ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"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

Warning: Keep connected with our support team for latest updates

Question: 1

What is a key feature of Juniper Mist Wired Assurance?

A. Dynamic VLAN assignment
B. AI-driven switch insights
C. Firewall rule orchestration
D. Zero Trust micro-segmentation

Answer: B

Explanation:

Wired Assurance offers AI-driven visibility into switch health, port performance, and client-level experience. This enables faster root cause analysis. It does not manage firewall rules or micro-segmentation.

Question: 2

Which Mist component enables user-level visibility across wired and wireless connections?

A. Marvis VNA
B. Mist Edge
C. Wired Assurance
D. Client Health SLE

Answer: D

Explanation:

The Client Health Service Level Expectation (SLE) provides unified visibility for wired and wireless experiences. It measures onboarding time, throughput, and other KPIs to help ensure consistent client connectivity.

Question: 3

Which data does Wireless Assurance collect for anomaly detection?

A. Client application data
B. DHCP and DNS stats
C. RF signal metrics
D. Switch port errors

Answer: C

Explanation:

Wireless Assurance collects real-time RF metrics, including signal strength, noise, SNR, and interference, to detect wireless anomalies. It does not focus on switch-level data or client app behavior.

Question: 4

Which two Service Level Expectations (SLEs) are part of Wireless Assurance? (Choose two.)

A. Roaming success
B. WAN latency
C. Throughput
D. BGP convergence

Answer: A, C

Explanation:

Wireless Assurance includes SLEs like roaming and throughput to monitor wireless experience. WAN latency and BGP convergence relate more to WAN and routing functions, not Wi-Fi health.

Question: 5

What role does Marvis play in Wired Assurance workflows?

A. Acts as a switch controller
B. Orchestrates campus routing
C. Uses AI to assist troubleshooting
D. Pushes firmware to switches

Answer: C

Explanation:

Marvis provides AI-driven troubleshooting for Wired Assurance by interpreting telemetry and logs. It suggests root causes and recommends actions but does not act as a switch controller.

Question: 6

Which capability helps Wireless Assurance reduce Mean Time to Repair (MTTR)?

A. Radio Resource Management
B. Virtual AP tunneling
C. Dynamic RF planning
D. Root cause identification

Answer: D

Explanation:

Wireless Assurance uses machine learning to analyze failures and identify the root cause rapidly. This directly contributes to reducing MTTR for Wi-Fi-related issues.

Question: 7

Which Mist solution provides port-level insights for connected wired clients?

A. Access Assurance
B. Wired Assurance
C. Secure Edge
D. Port Authentication Manager

Answer: B

Explanation:

Wired Assurance delivers real-time port-level analytics for wired clients, allowing visibility into traffic, errors, and power usage. It is not involved in access control or security.

Question: 8

Which two data types are collected by Wired Assurance? (Choose two.)

A. Port utilization metrics
B. Wireless signal strength
C. MAC address authentication
D. Switch health telemetry

Answer: A, D

Explanation:

Wired Assurance gathers switch health data, such as temperature, CPU, memory, and port-level metrics like utilization and errors. Wireless signal strength is managed under Wireless Assurance.

Question: 9

What is the function of Wireless Assurance onboarding SLE?

A. To measure software update time
B. To assess client authentication time
C. To monitor RF interference
D. To report PoE consumption

Answer: B

Explanation:

The onboarding SLE tracks how quickly and successfully clients connect to the network, including DNS, DHCP, and authentication stages. It ensures a smooth initial experience for users.

Question: 10

Which Mist tool would help visualize switch-level anomalies across time?

A. Anomaly Timeline
B. Port Inspector
C. Marvis Dashboard
D. Device Inventory

Answer: A

Explanation:

The Anomaly Timeline provides a historical view of abnormalities on switches, helping administrators track trends and identify recurring issues. Port Inspector offers real-time snapshots instead.

Question: 11

Which feature of Wireless Assurance helps optimize Wi-Fi performance proactively?

A. Scheduled VLAN rotation
B. Automatic RF adjustments
C. Intent-based micro-segmentation
D. Link Aggregation Control Protocol

Answer: B

Explanation:

Wireless Assurance uses AI to recommend or implement proactive RF adjustments for better signal and channel quality. VLANs and LACP relate to wired switching, not RF optimization.

