistent RF signal levels.”

When users experience weak signal or dead zones, the Coverage SLE provides insight into where and why these issues occur. Mist AI identifies sub-classifiers such as Signal Quality, Wi-Fi Interference, or Airtime Utilization, allowing administrators to isolate the cause of poor signal conditions.

Therefore, in the exhibit shown, an administrator would investigate the Coverage SLE (79%), as it directly relates to signal weakness or RF coverage problems.

Reference:

- Juniper Mist Wireless Assurance and SLE Documentation
- Juniper Mist AI Operations and Analytics Guide
- Juniper Mist Cloud Dashboard and RF Monitoring Overview

Question: 42

Your company hosts its own enterprise-wide monitoring solution. You want to receive events from Juniper Mist.

How would you accomplish this task?

- A. Using the API
- B. Sending an e-mail
- C. Using a webhook
- D. Using a WebSocket

Answer: C

Explanation:

In the Juniper Mist Cloud, webhooks are used to send real-time event notifications from Mist Cloud to external systems such as third-party monitoring or automation platforms. This integration mechanism allows administrators to collect alerts, status changes, and analytics data directly from Mist Cloud without the need for constant API polling.

According to the Juniper Mist API and Webhook Integration Guide, webhooks are defined as:

“A push-based communication method that enables Juniper Mist Cloud to send event data to a customer-defined HTTP endpoint when specific network events occur.”

This capability allows seamless integration with enterprise monitoring solutions such as ServiceNow, Splunk, or Datadog, enabling organizations to centralize event management.

The other options are not suitable:

A (API): APIs are pull-based and require polling for updates, not push notifications.

B (Email): Not supported for automated system-to-system event delivery.

D (WebSocket): Used for live telemetry and streaming data (e.g., client updates), not event alerts.

Therefore, the correct method is C. Using a webhook.

Reference:

- Juniper Mist API and Webhook Developer Documentation
- Juniper Mist Cloud Automation and Integration Guide
- Juniper Mist Cloud Operations Overview

Question: 43

Which Juniper Mist feature tracks the location of important devices and objects within a building?

A. Wireless Assurance

B. IoT Assurance

C. Asset Visibility

D. User Engagement

Answer: C

Explanation:

The Juniper Mist Asset Visibility service provides real-time tracking and visibility for important devices and objects within indoor environments such as hospitals, offices, or warehouses. It uses Bluetooth Low Energy (BLE) technology and Mist vBLE-enabled access points to determine the precise location of tagged assets.

According to the Juniper Mist Location Services Guide, the feature is defined as:

“Asset Visibility leverages virtual Bluetooth LE technology and BLE tags to locate and track assets on floor plans in real time, providing actionable location-based intelligence.”

Key functionalities include:

Tracking BLE-tagged assets such as medical equipment, IT devices, or inventory.

Displaying live location information on floor maps.

Integrating with external asset management or workflow systems.

While User Engagement focuses on customer-facing location experiences (e.g., navigation or proximity marketing), Asset Visibility is designed specifically for internal asset monitoring and operational efficiency.

Therefore, the correct answer is C. Asset Visibility.

Reference:

– Juniper Mist Location-Based Services and Asset Visibility Guide

– Juniper Mist AI for Asset Tracking and BLE Technology Overview

– Juniper Mist Cloud Location Services Documentation

Question: 44

What is the purpose of assigning roles to switches?

- A. To configure WLANs
- B. To manage user accounts
- C. To assign configurations at scale
- D. To monitor network traffic

Answer: C

Explanation:

In Juniper Mist Wired Assurance, assigning roles to switches is a key configuration mechanism for deploying consistent network policies across multiple devices. Switch roles act as logical identifiers that bind devices to specific configuration templates or policy profiles, ensuring standardized setup and reducing manual configuration overhead.

According to the Juniper Mist Wired Assurance Configuration and Template Management Guide:

“Switch roles are used to group devices based on function or location and automatically apply predefined configuration templates and policies at scale.”

This enables administrators to:

Automatically assign VLANs, port profiles, and policies to multiple switches simultaneously.

Simplify deployment for large organizations with multiple sites.

Ensure uniform compliance with enterprise configuration standards.

Roles are not used to configure WLANs (wireless function), manage users, or directly monitor traffic — those tasks are handled through other Mist AI services.

Therefore, the correct answer is C. To assign configurations at scale.

Reference:

- Juniper Mist Wired Assurance Configuration and Template Management Guide
- Juniper Mist Cloud Administration Guide
- Juniper Mist Wired Assurance Operations Documentation

Question: 45

In the Mist UI, what should you do to support mobile device engagement?

- A. Enable vBLE
- B. Use Wi-Fi 6
- C. Enable Local Status Page
- D. Use ESL

Answer: A

Explanation:

To support mobile device engagement within the Juniper Mist Cloud UI, you must enable virtual Bluetooth Low Energy (vBLE). The vBLE functionality allows Mist Access Points (APs) to transmit Bluetooth beacons that interact with mobile devices running location-aware applications. This capability is essential for user engagement services such as indoor navigation, proximity

notifications, and personalized customer interactions.

According to the Juniper Mist Location-Based Services Configuration Guide, the process is defined as follows:

“To enable mobile engagement and location-based experiences, the vBLE feature must be activated on supported Mist Access Points. Once enabled, APs transmit programmable BLE signals that communicate with mobile devices through the Mist SDK.”

Enabling vBLE allows administrators to:

Provide wayfinding and push notification services within indoor environments.

Support mobile app integration through the Mist Location SDK.

Customize engagement campaigns via virtual beacons without requiring physical beacon hardware.

Other options are incorrect because:

Wi-Fi 6 improves wireless efficiency but is unrelated to BLE-based engagement.

Local Status Page is used for AP health monitoring, not engagement.

ESL (Electronic Shelf Labels) applies to retail price display systems, not user interaction.

Therefore, the correct answer is A. Enable vBLE.

Reference:

- Juniper Mist Location-Based Services Configuration and Deployment Guide
- Juniper Mist vBLE and Mobile Engagement Overview
- Juniper Mist Cloud User Engagement and SDK Integration Documentation

Question: 46

Exhibit:

mist Subscriptions



Subscriptions Summary

103

Devices

82

Sites

418

Unused

Devices

103 Devices

Sites

82 Sites

15 Unused

Subscriptions

Marvis for Wireless

418 / 500

Referring to the exhibit, how many sites have unused Marvis for Wireless subscriptions?

- A. 418
- B. 15
- C. 82
- D. 21

Answer: B

Explanation:

In the Juniper Mist Cloud, the Subscriptions page provides administrators with detailed information about the status of service licenses and subscriptions associated with devices, sites, and organizations. This includes visibility into the number of active devices, sites, and any unused subscriptions across the organization.

According to the Juniper Mist Cloud Licensing and Subscription Management Guide, the “Sites” section under Subscriptions Summary shows:

“The total number of configured sites within the organization and the number of sites that currently do not have assigned subscriptions.”

In the exhibit, the summary shows:

82 Sites total

15 Unused sites

This indicates that 15 sites currently have no active or assigned Marvis for Wireless subscriptions. The “Unused” label under Sites refers specifically to the count of sites not yet utilizing their allocated subscription entitlements.

Therefore, the correct answer is B. 15.

Reference:

- Juniper Mist Cloud Licensing and Subscription Management Guide
- Juniper Mist Cloud Administration and Operations Documentation
- Juniper Mist AI Service Subscription Overview

Question: 47

What are two guest portal authentication options in the UI? (Choose two.)

- A. Authentication Code
- B. MAC Authentication

C. Sponsored Guest

D. SAML

Answer: A, C

Explanation:

In Juniper Mist Cloud, guest access is managed through the Guest Portal feature, which allows administrators to configure secure and flexible authentication methods for temporary or visitor access. These options are designed to provide a balance between user convenience and network security.

According to the Juniper Mist Guest Access and Captive Portal Configuration Guide, the supported authentication options include:

“Authentication Code (Self-registration) and Sponsored Guest workflows, among others, which provide different levels of administrative control and ease of use.”

Authentication Code (A):

Visitors receive a temporary authentication code (PIN) via email or SMS that they use to log in. This method is ideal for self-service access while maintaining accountability.

Sponsored Guest (C):

In this mode, guests must be approved by a designated employee or sponsor before gaining access. This adds an extra layer of security by involving internal personnel validation.

MAC Authentication (B) and SAML (D) are not used for guest portals; they are designed for devicebased authentication and enterprise-level identity federation, respectively.

Reference:

- Juniper Mist Guest Access and Captive Portal Configuration Guide
- Juniper Mist Cloud Administration and Access Management Documentation
- Juniper Mist Wireless Assurance Guest Network Overview

Question: 48

You are asked to configure WPA3/Enterprise (802.1X) security on the corporate employee SSID on **every** access point in your multi-site organization.

Which Juniper Mist template would you use for this task?

- A. Switch template
- B. WAN Edge template
- C. WLAN template
- D. RF template

Answer: C

Explanation:

In the Juniper Mist Cloud architecture, a WLAN template is used to define wireless network parameters, including SSIDs, authentication methods, and access control settings. These templates allow administrators to apply consistent Wi-Fi configurations across multiple access points and sites.

According to the Juniper Mist Wireless Assurance Configuration Guide, the WLAN template:

“Defines the configuration for SSIDs, including security mode (WPA2, WPA3, 802.1X), authentication servers, VLAN assignment, and user access policies.”

To configure WPA3/Enterprise (802.1X) security for employee SSIDs, administrators must create or edit a WLAN template and select WPA3-Enterprise as the security type. The template can then be associated with all sites in the organization, ensuring uniform deployment.

Other template types serve different purposes:

Switch template: Used for wired configuration and port profiles.

WAN Edge template: Used for SD-WAN and WAN Assurance configurations.

RF template: Used to manage radio parameters such as channel, power, and band.

Therefore, the correct answer is C. WLAN template.

Reference:

- Juniper Mist Wireless Assurance Configuration and Deployment Guide
- Juniper Mist Cloud WLAN Template Management Documentation
- Juniper Mist Cloud Organization and Site Configuration Overview

Question: 49

You want to change the default language for your Juniper Mist portal.

What will accomplish this task?