Question: 12

Which metric is used by the Wireless Assurance throughput SLE?

A. Ping latency
B. TCP throughput test results
C. Port error count
D. Wi-Fi channel width

Answer: B

Explanation:

Wireless Assurance uses TCP throughput tests to measure the actual user experience on Wi-Fi. It gives a realistic performance view, unlike latency or channel width alone.

Question: 13

What does the term "port bounce" refer to in Wired Assurance troubleshooting?

A. Port is overloaded
B. Port receives DDoS
C. Port is shut and enabled automatically
D. Port loops traffic

Answer: C

Explanation:

A "port bounce" is the process of administratively disabling and re-enabling a port to recover from issues like stuck sessions or failed negotiation. It’s a common troubleshooting method.

Question: 14

What information does Port Health in Wired Assurance display?

A. Firewall rule matches
B. Cable test results
C. VLAN routing paths
D. Application usage

Answer: B

Explanation:

Port Health includes cable diagnostics, power delivery stats, and traffic error monitoring. It does not handle firewall rules, VLAN paths, or app-layer data.

Question: 15

Which SLE category is not part of Wireless Assurance by default?

A. Coverage
B. Roaming
C. Gateway Latency
D. Throughput

Answer: C

Explanation:

Gateway Latency is typically not included in Wireless Assurance's default SLEs, which focus more on Wi-Fi-specific metrics like coverage, onboarding, throughput, and roaming.

Question: 16

What is a key outcome of using Wireless Assurance’s AI-driven insights?

A. Creation of physical network topologies
B. Reduction in manual ticket resolution
C. Improvement in routing table distribution
D. Faster cable replacement planning

Answer: B

Explanation:

Wireless Assurance uses AI to detect and suggest solutions for Wi-Fi issues, reducing the manual workload on IT teams and accelerating issue resolution through automation.

Question: 17

What is the purpose of assigning switch profiles in Wired Assurance?

A. To enforce IPS policies

B. To manage routing tables
C. To apply standardized port configs
D. To extend VLANs across buildings

Answer: C

Explanation:

Switch profiles are used to apply consistent port configurations across similar switch models or roles. They ensure uniform behavior, which simplifies operations and provisioning.

Question: 18

Which dashboard allows viewing site-wide wireless health KPIs in Mist?

A. Site Performance
B. Site Map
C. SLE Overview
D. Topology

Answer: C

Explanation:

The SLE Overview dashboard aggregates key metrics across the wireless infrastructure, such as onboarding time, throughput, and signal quality. It helps visualize client experience at a site level.

Question: 19

What key advantage does Mist Wireless Assurance have over traditional Wi-Fi monitoring tools?

A. MACsec encryption
B. AI-driven Root Cause Analysis
C. VLAN auto-provisioning
D. DNS inspection

Answer: B

Explanation:

Wireless Assurance uses Marvis AI to perform root cause analysis, which dramatically improves issue detection speed and accuracy compared to manual Wi-Fi monitoring.

Question: 20

Which two roles does Marvis play in Wireless Assurance? (Choose two.)

A. Chat-based interface for queries
B. L2/L3 policy orchestration
C. Suggests SLE optimization
D. Configures switch stack IDs

Answer: A, C

Explanation:

Marvis acts as a conversational AI to respond to IT queries and suggest optimizations, especially for SLEs. It doesn't configure switches or create routing policies directly.

Question: 21

What is a primary function of Juniper Mist Access Assurance?

A. Provides WAN optimization
B. Manages switch PoE profiles
C. Controls user access with 802.1X policies
D. Automates BGP peer configuration

Answer: C

Explanation:

Access Assurance provides identity-based access control using policies such as 802.1X, MAC authentication, and guest access. It does not handle WAN optimization or BGP configuration.

Question: 22

Which platform integrates with Mist Access Assurance to manage authentication policies?

A. RADIUS server
B. AWS Lambda
C. Azure Blob Storage
D. ElasticSearch

Answer: A

Explanation:

Mist Access Assurance integrates with a RADIUS server for identity authentication and policy enforcement. It supports 802.1X and MAC-based policies through the RADIUS protocol.