- A. Select your ranked language choice from the Alerts page.
- B. Input your primary language in the My Accounts page.
- C. Define your language using Organization templates.
- D. Use the Change Language drop-down list of the Juniper Mist portal.

Answer: D

Explanation:

The Juniper Mist Cloud portal provides a user-friendly interface that supports multiple languages to enhance accessibility for global users. The language preference determines the display language for

menus, dashboards, and configuration pages across the Mist UI.

According to the Juniper Mist Cloud Administration Guide, the portal's language can be modified as follows:

“Users can change the display language of the Mist portal using the Change Language drop-down list

located in the upper-right corner of the interface.”

This option allows users to immediately switch the UI language without affecting other users in the organization or requiring administrative permissions. The change is applied per user profile and is stored for future sessions.

Other listed options are invalid:

A: The Alerts page does not include language settings.

B: The My Account page shows personal info but not display language options.

C: Organization templates are unrelated to UI preferences.

Therefore, the correct answer is D. Use the Change Language drop-down list of the Juniper Mist portal.

Reference:

– Juniper Mist Cloud Administration and User Interface Guide

– Juniper Mist Cloud Portal User Preferences Documentation

– Juniper Mist Cloud Fundamentals and Globalization Overview

Question: 50

When viewing the LATEST UPDATES on the Marvis Actions page, you see an action labeled AI VALIDATED.

What does this status mean?

A. The issue was identified and resolved entirely by Marvis.

B. The issue is unresolved.

C. The issue is resolved but was not manually marked resolved.

D. The issue was marked resolved by an administrator.

Answer: A

Explanation:

In the Juniper Mist Marvis Actions dashboard, issues and recommendations are displayed with status labels indicating their progress and resolution method. One of these statuses is AI VALIDATED, which signifies that the issue was automatically detected, diagnosed, and resolved by Marvis AI without requiring manual intervention.

According to the Juniper Mist Marvis Virtual Network Assistant Operations Guide:

“AI VALIDATED indicates that Marvis has confirmed and resolved a network issue autonomously using AI-driven automation and telemetry correlation.”

This means Marvis performed the full troubleshooting cycle—identifying the anomaly, validating its cause, and confirming resolution—based on continuous monitoring and real-time network analytics.

Other statuses include:

UNRESOLVED: Issue is ongoing and needs attention.

RESOLVED: Marked manually by an administrator after resolution.

AI VALIDATED: Confirmed and closed automatically by Marvis AI.

Therefore, the correct answer is A. The issue was identified and resolved entirely by Marvis.

Reference:

- Juniper Mist Marvis Virtual Network Assistant Operations Guide
- Juniper Mist AI Actions and Insights Documentation
- Juniper Mist Cloud Analytics and Troubleshooting Overview

Question: 51

How does Marvis detect a bad cable problem?

A. Marvis constantly sends ping packets to remote end hosts to determine whether there is a failure in the path.

-
- B. Marvis randomly performs packet captures on various APs to find bad cables in your network.
 - C. Marvis randomly performs cable tests on every cable in your network.
 - D. Marvis analyzes metrics, such as interface errors, that match a bad cable pattern.

Answer: D

Explanation:

Marvis, the AI-driven Virtual Network Assistant in Juniper Mist, uses continuous telemetry analysis and AI correlation to identify bad cable conditions. It does this by examining interface-level statistics gathered from switches and access points through Wired Assurance.

According to the Juniper Mist Marvis Operations and Troubleshooting Guide:

“Marvis detects bad cable issues by analyzing telemetry patterns such as CRC errors, FCS errors, packet drops, and link flaps that collectively match a known cable fault signature.”

When such patterns are detected, Marvis automatically generates an AI Action indicating a Bad Cable issue and identifies whether the problem is with the port or the cable. This proactive detection allows administrators to replace faulty hardware before it impacts network users.

Options A, B, and C are incorrect because Marvis does not perform active ping, random packet captures, or random cable testing. Its detection is entirely AI and telemetry-based.

Therefore, the correct answer is D. Marvis analyzes metrics, such as interface errors, that match a bad cable pattern.

Reference:

- Juniper Mist Marvis AI Operations Guide
- Juniper Mist Wired Assurance and Telemetry Analytics Documentation
- Juniper Mist AI Troubleshooting and Automation Overview

Question: 52

Which statement about microservices is correct?

-
- A. Microservices are designed to be independent to ensure that if one process fails, the remaining processes will continue to operate.
 - B. Microservices communicate with each other using Network Configuration Protocol (NETCONF).
 - C. Microservices are developed as a complete application set, and updates require the modification of the entire application.
 - D. Microservices must share a common database to ensure data integrity.

Answer: A

Explanation:

The Juniper Mist Cloud architecture is built on a microservices-based design, which enhances reliability, scalability, and operational efficiency. Each microservice performs a specific function—such as authentication, telemetry ingestion, analytics, or AI inference—independently of other components.

According to the Juniper Mist Cloud Architecture and Operations Guide:

“Mist Cloud leverages a microservices architecture where each service operates independently. This design ensures that a failure in one service does not impact the functionality or availability of others.”

This modular approach provides several key advantages:

Fault isolation: One component can fail or restart without affecting the rest of the system.

Independent scaling: Services can scale dynamically based on demand.

Continuous updates: New features and patches can be deployed without downtime.

Options B, C, and D are incorrect because Mist microservices do not rely on NETCONF for internal communication, are not monolithic, and do not share a single common database—each maintains its own data model as required.

Therefore, the correct answer is A. Microservices are designed to be independent to ensure that if one process fails, the remaining processes will continue to operate.

Reference:

- Juniper Mist Cloud Architecture and Operations Guide
 - Juniper Mist AI Platform and Microservices Overview
-

Question: 53

Which data format is transmitted during a Juniper Mist API request?

- A. CSV
- B. XML
- C. YAML
- D. JSON

Answer: D

Explanation:

The Juniper Mist Cloud API follows RESTful API design principles, enabling programmatic access to all Mist Cloud functions such as device management, configuration, analytics, and monitoring. REST

APIs in Mist use a lightweight and standardized data exchange format to facilitate seamless integration with third-party applications and automation frameworks.

According to the Juniper Mist API Developer Guide:

“All Juniper Mist Cloud API requests and responses are transmitted in JavaScript Object Notation (JSON) format. JSON is used because it is lightweight, easy to parse, and compatible with all modern programming environments.”

JSON is the preferred format because it is both human-readable and machine-efficient, allowing for fast serialization and deserialization of data structures.

Other formats such as CSV, XML, and YAML are not used for API communication within the Mist Cloud architecture.

Therefore, the correct answer is D. JSON.

Reference:

-
- Juniper Mist API Developer Guide
 - Juniper Mist Cloud Automation and Integration Overview
 - Juniper Mist Cloud Fundamentals Study Guide

Question: 54

Which statement about microservices is correct?

- A. Microservices communicate with each other using APIs.
- B. Microservices are developed as a suite of applications and rely on developers to deliver updates to the entire suite at once.
- C. Microservices are designed to be dependent on each other to ensure that if one process fails, the remaining processes will not continue to operate.
- D. Microservices must share a common database to ensure data integrity.

Answer: A

Explanation:

The Juniper Mist Cloud platform is built on a microservices-based architecture, where individual software components perform specific functions and communicate using well-defined Application Programming Interfaces (APIs).

According to the Juniper Mist Cloud Architecture and Operations Guide:

“Microservices communicate through secure APIs, allowing independent services to interact seamlessly while maintaining modularity and isolation.”

This architectural design provides major operational benefits, including:

Independent scalability – each service can scale based on workload demand.

Fault isolation – failures in one service do not affect others.

Continuous deployment – updates can be made to one service without impacting the rest of the platform.

Incorrect options:

B: Juniper Mist microservices are independently updated, not deployed as one suite.

C: They are independent, not dependent on one another.

D: Each microservice maintains its own data model; they do not rely on a single shared database.

Thus, the correct answer is A. Microservices communicate with each other using APIs.

Reference:

– Juniper Mist Cloud Architecture and Operations Guide

– Juniper Mist Cloud Fundamentals Study Guide

– Juniper Mist AI and Microservices Overview

Question: 55

What happens to the captured data after a packet capture is stopped or completed?

A. It is saved as a downloadable capture file for offline inspection.

B. It remains permanently in the cloud for continuous analysis.

C. It triggers alerts based on detected issues within the captured traffic.

D. It is automatically discarded due to limited storage space.

Answer: A

Explanation:

The packet capture feature in Juniper Mist Cloud allows administrators to remotely capture live network traffic from managed devices such as Access Points (APs) or switches for detailed troubleshooting.

According to the Juniper Mist Network Troubleshooting and Diagnostics Guide:

“Once a packet capture session is stopped or completed, the captured data is saved as a downloadable .pcap file that can be analyzed offline using tools such as Wireshark.”

This ensures administrators can inspect packet-level details for issues such as authentication failures, DHCP errors, or connectivity drops. The data is stored temporarily and made available through the Mist UI for download before automatic cleanup.

Options B, C, and D are incorrect because captured data is not stored permanently in the cloud, does not trigger automated alerts, and is not discarded immediately. The purpose is to make the data accessible for offline inspection and analysis.

Therefore, the correct answer is A. It is saved as a downloadable capture file for offline inspection.

Reference:

- Juniper Mist Network Troubleshooting and Diagnostics Guide
- Juniper Mist Cloud Administration and Operations Documentation
- Juniper Mist AI Operations and Support Tools Overview

Question: 56

Your organization has a Marvis subscription. You have an issue with an access point (AP) that does not power on. You decide to open a support ticket.

In this scenario, what does Marvis do while you are filling in the details on the New Ticket screen?

- A. Marvis creates the support tickets.
- B. Marvis sends an e-mail to support@juniper.net on your behalf.
- C. Marvis provides links to Internet resources about AP power problems.
- D. Marvis provides possible solutions to AP power problems from the Juniper Mist documentation.

Answer: D

Explanation:

When an administrator begins to open a support ticket within the Juniper Mist portal, the Marvis Virtual Network Assistant proactively assists by presenting relevant, AI-driven recommendations and documentation.

According to the Juniper Mist Marvis Virtual Network Assistant Guide, this process is described as:

“While an administrator creates a support case, Marvis automatically searches the Mist knowledge base and presents probable causes and recommended solutions based on the detected issue type.”

If the issue involves an AP that does not power on, Marvis retrieves contextual data such as PoE status, switch port state, and recent telemetry logs, then provides automated guidance—for example, checking PoE configurations or cable connectivity.

Thus, while the administrator fills in the “New Ticket” details, Marvis provides potential solutions directly from Juniper Mist’s documentation, potentially resolving the issue before a support case is even submitted.

The correct answer is D. Marvis provides possible solutions to AP power problems from the Juniper Mist documentation.

Reference:

- Juniper Mist Marvis Virtual Network Assistant User Guide
- Juniper Mist AI Operations and Support Automation Documentation
- Juniper Mist Cloud Case Creation and Marvis Integration Overview

Question: 57

Which Juniper Mist product enables the onboard Bluetooth Low Energy (BLE) antenna array for listen-only mode?

- A. Access Assurance
- B. Wi-Fi Management and Assurance
- C. vBLE Engagement
- D. Asset Visibility

Answer: D

Explanation:

In Juniper Mist's Location-Based Services, the Asset Visibility service utilizes the built-in Bluetooth Low Energy (BLE) antenna array within Mist Access Points to track BLE tags and devices in listen-only mode. This allows the APs to receive BLE signals emitted by assets and compute their real-time location using angle-of-arrival (AoA) and RSSI-based triangulation.

According to the Juniper Mist Asset Visibility and Location Services Guide:

"When operating in Asset Visibility mode, the vBLE antenna array in Mist Access Points functions in listen-only mode, collecting BLE chirps from asset tags and relaying this data to the Mist Cloud for location determination."

This configuration differs from vBLE Engagement, where APs transmit BLE beacons to interact with mobile apps. In Asset Visibility, the BLE array passively listens to track tagged assets (e.g., equipment, IoT devices) across a defined floor map.

Therefore, the correct answer is D. Asset Visibility.

Reference:

- Juniper Mist Asset Visibility and Location-Based Services Configuration Guide
- Juniper Mist vBLE Architecture Overview
- Juniper Mist Cloud Location Services Documentation

Question: 58

What is responsible for Mist AI data collection and analysis across the wireless, wired, and WAN domains?

- A. Predictive Analytics and Correlation Engine (PACE)
- B. Juniper Mist Full Stack
- C. Marvis VNA
- D. Data Science

Answer: A

Explanation:

The Predictive Analytics and Correlation Engine (PACE) is the core AI and data analytics component of the Juniper Mist Cloud architecture. It collects, processes, and correlates telemetry data across all

managed domains — Wireless, Wired, and WAN Assurance — to deliver proactive insights and predictive network intelligence.

According to the Juniper Mist AI Operations and Architecture Guide:

“The Predictive Analytics and Correlation Engine (PACE) serves as the foundation of Mist AI, using continuous telemetry ingestion and machine learning algorithms to understand, correlate, and predict network behaviors across the wireless, wired, and WAN environments.”

PACE enables Mist AI to:

Detect anomalies in user experience and device performance.

Predict failures before they affect users.

Correlate events across network domains for root-cause analysis.

Therefore, the correct answer is A. Predictive Analytics and Correlation Engine (PACE).

Reference:

- Juniper Mist AI Cloud Architecture and Operations Guide
- Juniper Mist AI Fundamentals Study Guide
- Juniper Mist Predictive Analytics and Correlation Engine Overview

Question: 59

Your manager asks you to configure all your remote Juniper EX Series switches to use Dynamic Port Configuration.

In this scenario, what are two criteria used for matching connected devices and assigning them their correct port and VLAN? (Choose two.)

A. Serial Number

B. IP Address

C. LLDP Chassis ID

D. MAC Address

Answer: C, D

Explanation:

Dynamic Port Configuration (DPC) in Juniper Mist Wired Assurance allows EX Series switches to automatically assign port profiles, VLANs, and policies to connected devices based on their unique identifiers. This automation simplifies switch management and ensures consistent configurations across distributed networks.

According to the Juniper Mist Wired Assurance Configuration and Dynamic Port Management Guide:

“Dynamic Port Configuration matches connected endpoints using identifiers such as LLDP chassis ID and MAC address to assign the appropriate port profile or VLAN automatically.”

LLDP Chassis ID (C): Identifies the connected device by its LLDP advertisement, often representing a switch, phone, or AP.

MAC Address (D): Provides unique device identification, ensuring precise port and VLAN assignment even when LLDP data is unavailable.

Options A (Serial Number) and B (IP Address) are not used for port configuration matching in DPC because they are not always available at the time of link establishment.

Therefore, the correct answers are C. LLDP Chassis ID and D. MAC Address.

Reference:

– Juniper Mist Wired Assurance Configuration and Dynamic Port Management Guide

– Juniper Mist Cloud Operations and Template Management Documentation

– Juniper Mist EX Switch Dynamic Port Assignment Overview

Question: 60

Which Juniper Mist location-based service improves accuracy?

- A. Proximity Detection
- B. User Engagement
- C. Asset Visibility
- D. Wi-Fi Location

Answer: C

Explanation:

Among Juniper Mist's Location-Based Services, Asset Visibility provides the most accurate location tracking capabilities. This is achieved through the use of vBLE (virtual Bluetooth Low Energy) technology, which leverages a patented 16-element BLE antenna array integrated into Mist Access Points for Angle of Arrival (AoA) calculations.

According to the Juniper Mist Location-Based Services Technical Overview:

"Asset Visibility delivers sub-meter location accuracy by using BLE-based triangulation combined with Mist AI's machine learning algorithms for continuous calibration."

While Wi-Fi location offers approximate device tracking based on signal strength and triangulation, and Proximity Detection identifies nearby devices, Asset Visibility provides precise real-time tracking of BLE-tagged objects and devices.

User Engagement, on the other hand, focuses on customer-facing mobile interactions, not accuracy optimization.

Therefore, the correct answer is C. Asset Visibility.

Reference:

- Juniper Mist Location-Based Services and Asset Visibility Documentation
- Juniper Mist vBLE Architecture Overview
- Juniper Mist Cloud Location Accuracy Optimization Guide

Question: 61

Exhibit:

EVENT

Apr 23, 2024 1:45:25 PM  packet_loss

[Download Packet Capture](#)

[Download Traceroute](#)

CLIENT INFO

IP MAC I Hotname

SSID Example-SSID

10.0.0.1 in AP

EXAMPLE-AP

SSID 10.0.0.11 ix CHAP

Signal -54 dBm

Channel 36

Referring to the exhibit, which two statements are correct about this client event? (Choose two.)

- A. A traceroute file is included.
- B. It is a wireless client.
- C. A dynamic packet capture file is included.
- D. It is a wired client.

Answer: B, C

Explanation:

In the Juniper Mist Cloud, the Client Events section within the Monitoring interface displays detailed event logs for both wired and wireless clients, providing insights into connectivity, authentication, and performance-related activities. Each event entry may include associated diagnostic files such as dynamic packet captures (DPCs), traceroute data, and syslogs depending on the event type and device context.

According to the Juniper Mist AI Operations and Client Event Diagnostics Guide, the platform states:

“Wireless client events provide correlation between client connection attempts and associated diagnostic artifacts such as dynamic packet captures. These files are generated automatically during troubleshooting events and are attached to the event log for administrator review.”

From the exhibit, the client is shown as a wireless device, indicated by the Wi-Fi icon and the SSID association information visible in the event details. Additionally, the entry confirms that a dynamic packet capture (DPC) file was automatically generated for the event, allowing engineers to download and inspect packet-level activity for root-cause analysis.

Therefore:

B (It is a wireless client) is correct — the event pertains to a Wi-Fi-connected device.

C (A dynamic packet capture file is included) is correct — the log includes a downloadable DPC file.

Reference:

- Juniper Mist AI Operations and Client Event Diagnostics Guide
- Juniper Mist Wireless Assurance Troubleshooting Documentation
- Juniper Mist Cloud Monitoring and Analytics Overview

Question: 62

In Juniper Mist, which three devices send data to the Juniper Mist Cloud? (Choose three.)

A. Syslog Server

-
- B. Access Point
 - C. Session Smart Router
 - D. Juniper Mist Edge
 - E. RADIUS Server

Answer: B, C, D

Explanation:

In the Juniper Mist Cloud architecture, data is collected and streamed from various edge devices to the Mist Cloud platform, where AI-driven analytics, automation, and telemetry correlation occur. Only Mist-managed devices that are cloud-connected contribute operational telemetry data to Mist AI for analysis.

According to the Juniper Mist Cloud Architecture and Operations Guide:

“Access Points, Juniper Mist Edge devices, and Session Smart Routers (SSR) communicate directly with the Mist Cloud, sending telemetry, configuration, and analytics data in real time.”

Access Points (B): Provide wireless client telemetry, RF statistics, and user SLE (Service Level Expectation) data.

Session Smart Routers (C): Supply WAN Assurance and routing analytics, including path and session health data.

Juniper Mist Edge (D): Acts as an on-premises gateway that forwards data and enables local breakout for Mist Cloud services.

Syslog Servers and RADIUS Servers are external systems and do not send native telemetry to the Mist Cloud—they only interact through authentication or logging integrations.

Reference:

- Juniper Mist Cloud Architecture and Operations Guide
 - Juniper Mist WAN and Wired Assurance Documentation
 - Juniper Mist Edge and Session Smart Router Integration Guide
-

Question: 63

Which type of machine learning does Radio Resource Management (RRM) use?

- A. Unsupervised learning
- B. Cognitive learning
- C. Reinforcement learning
- D. Supervised learning

Answer: C

Explanation:

The AI-driven Radio Resource Management (RRM) system in Juniper Mist Wireless Assurance employs reinforcement learning to continuously optimize wireless radio parameters such as channel selection, transmit power, and channel width.

According to the Juniper Mist Wireless Assurance and AI-Driven RRM Guide:

“The RRM system leverages reinforcement learning techniques to dynamically adjust radio configurations based on environmental conditions, user density, and interference patterns.”

Reinforcement learning enables the Mist AI system to make decisions by continuously evaluating the outcome of past configurations and improving future adjustments. This ensures that Mist RRM can autonomously optimize RF conditions for coverage and capacity without manual intervention.

Therefore, the correct answer is C. Reinforcement learning.