Question: 23

Which two user roles can be assigned in Mist Access Assurance? (Choose two.)

A. Contractor
B. Guest
C. Static route
D. BGP neighbor

Answer: A, B

Explanation:

Access Assurance allows defining user roles like guest or contractor, each with specific access permissions. Routing-related roles like BGP neighbor are not user-level assignments.

Question: 24

Which data type is used to define policy in Access Assurance?

A. ASN
B. User identity and role
C. TCP port numbers
D. VLAN priority bits

Answer: B

Explanation:

Policies in Access Assurance are defined based on user identity and role, allowing dynamic segmentation. This enables context-aware network access enforcement for users or devices.

Question: 25

What is the role of Mist Edge in Access Assurance?

A. Hosts the routing table
B. Acts as the AAA server
C. Extends policy enforcement to campus network
D. Performs MAC learning

Answer: C

Explanation:

Mist Edge acts as a policy enforcement point in distributed enterprise networks, bringing Mist cloud policies to the wired and wireless edge. It doesn't host routing or perform AAA directly.

Question: 26

Which Juniper feature enables seamless user movement across sites with consistent access policies?

A. Dynamic DNS
B. Dynamic User Segmentation
C. BGP Confederations
D. Route Reflectors

Answer: B

Explanation:

Dynamic User Segmentation ensures that users have consistent policy enforcement across multiple network locations, regardless of their physical attachment point.

Question: 27

Which component of Routing Assurance validates configuration consistency across routers?

A. Marvis Edge Engine
B. EVPN Instance Validator
C. Routing Policy Checker
D. Configuration Drift Detection

Answer: D

Explanation:

Routing Assurance detects configuration drifts across routing devices and compares intended vs. running configurations to ensure consistency. It proactively prevents misconfiguration issues.

Question: 28

Routing Assurance allows integration with which of the following systems for path monitoring?

A. Syslog collectors
B. SNMPv1 traps
C. Telemetry platforms
D. ChatGPT API

Answer: C

Explanation:

Routing Assurance integrates with telemetry platforms to gather real-time data for route validation, anomaly detection, and SLA monitoring. SNMPv1 and Syslog provide basic monitoring but are not primary.

Question: 29

What type of anomalies does Routing Assurance detect in BGP sessions?

A. Web traffic spikes
B. DNS lookup failures
C. Peer flaps and misroutes
D. MAC address duplication

Answer: C

Explanation:

Routing Assurance detects BGP-related anomalies like frequent flapping, route leaks, and unexpected peer behaviors. It does not monitor DNS, web traffic, or MAC-related issues.

Question: 30

What functionality does Marvis provide for Routing Assurance?

A. Assigns OSPF priorities
B. Suggests fixes for routing misconfigurations
C. Detects DHCP server failures
D. Provides cable diagnostics

Answer: B

Explanation:

Marvis can interpret routing telemetry data and offer suggestions to resolve misconfigurations, especially for BGP or OSPF. It does not handle physical layer diagnostics or DHCP monitoring.

Question: 31

Which two routing protocols are monitored under Routing Assurance? (Choose two.)

A. OSPF
B. RIPv1
C. BGP
D. SMTP

Answer: A, C

Explanation:

Routing Assurance monitors dynamic routing protocols like OSPF and BGP for health, topology changes, and SLA violations. SMTP is a mail protocol and RIPv1 is outdated.

Question: 32

Which SLE metric might be used in Access Assurance to evaluate onboarding time?

A. Time to first DHCP lease
B. Route convergence
C. TCP retransmissions
D. Number of BGP AS paths

Answer: A

Explanation:

Access Assurance evaluates user onboarding using metrics like DHCP success, authentication time, and role assignment delays. Routing metrics like AS paths or TCP retransmissions are unrelated.

Question: 33

What does "policy intent verification" mean in Routing Assurance?

A. Logging commands for firewall rules
B. Verifying that route paths match desired policies
C. Checking for ARP table consistency
D. Inspecting packet payloads

Answer: B

Explanation:

Routing Assurance verifies whether actual route paths match the intended policy configuration (intent). This helps ensure that traffic flows are following business-defined policies.

Question: 34

Which key benefit does Access Assurance provide for regulatory compliance?