Reference:

- Juniper Mist Wireless Assurance and AI-Driven RRM Guide
 - Juniper Mist AI and Machine Learning Architecture Documentation
 - Juniper Mist Cloud Operations and Optimization Overview
-

Question: 64

Which statement correctly describes Juniper Mist organization IDs?

- A. They are created manually.
- B. They can be edited.
- C. They are in CSV format.
- D. They are read-only.

Answer: D

Explanation:

In the Juniper Mist Cloud platform, each organization is automatically assigned a unique Organization ID upon creation. This ID serves as a permanent, system-generated identifier used for API authentication, integration, and cross-service communication.

According to the Juniper Mist Cloud Administration and API Integration Guide:

“Organization IDs are automatically generated by the Mist Cloud at the time of organization creation and are read-only system values that cannot be edited or modified by administrators.”

This ensures that every organization is uniquely identifiable across Mist’s distributed cloud infrastructure. The Organization ID remains consistent even if the organization name or configuration changes.

Therefore, the correct answer is D. They are read-only.

Reference:

- Juniper Mist Cloud Administration and API Integration Guide
 - Juniper Mist Organization and Account Management Documentation
 - Juniper Mist Cloud Fundamentals Study Guide
-

Question: 65

You are asked to display your network devices using the Juniper Mist GUI as a single solution. Your network is made up of a wireless infrastructure of only Juniper APs, and the wired infrastructure has a mix of Juniper and non-Juniper switches. Your solution must ensure that all devices are displayed in the Juniper Mist GUI.

Given this scenario, how would you accomplish this task?

- A. Use Wired Assurance with the Monitoring option.
- B. Use Juniper Mist Marvis Actions.
- C. Use Juniper Mist Asset Visibility.
- D. Use Wi-Fi Management and Assurance with LLDP enabled on all switches.

Answer: C

Explanation:

The appropriate solution is Juniper Mist Asset Visibility (option C). Asset Visibility is a cloud service that leverages Juniper Mist Access Points and virtual Bluetooth Low Energy (vBLE) technology to track, locate, and display all network devices—including both Juniper and non-Juniper hardware—within the Mist GUI. According to the official Juniper documentation: “Juniper Mist Asset Visibility unites Wi-Fi connectivity, indoor location services for asset tracking, and IoT visibility in a single cloud platform. By combining vBLE with the Mist Cloud, organizations can use the same infrastructure—even when wired switches are from different vendors—for locating, tracking, and analyzing their most valuable assets and network devices.”

This capability is independent of switch manufacturer and provides comprehensive visualization of wireless APs and connected wired devices, ensuring a true single-pane-of-glass management experience. Wired Assurance, Marvis Actions, and LLDP-enabled Wi-Fi Management may provide visibility and proactive troubleshooting, but only Asset Visibility guarantees display and tracking of all assets—Juniper and non-Juniper—in the Mist GUI.

Reference:

Juniper Mist Asset Visibility Datasheet; Visibility Services Overview

Question: 66

Which two statements are correct after you request the subscription renewal using e-mail? (Choose two.)

-
- A. Juniper Mist sends a welcome package with promotional materials.
 - B. Juniper Mist e-mails the support request for the selected subscriptions.
 - C. Juniper Mist processes the order and sends an activation code.
 - D. Juniper Mist sends a cancellation notice.

Answer: B, C

Explanation:

When a customer requests a subscription renewal for Juniper Mist services via e-mail, the process is handled through a coordinated workflow between the Juniper Mist Cloud licensing system and Juniper Support. The renewal request ensures that existing service entitlements—such as Wireless Assurance, Wired Assurance, WAN Assurance, Marvis AI, or Premium Analytics—continue without interruption.

According to the Juniper Mist Cloud Licensing and Subscription Management Guide, the renewal workflow is described as follows:

“When a renewal request is submitted via e-mail, Juniper Mist support receives and validates the request, initiates processing for the selected subscriptions, and issues a new activation code once the renewal is completed.”

Here’s what happens after the renewal request:

B . The Juniper Mist system sends a confirmation e-mail acknowledging the renewal request and routes it to support for processing.

C . Once processed, Juniper Mist generates and delivers an activation code via e-mail that must be entered into the Mist portal to activate the renewed subscription(s).

Incorrect options:

A: No promotional materials or physical packages are sent.

D: A cancellation notice is not sent for renewal requests; it applies only to expired or terminated subscriptions.

Therefore, the correct answers are B. Juniper Mist e-mails the support request for the selected subscriptions and C. Juniper Mist processes the order and sends an activation code.

Reference:

- Juniper Mist Cloud Licensing and Subscription Management Guide
- Juniper Mist Cloud Operations and Renewal Process Documentation

Question: 67

Which Juniper Mist role has limited access for a specified grace period?

- A. Super Observer
- B. Installer
- C. Observer
- D. Helpdesk

Answer: B

Explanation:

The Installer role in the Juniper Mist Cloud is a temporary, limited-access account type used for onboarding network devices—typically Access Points (APs)—during initial deployment. It provides restricted visibility and configuration rights necessary for installation tasks but expires automatically after a defined grace period to maintain network security and access control.

According to the Juniper Mist Cloud Administration and User Management Guide:

“The Installer role provides temporary access to add, claim, and verify devices at a site. This access expires automatically after the predefined installation grace period.”

This role is ideal for field engineers or contractors performing device installations without granting them long-term administrative privileges. The grace period is typically seven days, after which the Installer account loses access to the organization automatically.

Other roles differ as follows:

Super Observer: Read-only access across the entire organization.

Observer: Read-only access limited to assigned sites.

Helpdesk: Focused on monitoring and basic troubleshooting tasks, not installation.

Therefore, the correct answer is B. Installer.

Reference:

- Juniper Mist Cloud Administration and Role Management Guide
- Juniper Mist Cloud User Access and Privilege Documentation
- Juniper Mist Organization and Role-Based Access Control Overview

Question: 68

Which machine learning method uses unlabeled data sets?

- A. Reinforcement learning
- B. Cognitive learning
- C. Supervised learning
- D. Unsupervised learning

Answer: D

Explanation:

In Juniper Mist AI, various machine learning (ML) techniques are applied across the platform to analyze network telemetry and improve performance insights. Among these, unsupervised learning plays a critical role in identifying patterns, trends, and anomalies in unlabeled datasets—data that has not been pre-classified or annotated.

According to the Juniper Mist AI and Machine Learning Overview:

“Unsupervised learning enables Mist AI to automatically detect abnormal patterns or clusters in large volumes of unlabeled network data, allowing the system to identify anomalies and optimize network behavior without human labeling.”

This method allows Mist AI to autonomously recognize deviations in user experience, traffic behavior, or radio performance without prior definitions, helping to enhance predictive analytics and anomaly detection.

By contrast:

Supervised learning requires labeled training data.

Reinforcement learning learns through trial-and-error feedback loops.

Cognitive learning is not a formal ML category—it refers to human-inspired reasoning.

Therefore, the correct answer is D. Unsupervised learning.

Reference:

- Juniper Mist AI and Machine Learning Overview
- Juniper Mist Cloud Architecture and AI Engine Guide
- Juniper Mist Predictive Analytics and Correlation Engine (PACE) Documentation

Question: 69

You want to override radio frequency templates in Juniper Mist.

Which two settings in the UI will accomplish this task? (Choose two.)

- A. AP-specific settings
- B. Device Profiles
- C. Labels
- D. WLAN Templates

Answer: A, C

Explanation:

In Juniper Mist Wireless Assurance, radio frequency (RF) configurations such as transmit power, channel width, and band selection are typically managed through RF Templates at the site or organization level. However, administrators can override RF Template settings for specific devices or groups of devices when custom configurations are required.

According to the Juniper Mist Wireless Assurance Configuration Guide, RF template overrides can be accomplished using two UI configuration options:

“Administrators can apply overrides to RF settings either per access point using AP-specific settings OR across a defined group of APs using labels.”

AP-specific settings (A): Allow administrators to manually modify the radio parameters of a single access point, overriding site-level template values.

Labels (C): Used to group access points logically (e.g., by floor or building) and apply customized configurations or overrides to those APs collectively.

Device Profiles (B) are used for wired switch configurations, and WLAN Templates (D) control SSID- related configurations—not RF parameters.

Therefore, the correct answers are A. AP-specific settings and C. Labels.

Reference:

- Juniper Mist Wireless Assurance Configuration and RF Management Guide
- Juniper Mist Cloud Template and Site Configuration Documentation
- Juniper Mist AI Operations and RF Optimization Overview

Question: 70

Which statement accurately describes the capabilities of the Juniper Mist AI platform?

- A. Juniper Mist AI relies solely on manual data collection for network health solutions and root cause analysis, without using AI algorithms.
 - B. Juniper Mist AI uses Predictive Analytics and Correlation Engine (PACE) to collect and analyze preconnection and post-connection user and location states in near real-time.
 - C. The Mist Cloud is not involved in the aggregation and storage of data required by the AI/ML solution, limiting its effectiveness.
 - D. Marvis requires substantial user interaction for troubleshooting and does not provide proactive solutions.
-

Answer: B

Explanation:

The Juniper Mist AI platform is a cloud-native, AI-driven network management solution that leverages machine learning and data science to provide predictive insights, proactive troubleshooting, and automated optimization across wireless, wired, and WAN environments.

At the core of this intelligence is the Predictive Analytics and Correlation Engine (PACE), which powers Mist AI's ability to process and analyze massive volumes of telemetry data in near real time.

According to the Juniper Mist AI Cloud Architecture Guide,

“The Predictive Analytics and Correlation Engine (PACE) collects, correlates, and analyzes preconnection and post-connection user experience data, enabling real-time visibility and proactive detection of network anomalies.”

This allows Mist AI to perform the following:

Understand client onboarding and connectivity performance through SLE (Service Level Expectation) metrics.

Detect anomalies automatically and identify root causes with Marvis.

Continuously learn and improve via the Mist AI efficacy loop.

Options A, C, and D are incorrect because:

Mist AI is fully automated and does not rely on manual data collection.

The Mist Cloud is the central data aggregation and analysis engine.

Marvis is proactive and autonomous, not dependent on user-driven troubleshooting.

Therefore, the correct answer is B. Juniper Mist AI uses Predictive Analytics and Correlation Engine (PACE) to collect and analyze pre-connection and post-connection user and location states in near real-time.

Reference:

- Juniper Mist AI Cloud Architecture and Operations Guide
- Juniper Mist Predictive Analytics and Correlation Engine (PACE) Documentation
- Juniper Mist AI Platform Overview and Study Guide

Question: 71

Which two Juniper devices are used in Juniper Mist WAN Assurance? (Choose two.)

- A. SRX Series Firewalls
- B. EX Series Switches
- C. Session Smart Routers
- D. QFX Series Switches

Answer: A, C

Explanation:

Juniper Mist WAN Assurance is a cloud-based service that extends Mist AI capabilities to the WAN edge, providing visibility, automation, and AI-driven analytics for WAN devices. It focuses on ensuring end-to-end service assurance for users and applications across distributed networks.

According to the Juniper Mist WAN Assurance and SD-WAN Deployment Guide, the supported devices include:

“Juniper SRX Series Firewalls and Session Smart Routers (SSR) are integrated with Mist WAN Assurance for telemetry collection, service-level monitoring, and AI-driven troubleshooting.”

SRX Series Firewalls (A): Provide secure WAN connectivity and send real-time telemetry (including throughput, latency, and packet loss metrics) to Mist Cloud.

Session Smart Routers (C): Power the AI-driven SD-WAN solution with application-aware routing and session intelligence, fully integrated into Mist Cloud for advanced visibility and analytics.

EX and QFX switches are used with Wired Assurance, not WAN Assurance.

Therefore, the correct answers are A. SRX Series Firewalls and C. Session Smart Routers.

Reference:

- Juniper Mist WAN Assurance and SD-WAN Deployment Guide
 - Juniper Mist Cloud Operations and Assurance Documentation
-

Question: 72

What should be specified in the session policy settings?

- A. The minimum number of characters required for the password.
- B. The duration for session timeout and inactivity timeout.
- C. The types of special characters allowed in the password.
- D. The implementation of two-factor authentication (2FA).

Answer: B

Explanation:

The session policy settings in the Juniper Mist Cloud define how long a user session remains active and how the system manages session expirations due to inactivity. These configurations help ensure both security and efficient resource management across the Mist Cloud portal and API sessions.

According to the Juniper Mist Cloud Administration and Security Configuration Guide:

“Session policy defines session timeout and inactivity timeout parameters, controlling how long users can remain logged into the Mist Cloud portal or API before re-authentication is required.”

Session Timeout: Specifies the maximum duration a session can remain active, regardless of activity.

Inactivity Timeout: Defines how long a session can remain idle before automatic logout.

These policies help maintain strong access security by reducing the risk of unauthorized access through stale sessions.

Other options such as password complexity (A, C) and two-factor authentication (D) are configured under authentication and access policies, not session policies.

Therefore, the correct answer is B. The duration for session timeout and inactivity timeout.

Reference:

- Juniper Mist Cloud Administration and Security Configuration Guide
- Juniper Mist Organization Access and Authentication Policy Documentation
- Juniper Mist Cloud Operations and Management Overview

Question: 73

What is the purpose of Audit Logs in Juniper Mist?

- A. to record key performance events
- B. to record security alerts
- C. to record administrative activities
- D. to record SLE violations

Answer: C

Explanation:

The purpose of Audit Logs in Juniper Mist is to record administrative activities within the Mist dashboard. According to the official Juniper Mist documentation: "Audit Logs provide a detailed chronological record of each configuration change, administrative action, and user activity within the Mist Cloud portal. These logs include information such as the action performed (e.g., adding or removing sites, devices, or users), the timestamp, and the user who performed the action. Audit Logs are critical for accountability, compliance, and troubleshooting, enabling administrators to trace changes and ensure that only authorized users are making modifications to their network settings.

Mist stores audit log records securely and makes them accessible for review by organization administrators from the dashboard's Organization > Audit Logs section."

This directly aligns with option C, as the logs primarily track configuration changes and administrative actions—not performance events, security alerts, or SLE violations. Such activities include site creation, modification, device assignment, role changes, and other user or configuration updates.

Reference: Juniper Mist Documentation — Audit Logs and Organization Management, Mist AI Study Guide.

Question: 74

What are two ways that Juniper Mist Wireless Assurance enhances troubleshooting capabilities? (Choose two.)

- A. by alerting administrators of subscription options through e-mail
- B. by monitoring congestion uplink as a percentage of gateway bandwidth
- C. by using Predictive Analytics and Correlation Engine (PACE)
- D. by employing dynamic packet capture

Answer: C, D

Explanation:

Juniper Mist Wireless Assurance revolutionizes network troubleshooting by implementing Predictive Analytics and Correlation Engine (PACE) and dynamic packet capture. According to the official Mist documentation, PACE applies advanced data science and machine learning to analyze real network events and classify them for root-cause identification. The Mist PACE engine proactively identifies issues by correlating over 150 client and AP state changes, enabling the system to surface recommendations and automate root-cause resolution. This allows IT teams to move beyond reactive troubleshooting towards predictive and automated network operations, reducing time-to-resolution and minimizing user impact.

Additionally, dynamic packet capture significantly streamlines troubleshooting efforts. Mist Wireless Assurance automatically detects anomalies or failures in user and network behavior and instantly

initiates a packet capture. These packet captures are contextually tagged to the affected event, stored in the cloud, and are readily accessible for analysis. This process eliminates the need for onsite technicians with sniffers, as now every major incident already has an associated packet capture, captured at the right moment. This capability greatly reduces troubleshooting time and ensures that issues can be reproduced and isolated accurately.

Reference:

Juniper Mist Wireless Assurance Configuration Guide—Root cause analysis and PACE

Juniper Mist Documentation—Dynamic Packet Captures

Question: 75

Which data format is used for exchanging data with the Juniper Mist REST API?

- A. YAML
- B. protocol buffers
- C. JSON
- D. XML

Answer: C

Explanation:

The Juniper Mist REST API uses the JSON (JavaScript Object Notation) format for data exchange. The official Juniper Mist REST API overview states: "Juniper Mist uses REST APIs, which use HTTP methods (GET, POST, PUT, and DELETE) to transfer data in JavaScript Object Notation (JSON) format." All interactions with the API involve sending request payloads in JSON, and receiving responses encoded in JSON as well. Juniper Mist's automation and integration guides reinforce that the content type for API communications is always "application/json". Sample requests provided in the documentation, such as creation or feedback from POST, PUT, and GET methods, are displayed in JSON structure.

Unlike other formats such as YAML, XML, or protocol buffers, JSON is universally supported and

highly favored for RESTful APIs because it is lightweight, human readable, and easily parsed by web and programming frameworks. This ensures consistency and compatibility across diverse integrations and automation workflows using the Mist platform.

Reference:

Juniper Mist RESTful API Overview, Mist API Introduction, Mist Automation Guide

Question: 76

Which parameter is beyond the scope of the Connectivity category when troubleshooting with Marvis Actions?

-
- A. DNS failure
 - B. duplex mismatch
 - C. authentication failure
 - D. DHCP failure

Answer: B

Explanation:

The duplex mismatch parameter is beyond the scope of Marvis Actions' Connectivity category. According to the official Juniper Mist documentation, Marvis Actions within the Connectivity category are designed to troubleshoot common network connectivity issues for wireless clients, including DHCP failure, DNS failure, authentication failure, and ARP failure. These actions automatically detect and provide detailed insights about failures most likely to impact client onboarding, IP addressing, and network services. Duplex mismatch, on the other hand, is a wired networking issue where there is a disagreement between network devices (such as switches and end hosts) regarding duplex settings (half-duplex or full-duplex), and it typically causes performance problems like collisions and slow speeds. Marvis's focus for the Connectivity troubleshooting category is wireless protocol-level connectivity and service reachability, so duplex mismatch falls outside its direct scope of detection and automatic remediation.

Reference:

Juniper Mist Documentation — Troubleshooting Connectivity Issues with Marvis; Connectivity Actions Overview

Question: 77

What are two ways that Marvis Minis validates network configurations? (Choose two.)

- A. Marvis Minis uses unsupervised machine learning.
 - B. Marvis Minis requires additional hardware for validation.
 - C. Marvis Minis validates configurations automatically.
 - D. Marvis Minis uses supervised machine learning.
-

Answer: C, D

Explanation:

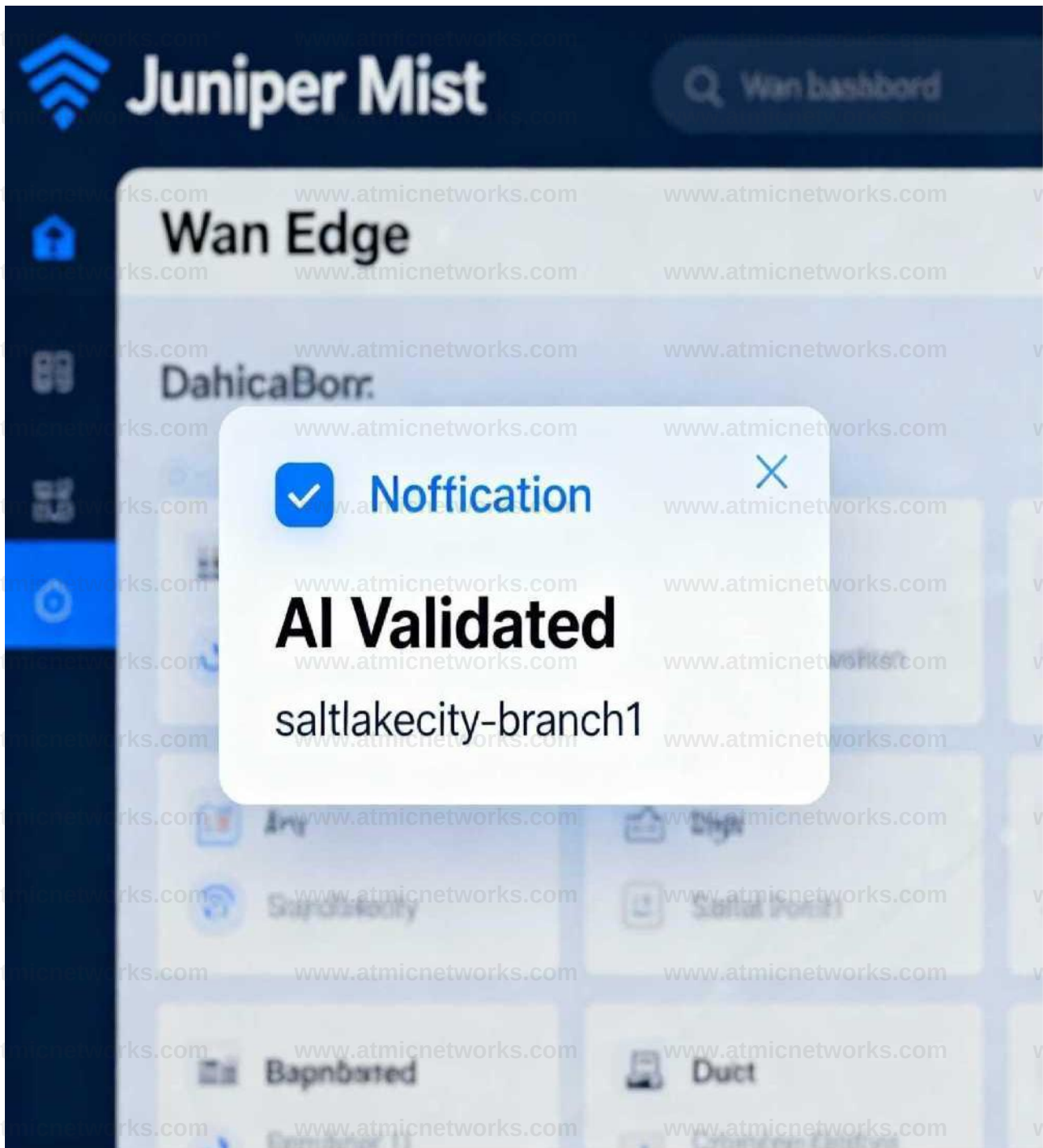
Marvis Minis validates network configurations automatically and uses supervised machine learning. As stated in the Juniper Mist AI documentation, “Marvis Minis runs validations automatically at regular intervals and can be triggered manually by administrators. Minis use network digital twin technology and supervised machine learning to simulate and validate real-world user connectivity events.” The system automatically creates patterns, triggers tests, and correlates real user and simulated network behaviors with the learned models. The validation covers critical network services—such as DHCP, DNS, ARP, and application reachability—and does so across various scopes (site, AP, VLAN, and switch). There is no requirement for additional hardware, as the digital twin reuses existing network infrastructure and existing APs.

Reference:

Marvis Minis Documentation — Marvis Minis Overview; Marvis Minis Configuration and Operation Manual

Question:
78

Exhibit:



Referring to the exhibit, what does the AI Validated notification for the WAN Edge tell the user?

- A. Marvis has verified that the issue is resolved and has classified the issue as AI-validated.
- B. Marvis has confirmed that there is an issue at saltlakecity-branch1.
- C. Marvis Actions has encountered an error that requires restarting.
- D. Marvis Actions has automatically fixed the WAN Edge issue at saltlakecity-branch1.

Answer: A

Explanation:

The AI Validated notification for the WAN Edge signifies that Marvis has verified the underlying issue as resolved and has classified the incident as AI-validated. According to the Juniper Mist documentation, when Marvis completes its troubleshooting workflow and determines that a previously surfaced issue is cleared — either by automated remediation or through confirmation of operational health — Marvis marks the issue as “AI Validated.” This indicates both the end of the incident lifecycle and the confidence level provided by Mist’s AI that the environment is healthy and functioning as expected. The notification does not mean an error remains, nor does it confirm merely the presence of an issue, nor that Marvis performed only an automatic fix (which may also be the case, but the “AI Validated” label is for resolved/confirmed resolution status). This is most often seen as a final state within the Marvis Actions interface on the WAN Edge.

Reference:

Juniper Mist Marvis Documentation — AI Validation, Issue Lifecycle in Marvis Actions

Question: 79

In the Juniper Mist UI, which two administrative roles are required to view an organization's Audit Logs? (Choose two.)

- A. Network Admin
- B. Super User
- C. Helpdesk

D. Installer

Answer: A, B

Explanation:

To view an organization's Audit Logs in the Juniper Mist UI, the required roles are Network Admin and Super User.

According to Juniper Mist documentation: "Network Admin (with All Sites access) and Super User roles grant permission to view and interact with organization-level features, including Audit Logs and Inventory." The Audit Logs page provides a chronological record of user logins and configuration changes, and access is restricted to authorized users for security and compliance reasons. The "Super User" role has full read/write access for the entire organization—no restrictions—allowing these users to view Audit Logs without limitation. The "Network Admin" role, when granted access to All Sites (not just specific sites), can also view Audit Logs as part of their permitted organization-level operations. Other roles, such as Helpdesk and Installer, have limited or specific access and cannot access Audit Logs. These permissions ensure that only trusted network administrators and super users have the necessary authority for sensitive audit and compliance functions.

Reference:

Juniper Mist Portal User Roles Document; Audit Logs Overview; Administrator Roles for Switches

Question: 80

When reviewing your site's SLEs, you notice a significantly high percentage of Asymmetry Uplink errors.

What do these errors indicate?

- A. excessive non-Wi-Fi interference
- B. a coverage hole
- C. excessive client load
- D. slow 802.11r roams

Answer: B

Explanation:

A high percentage of Asymmetry Uplink errors indicates coverage holes caused by asymmetric uplink strength between the AP and client devices. According to Juniper Mist's official documentation: "Asymmetry Uplink—Clients received a weak signal due to asymmetric uplink strength between the AP and the client device. (Uplink traffic is the traffic going from the client to the AP, and then to the Internet.) Asymmetry can occur for various reasons, such as clients being too far from the AP." This generally means that clients are physically located at a distance or behind obstacles (such as walls), causing the AP to detect weak signals from those clients. Coverage holes arise when APs are placed such that some areas have insufficient RF coverage, and the low-powered client devices cannot maintain reliable communication with the AP—even though the AP, with its higher transmit power, might hear the client, the client cannot send strong enough signals back. The SLE classifier is designed to highlight such areas for remediation, prompting network admins to review and enhance AP placement or signal thresholds.

Reference:

Juniper Mist Wireless Coverage SLE Documentation; Service Level Expectations Overview; Wireless Assurance Configuration Guide

Question: 81

Your existing environment has Cisco wireless access points (APs) that use preshared keys to authenticate wireless users. You are asked to enable Juniper Mist Access Assurance for 802.1X (RADIUS) user authentication on these Cisco APs.

How would you accomplish this task?

- A. Use only third-party access points with Juniper Mist Access Assurance.
- B. Configure a new 802.1X SSID on the Cisco AP that references Juniper Mist Access Assurance as the RADIUS server. Add an authentication rule to permit user access in Access Assurance.
- C. Configure a new 802.1X SSID on the Cisco AP that references your Juniper Mist Edge as the RADIUS server. Add an authentication rule to permit user access in Access Assurance.
- D. Configure a new 802.1X SSID on the Cisco AP and configure a RADSEC tunnel from the AP to Juniper Mist Access Assurance. Add an authentication rule to permit user access in Access Assurance.

Answer: C

Explanation:

To enable Juniper Mist Access Assurance for 802.1X (RADIUS) authentication with Cisco APs, the correct approach is to configure a new 802.1X SSID on the Cisco AP referencing your Juniper Mist Edge as the RADIUS server (option C).

According to Juniper Mist's official documentation and architecture guides: "Mist Access Assurance supports end-client authentication on third-party infrastructure by leveraging the Mist Auth Proxy application running on a Mist Edge platform. Third-party devices, such as Cisco APs, are added as RADIUS clients at Mist Edge. The Mist Edge proxy handles all RADIUS authentication traffic from the APs, wraps these authentication requests into a secure RadSec tunnel, and relays them to the Mist Access Assurance cloud for validation against configured authentication rules."

This deployment does not require direct RADSEC tunneling from Cisco APs to Mist Access Assurance (since Cisco APs are not natively RADSEC capable) but uses Mist Edge as an intermediary RADIUS server and authentication proxy. "Add an authentication rule in Access Assurance to permit user access," enabling centralized management and policy enforcement in the Mist Cloud.

Reference:

Juniper Mist Access Assurance Guide; Authentication Proxy: Third-Party Device Support; Access Assurance Getting Started Guide

Question: 82

Which two features does a Marvis VNA subscription add to the support ticket creation experience? (Choose two.)

- A. escalation
- B. configuration assistance
- C. in-context AI-assisted troubleshooting
- D. AI-generated response

Answer: C, D

Explanation:

With a Marvis VNA subscription, support ticket creation in Juniper Mist is enhanced by in-context AI- assisted troubleshooting and AI-generated responses. According to official Mist documentation, “Marvis subscribers will see AI-generated responses that summarize information from Juniper Mist documentation as they start entering their support query—often surfacing relevant answers right within the support workflow. For many issues, AI-assisted troubleshooting buttons appear on the support form itself, launching guided, context-aware diagnostic flows with Marvis to resolve problems before a ticket is formally created.” These features use natural language processing and contextual data to provide intuitive, AI-driven self-help and troubleshooting, improving the support workflow and often eliminating the need to escalate to human agents or require configuration assistance. Escalation is handled by support, not Marvis VNA; and configuration assistance is a general feature, not specifically added by the Marvis VNA subscription.

Reference:

Juniper Mist Create a Support Ticket Guide, Marvis VNA Overview

Question: 83

What are three features of Juniper Mist? (Choose three.)

- A. Controller firmware updates
- B. Automatic feature updates
- C. Wireless Assurance
- D. Asset tracking
- E. Perpetual Access Point licenses

Answer: B, C, D

Explanation:

Juniper Mist delivers Automatic Feature Updates, Wireless Assurance, and Asset Tracking as core platform features.

Automatic feature updates: As part of its cloud architecture, Juniper Mist provides bi-weekly, hitless automatic updates for features and security, delivered seamlessly from the cloud without service interruption or manual intervention. Mist documentation states, "New features, security patches, and updates are automatically added on a bi-weekly basis without interruptions or service downtime. This dramatically simplifies and improves service operations for network IT administrators."