A. Manual logging of all devices
B. Auditable access control and identity enforcement
C. Integration with firewall clustering
D. IPsec VPN auto-negotiation

Answer: B

Explanation:

Access Assurance logs identity-based access activity and policy enforcement, making it easier to meet compliance standards like HIPAA, PCI-DSS, and SOX.

Question: 35

What happens if Access Assurance fails to authenticate a client?

A. Client is always disconnected
B. Client is given full access by default
C. Guest fallback policy can be applied
D. Static IP is assigned

Answer: C

Explanation:

If Access Assurance fails to authenticate a client, it can apply a fallback policy (e.g., limited guest access) based on predefined rules. This ensures continuity with restricted access.

Question: 36

Which feature of Routing Assurance helps ensure redundancy and SLA compliance?

A. Route path visualization
B. Ping test scripts
C. Application-layer deep packet inspection
D. DNSSEC verification

Answer: A

Explanation:

Routing Assurance visualizes route paths and detects issues like single points of failure or degraded performance, helping meet SLAs. It operates at the network layer, not application layer.

Question: 37

What does Access Assurance dynamically assign upon successful authentication?

A. Port speed
B. VLAN and Role
C. IP route
D. Switch hostname

Answer: B

Explanation:

Access Assurance dynamically assigns VLANs and user roles based on authentication results. This enables network segmentation and access control tied to identity.

Question: 38

Which component enables Access Assurance to detect rogue devices?

A. Spanning Tree Protocol
B. Marvis anomaly detection
C. MAC Authentication Bypass
D. Device fingerprinting

Answer: D

Explanation:

Access Assurance uses device fingerprinting to identify known vs. unknown devices, allowing policies to be applied or alerts triggered for rogue detection. STP is a loop prevention protocol.

Question: 39

Which two services are part of Juniper's Routing Assurance offering? (Choose two.)

A. Route simulation
B. Wi-Fi onboarding
C. Peer state monitoring
D. Switch stacking

Answer: A, C

Explanation:

Routing Assurance includes features like route simulation for intent verification and peer state monitoring for dynamic protocols. Wi-Fi and stacking are not its primary domains.

Question: 40

Which Juniper Mist service enforces policy across both wired and wireless networks based on user identity?

A. Access Assurance
B. Routing Assurance Marvis VNA Mist Edge Fabric
C. **Answer: A**
D. **Explanation:**

Access Assurance is responsible for enforcing identity-based access control across both wired and wireless environments. It works in tandem with cloud policies and local enforcement points.

Question: 41

What is the primary function of Apstra within Juniper's data center architecture?

A. Enforces endpoint firewalls
B. Provides AI-driven data center intent-based networking
C. Manages PoE budgets across campuses
D. Controls SD-WAN tunnels

Answer: B
Explanation:

Apstra is Juniper's intent-based networking platform for data centers. It abstracts the desired state (intent) and ensures the infrastructure behaves accordingly, with continuous validation and closed-loop automation.

Question: 42

What does Marvis VNA for Data Center help visualize and monitor?

A. L7 application logs
B. User onboarding flows
C. Data center fabric anomalies
D. VPN tunnels

Answer: C
Explanation:

Marvis VNA in the data center context detects anomalies in fabric operations, such as misconfigured links, traffic bottlenecks, or underlay/overlay issues. It doesn't handle application or VPN monitoring.

Question: 43

Which two features are provided by Apstra intent-based analytics? (Choose two.)

A. Predictive link failure detection
B. Intent-based policy rollback
C. Native email encryption
D. VLAN mirroring

Answer: A, B
Explanation:

Apstra includes analytics to predict issues like link failures and provides rollback features for policy changes that violate intent. It does not deal with email encryption or VLAN-specific diagnostics.

Question: 44

In SD-WAN, which component is responsible for establishing secure tunnels across WAN links?

A. WAN Edge device
B. Apstra Agent
C. Marvis VNA
D. Top-of-rack switch

Answer: A
Explanation:

WAN Edge devices manage IPsec or SSL tunnels between sites, enabling secure connectivity over public or private WANs. They handle dynamic path selection and traffic prioritization.

Question: 45

Which protocol is primarily used by Juniper SD-WAN for control plane operations?