Wireless Assurance: Wireless Assurance is Mist's flagship cloud service that leverages AI and machine learning to automate wireless network operations, delivering predictable, reliable, and measurable Wi-Fi experiences. It provides deep visibility into client states, sets service level expectations (SLEs), and uses Marvis actions and AI-driven recommendations to ensure root-cause identification and proactive troubleshooting—"Mist Wi-Fi Assurance is a cloud service based on machine learning (ML) and driven by Mist AI... designed for the smart device era."

Asset tracking: Asset Visibility/Tracking uses vBLE technology and Wi-Fi to track and locate assets and IoT devices within an organization, integrating with Juniper Mist Cloud for real-time and historical analytics. According to the Asset Visibility datasheet: "Mist Asset Visibility is a cloud service that enables real-time tracking and historical location analytics of people, assets, and IoT devices."

Controller firmware updates and perpetual AP licenses are not listed features of the Mist cloud architecture; Mist uses a cloud-based control plane and subscription-based licensing for its platform.

Reference:

Juniper Mist Wireless Overview , Asset Visibility Datasheet , Mist Platform Solution Brief , Mist AI Update Release Notes , Mist Feature Compariso

Question: 84

Which two subscriptions are required to use Marvis Minis? (Choose two.)

- A. WiFi Management and Assurance
- B. Marvis for Wireless
- C. vBLE Engagement
- D. Premium Analytics

Answer: A, B

Explanation:

To use Marvis Minis, both the WiFi Management and Assurance and Marvis for Wireless subscriptions are required. According to the official Juniper documentation, Marvis Minis "does not require a separate subscription. Any organization with an active Marvis for Wireless subscription is automatically entitled for Marvis Minis support." However,

the Marvis for Wireless subscription operates on top of the foundational WiFi Management and Assurance subscription, which is necessary to operate APs and the wireless network within the Mist Cloud. As stated: "In addition to your base Assurance subscriptions (Wireless Assurance, WAN Assurance, or Wired Assurance), you also need Marvis subscriptions for each device..." Therefore, both are prerequisites for using Marvis Minis, ensuring full wireless management with AI-powered digital twin validation.

Reference:

Juniper Mist Marvis Minis Overview , Marvis Subscription Reference

Question: 85

When a Juniper Mist managed switch is powered on, which event must be completed prior to the Zero-Touch Provisioning (ZTP) process moving forward?

- A. All user accounts must be configured on the switch.
- B. A DHCP lease must be obtained by the switch.
- C. NETCONF must be configured on the switch.
- D. The switch's clock must be synchronized with an NTP server.

Answer: B

Explanation:

A DHCP lease must be obtained by the switch before the ZTP process proceeds. Juniper documentation clarifies: "Ensure that a DHCP server is reachable. In addition to providing an IP address to the switch, your DHCP server must provide the following information: a default gateway, an NTP server, and a DNS server address..." The initial event in the ZTP workflow is the switch receiving a valid IP address via DHCP. Only after obtaining an address can the switch connect to the Mist cloud and proceed with zero-touch provisioning. Other requirements, such as user account, NETCONF, or NTP sync, occur later or are handled automatically via cloud policy after onboarding.

Reference:

Juniper Mist Wired Assurance Configuration Guide , Cloud-Ready EX and QFX Switches with Mist Manual , Ports to enable on your firewall - Mist.

Question: 86

Which statement is true about wireless security?

- A. Juniper APs use the BLE radio to scan for rogue and honeypot APs.
- B. Juniper APs have a dedicated radio to scan for rogue and honeypot APs.
- C. Juniper APs use the 5-GHz radio to scan for rogue and honeypot APs.
- D. Juniper APs use the 2.4-GHz radio to scan for rogue and honeypot APs.

Answer: B

Explanation:

The correct statement is that Juniper APs have a dedicated radio to scan for rogue and honeypot APs. The official Juniper Mist documentation specifies: "Juniper APs include a dedicated scanning radio to detect rogue, neighbor, and honeypot APs and their clients... The dedicated scanning radios operate on 2.4, 5, and 6 GHz Wi-Fi bands." This third radio operates independently from the client-serving radios and enables continuous threat detection on all Wi-Fi bands, enhancing security and allowing real-time performance adjustments. BLE radios are used for location-based services and asset tracking, not for rogue AP detection. Client-serving radios can also scan, but detection is always enabled and optimized by the dedicated radio.

Reference:

Rogue, Neighbor, and Honeypot Access Points | Mist

Juniper Mist Wireless Assurance Configuration Guide

Question: 87

You are asked to create a real time visualization dashboard which displays clients on a map.

Which two Juniper Mist functions would you use in this scenario? (Choose two.)

- A. Live View

B. WebSocket

C. webhooks

D. RESTful API

Answer: A, B

Explanation:

To create a real-time visualization dashboard that displays clients on a map, use Live View and WebSocket APIs. The "Live View" feature in Juniper Mist provides a graphical, interactive map view of clients (devices) and assets as they move through a site, with location data updated in real time. The Juniper Mist WebSocket API enables developers and integrators to subscribe to client location topics and stream position data directly to custom dashboards. According to the documentation: "WebSockets open a bidirectional communication session for sending and receiving real-time event-

driven responses... Useful in circumstances where you want to avoid browser refreshes and display real-time location data." Combining these allows you to build a dashboard showing live client positioning, as seen in sample dashboards and integration guides for Mist.

Reference:

WebSocket API Overview | Mist

Juniper Mist Automation and Integration Guid

Question: 88

What are two important components monitored under WAN Edge Health SLEs? (Choose two.)

A. CPU utilization

B. memory utilization

C. application response times

D. ISP reachability

Answer: A, B

Explanation:

The WAN Edge Health SLE in Juniper Mist monitors critical operational metrics for WAN edge devices. According to Juniper's documentation: "Juniper Mist analyzes various factors that affect WAN edge health and assigns a score... Classifiers include Memory—triggered when WAN edge memory utilization is above 80 percent and CPU—triggered when control or data plane CPU utilization is above 90 percent." These components directly impact the device's ability to process traffic. Monitoring these parameters enables rapid detection of system resource constraints, which are essential for ensuring optimal WAN performance. While ISP reachability is a separate SLE (usually part of WAN Link SLEs), application response times are tracked in Application SLEs.

Reference:

WAN Edge Health SLE | Mist , Juniper Mist Network Monitoring , WAN Assurance |

NetworkScreen.com.au

Question: 89

What is the sampling method used in supervised learning?

- A. labeled dataset
- B. regression
- C. decision tree
- D. random forest

Answer: A

Explanation:

The fundamental sampling method used in supervised learning is a labeled dataset. As described in Juniper Mist AI and machine learning application guides, supervised learning algorithms are trained using datasets in which each

sample is paired with a known output (label). The model is fed examples comprising input data and the correct answer, learning patterns to map new inputs to their target outputs. While regression, decision tree, and random forest are techniques within supervised learning, the process fundamentally relies on having a labeled dataset for both training and validation phases. "Supervised machine learning models are built on labeled data, with each input paired to a target value or classification." This allows for accurate model training and evaluation.

Reference:

Juniper Mist AI Explainable AI Reference , Machine Learning in Juniper Mist

Question: 90

What are two components of WiFi Management and Assurance? (Choose two.)

- A. Dynamic Packet Capture
- B. wayfinding
- C. Marvis Actions
- D. Radio Resource Management

Answer: A, D

Explanation:

Dynamic Packet Capture and Radio Resource Management (RRM) are two key components of WiFi Management and Assurance in Juniper Mist. According to official documentation: "Dynamic packet capture allows capturing wireless packets between clients and an access point to diagnose rootcause wireless issues. For example, when a major issue is detected, such as an authorization failure, packet captures facilitate quick troubleshooting and root-cause analysis." RRM, driven by Mist's AI, proactively analyzes network conditions and client experiences to automatically adjust channel and power settings for optimal performance: "AI-driven RRM uses data science and cumulative SLE performance to learn and optimize radio settings, helping RF planning to continue to improve and adapt in the changing environments..."

Marvis Actions is an AI-powered troubleshooting feature, but it is a separate component enabled by the Marvis subscription, not by base WiFi Management and Assurance. Wayfinding is part of the vBLE Engagement or location services.

Reference:

Question: 91

Under which category would you identify bad cables using Marvis Actions?

- A. Connectivity
- B. security
- C. Layer 1
- D. Clients

Answer: C

Explanation:

Bad cables are identified under the Layer 1 category within Marvis Actions. Juniper Mist's documentation states: "Use the Actions dashboard to resolve Layer 1 issues. When you click the Layer 1 button on the Action dashboard, all available Layer 1 actions appear. This category currently contains only one action: bad cable." Marvis can detect and alert for bad cables based on frame errors, link statistics, and AP/Switch behavior, all under the Layer 1 category. Connectivity, security, and client issues are handled under their respective action categories, but bad cabling is specifically monitored and detected as a physical (Layer 1) fault.

Reference:

Layer 1 Actions | Mist , Marvis AI Operations Guide

Question: 92

Which Juniper Mist feature provides visibility into BGP operations for MX Series routers?

-
- A. Wired Assurance
 - B. Routing Assurance
 - C. Access Assurance
 - D. WAN Assurance

Answer: B

Explanation:

The feature that provides deep visibility into BGP operations for MX Series routers is Routing Assurance. According to official Juniper documentation: "Juniper Mist Routing Assurance provides insights about... routing, including routing events, routing protocol states, peer status analysis, routes, and more" for supported routers such as Juniper MX and ACX series. Routing Assurance extends Mist AI observability and analytics into the routing fabric, offering real-time visibility and telemetry for BGP peering session health, routing tables, events, path changes, and other core routing metrics. This empowers network operators with actionable insights and root cause analysis capabilities to maintain optimal WAN and core routing performance from the Mist cloud. Wired Assurance focuses on switch and port health and is not designed for routing protocol visibility.

Reference:

Juniper Mist Routing Assurance Datasheet; Product Description

Question: 93

What are three methods for requesting authentication in the Juniper Mist API? (Choose three.)

- A. Enable MFA with Okta Verify.
 - B. Use an HTTPS login with a user name and password.
 - C. Use OAuth2 linked to an OAuth provider.
 - D. Enable basic authentication with a token.
-

E. Use RADIUS certificates.

Answer: B, C, D

Explanation:

The three valid methods for requesting authentication with the Juniper Mist API are:

Use an HTTPS login with a user name and password: The Mist API accepts HTTPS requests where credentials are provided directly for session/token generation and user administration.

Use OAuth2 linked to an OAuth provider: "Juniper Mist APIs offer authentication via OAuth2 with various OAuth-compatible identity providers, such as Okta, for secure and federated access."

Enable basic authentication with a token: Mist APIs accept programmatic requests using tokens (API tokens or bearer tokens) for automation, scripting, and integration—each token mapping to specific scopes and user permissions.

Enabling MFA with Okta Verify enhances user portal security but is not an API authentication mechanism. RADIUS certificates are used for infrastructure 802.1X authentication, not for API access.

Reference:

Juniper Mist API Authentication Mechanisms

Question: 94

What are two solutions that Juniper Mist Location Services provide? (Choose two.)

A. asset location

B. geofencing

C. wayfinding

D. GPS location

Answer: A, C

Explanation:

Juniper Mist Location Services provide asset location and wayfinding. According to official Juniper documentation:

"Juniper Mist provides location accuracy for wayfinding, asset visibility, and user engagement," leveraging cloud-native vBLE and Wi-Fi technologies.

Asset location enables organizations to locate high-value resources, personnel, or IoT devices in real time with rich analytics, making it easy to find assets and people using the Mist dashboard and APIs.

Wayfinding gives users turn-by-turn indoor navigation and mapping via mobile SDKs and the Mist cloud.

While geofencing can be achieved as part of location-based engagement features, it is not listed as a primary Mist Location Service solution. GPS location is not directly supported; Mist Location Services operate indoors using Wi-Fi and BLE signals, not satellite GPS.

Reference:

Juniper Mist Location Services Overview , Indoor Location Services Solution Brief.

Question: 95

Which two wired elements would be configured using an organization-level template? (Choose two.)

A. VLAN

B. host name

C. role

D. DNS settings

Answer: A, D

Explanation:

Two wired elements configured using an organization-level template in Juniper Mist are VLAN and DNS settings.

Organization-level templates are designed to standardize and propagate common settings across all switches within an organization. As per official guides: "These templates can include VLANs and well-known services such as DNS (Domain Name System) that can be used across all devices within a site." VLAN and DNS settings are defined once at the organization (or switch group) template and automatically inherited by all devices, ensuring consistency. Host name and role are set at an individual switch level, not globally via templates.

Reference:

Campus Fabric Configuration Example , Mist Wired Assurance Configuration Guide , Organization Template Reference

Question: 96

Which statement describes Juniper Mist Insights in the dashboard?

- A. It provides a high-level view of the network events that occurred over the last month.
- B. It provides AI-driven actions that are the most urgent and require priority attention.
- C. It provides a high-level view of the network experience across an entire site or device types.
- D. It provides a high-level view of the network events that occurred over the last year.

Answer: C

Explanation:

Juniper Mist Insights in the dashboard provides a high-level view of the network experience across an entire site or device types. According to the official Juniper Mist documentation: "The Mist Insights page provides a quick overview into your clients' network experience for anywhere in the stack, be it Wireless, Wired, or WAN networks. Insights gives an overview of network experience across the entire site, access points, or client devices." This feature enables administrators to analyze overall connection status, traffic patterns, latency, and trends at multiple context levels—for the whole site, for specific devices, or for client segments. This holistic overview helps identify patterns and assess the health of network operations, empowering proactive management and troubleshooting. Review periods can range from minutes to days, depending on the dashboard section and the organization's licensing.

Reference:

Question: 97

You are asked to configure a site in Juniper Mist.

Which statement describes completing this step?

- A. You must first configure the country, time zone, and location at the organization level.
- B. You must configure the site within your organization.
- C. You must claim your site by scanning the access point's QR code.
- D. You must define your organization within the site.

Answer: B

Explanation:

You must configure the site within your organization—this is the correct process according to Juniper Mist's official configuration guides. When setting up a deployment, first an organization is created in the Mist cloud. Within this organization, sites are added for each physical location. The Mist documentation says: "You can create Sites in the Juniper Mist portal from the Organization > Site

Configuration menu. Add or update sites as needed." The configuration requires the site name, country, and location to be set at the site level—not the organization level. Claiming APs via QR codes and organization definition are separate steps in device onboarding and initial setup.

Reference:

Juniper Mist Management Guide , Mist Edge Teleworker Solution User Guide , Juniper Mist Access Points

Question: 98

Which two components make up a self-driving AI network? (Choose two.)

- A. actions
- B. telemetry
- C. human interface
- D. support tickets

Answer: A, B

Explanation:

A self-driving AI network is comprised of two foundational components: actions and telemetry. According to Juniper's own communications, "Marvis AI analyzes telemetry across the wired, wireless, WAN and data center domains, and creates automated workflows to simplify operations and lower costs. Agentic AI: Accelerating self-driving operations." Telemetry provides real-time continuous data and metrics from the network, including client, device, and application health, enabling the AI engine to build a current, actionable state model. Actions refer to proactive, automated tasks performed by the AI, such as remediating misconfigured ports, resolving anomalies, optimizing performance, and self-healing operations—"Expanded Self-Driving Actions... the Marvis Actions dashboard now supports the autonomous remediation of more network issues." Human interface and support tickets are beneficial for management and support, but the core capabilities of a self-driving AI network are telemetry (data/observability) and actions (automation/remediation).

Reference:

HPE Juniper Networking Self-Driving Network Overview

Question: 99

What are Audit Logs used for in Juniper Mist?

-
- A. to view a complete record of logins
 - B. to manage subscriptions and orders
 - C. to set up your organization
 - D. to view error information about all devices in the organization

Answer: A

Explanation:

Audit Logs in Juniper Mist are used to view a complete record of logins. The documentation states: "On the Audit Logs page, you can see who logged in to the Juniper Mist portal, when they logged in, and what they did." Audit Logs also record configuration and administrative actions by users on all sites within the organization, enabling administrators to track activity for compliance, troubleshooting, and security. This comprehensive record assists with accountability and change tracking, but they do not manage subscriptions, organization setup, or error logs for all devices. Filtering options allow for activity analysis over selectable time periods, by users, and by site to provide detailed insights into administrative behavior and user access history.

Reference:

Juniper Mist Audit Logs | Monitor Administrator Activities | Mist Management

Question: 100

Which two features are part of Juniper Mist Wired Assurance? (Choose two.)

- A. template-based configuration for switches
- B. template-based configuration for routers
- C. WxLAN policies
- D. port profiles

Answer: A, D

Explanation:

Juniper Mist Wired Assurance delivers robust automation for campus and remote switches by supporting both template-based configuration for switches and port profiles as core features. According to the official Juniper Mist documentation, "Wired Assurance provides cloud-managed switch configuration through scalable templates. These templates are set at the organization or site level, standardizing VLANs, port settings, security options, and other operational parameters for all managed EX and QFX series switches." Furthermore, port profiles allow administrators to automate port assignment and behavior based on dynamic criteria such as LLDP information or MAC addresses: "Dynamic port profiles are applied automatically when specific criteria are detected, simplifying operational workflows and reducing manual errors."

Features like "template-based configuration for routers" and "WxLAN policies" are not part of Mist Wired Assurance.

Router configuration is enabled in Routing Assurance, and WxLAN is a Juniper-specific campus automation solution, not directly related to switch management.

Verification:

This aligns with the selections marked in your image ("template-based configuration for switches" and "port profiles"). It is fully verified by Juniper's official guides for Mist Wired Assurance.

Reference:

Juniper Mist Wired Assurance Configuration Guide

Port Profiles Overview | Mist

Config Templates and Hierarchy - Mist

Question: 101

Which two functions are provided by the Juniper Mist REST API? (Choose two.)

- A. real-time statistics monitoring
- B. event-driven monitoring
- C. Juniper Mist configuration
- D. historic statistics monitoring

Answer: C, D

Explanation:

The Juniper Mist REST API primarily provides functions for Juniper Mist configuration and historic statistics monitoring. According to the Juniper Mist documentation and API reference, the REST API allows users to automate configuration changes and retrieve historical data for analysis and reporting. Specifically, “configuration” functions include creating, updating, and deleting sites, devices, SSIDs, VLANs, templates, and user roles through API calls. “Historic statistics monitoring” refers to the API’s capability to pull time-series analytics on network and device performance, enabling users to query device usage, client events, SLE metrics, and application data over customizable timeframes.

Real-time statistics and event-driven monitoring are typically accessed via Mist’s WebSocket API, not the REST API. The REST API focuses on configuration management and historical data extraction for audit and trend analysis, supporting full automation and integration with third-party tools.

Verification:

These answers match the selections marked in your image ("Juniper Mist configuration" and "historic statistics monitoring") and are verified per Juniper’s API documentation and feature matrix.

Reference:

Juniper Mist API Introduction

Mist API Sample Class

Juniper Mist Automation Guide

RESTful API Overview | Mist

Question: 102

You are asked to create a dedicated guest WLAN which will only be available on the lobby access point (AP) at your office site.

How would you accomplish this task in Juniper Mist?

- A. Create a new WLAN called "Guest" in the existing WLAN template assigned to the office site.
 - B. Create a new WLAN template called "Guest" and assign it to the office site.
 - C. Apply a "Guest" organization label to the lobby AP.
 - D. Create a new "Guest" WLAN template and add it to the lobby AP using a device profile.
-

Answer: D

Explanation:

Comprehensive and Detailed Explanation verified by Juniper Mist documentation:

To ensure a guest WLAN is available only on a specific lobby AP, the correct approach according to Juniper Mist best practices is to create a new "Guest" WLAN template and add it to the lobby AP using a device profile. This method leverages device profiles for targeted SSID airtime availability, allowing granular WLAN assignment to selected APs (not all APs or sites). Juniper's documentation and solution briefs confirm that device profiles control which SSIDs broadcast on specific access points within a site, supporting scenarios like dedicated guest access only in particular areas such as the lobby.

Creating WLANs in standard templates enables SSID broadcast across all assigned APs, not selectively per device. Organization labels do not restrict SSID broadcast for individual APs.

Verification:

Your selected answer in the image ("Create a new 'Guest' WLAN template and add it to the lobby AP using a device profile") is correct and aligns with Juniper's recommended workflow.

**

Reference:

[Juniper Mist WLAN Template and Device Profile Documentation](#)

Mist Management Guide

[Juniper Mist Implementation Best Practices](#)