A. OSPF
B. BGP-LS
C. TCP over TLS
D. Secure Vector Routing (SVR)

Answer: D

Explanation:

Juniper's SD-WAN solution uses Secure Vector Routing (SVR) for control and data plane communications. It securely distributes routes and policies across WAN Edge devices.

Question: 46

Which key capability does Apstra provide to prevent human-induced errors?

A. Real-time IP scanning
B. Intent validation and continuous assurance
C. Port mirroring
D. VLAN pruning

Answer: B

Explanation:

Apstra's closed-loop assurance continuously validates configurations against the intended design, reducing configuration errors caused by human missteps or misalignment.

Question: 47

What is the role of Marvis in SD-WAN monitoring?

A. Encrypts MPLS circuits
B. Performs AI-driven troubleshooting for WAN links
C. Applies dynamic IPsec configuration
D. Hosts web-based configuration UI

Answer: B

Explanation:

Marvis uses telemetry and AI models to monitor and troubleshoot SD-WAN performance, helping identify link issues, congestion, or path flaps. It is not used for encryption or hosting UI.

Question: 48

What does Apstra use to continuously validate the network state against the intended design?

A. SNMP walk
B. Real-time CLI commands
C. Telemetry + intent graph comparison
D. NetFlow data export

Answer: C

Explanation:

Apstra combines real-time telemetry with an intent-based graph that models the desired network state. This allows it to detect and alert on deviations from the intended architecture.

Question: 49

Which topology model does Apstra typically deploy in a data center?

A. Hub-and-Spoke
B. Ring topology
C. EVPN-VXLAN Clos fabric
D. Full Mesh Layer 3 VPN

Answer: C

Explanation:

Apstra supports EVPN-VXLAN in a Clos (leaf-spine) fabric as a common data center architecture. It enables scalability, segmentation, and consistent policy enforcement across the fabric.

Question: 50

Which two benefits does Mist SD-WAN offer compared to traditional WAN? (Choose two.)

A. Manual route updates
B. AI-based path selection
C. Secure vector routing
D. Static policy enforcement

Answer: B, C

Explanation:

Mist SD-WAN leverages AI to make dynamic path decisions based on performance and uses Secure Vector Routing (SVR) for secure, scalable control. Manual updates and static policies are legacy approaches.

Question: 51

Which tool can be used to simulate the effect of a proposed change in Apstra?

A. Mist Insights
B. Change Control Simulation Engine
C. Marvis CLI
D. Cloud Telemetry Sandbox

Answer: B

Explanation:

Apstra includes a Change Control Simulation Engine that allows administrators to preview the impact of network changes. This helps prevent configuration errors before deployment.

Question: 52

Which aspect of SD-WAN does Application-Aware Routing impact?

A. Firewall logging
B. DNS redirection
C. Path selection based on app performance
D. VRF segmentation

Answer: C

Explanation:

Application-Aware Routing (AAR) dynamically routes application traffic based on real-time link performance (jitter, latency, loss). It ensures critical apps use the best path.

Question: 53

What is the function of the Apstra Intent Graph?

A. Maps wireless client onboarding
B. Represents the desired state of the data center fabric
C. Logs all firewall rule updates
D. Converts VRF to VLAN

Answer: B

Explanation:

The Intent Graph is a visual representation of how the data center is intended to operate, including connectivity, protocols, and services. It helps track compliance to the intended network behavior.

Question: 54

What problem does Apstra's rollback mechanism help solve?

A. DNS poisoning
B. Policy violation due to misconfigurations
C. High CPU usage on switches
D. Link-level jitter

Answer: B

Explanation:

Apstra supports rollback to a previously known good state if a configuration causes an intent violation. This helps quickly restore network compliance and availability.

Question: 55

Which metrics are monitored by SD-WAN to determine path performance?

A. BGP AS path length
B. CPU temperature
C. Latency, jitter, and packet loss
D. DNS TTL values

Answer: C

Explanation:

SD-WAN solutions track link metrics such as latency, jitter, and packet loss to choose optimal paths for application traffic. These are critical for maintaining user experience.

Question: 56

What is a key difference between Apstra and traditional data center management?

A. Apstra uses VLANs only
B. Apstra provides closed-loop automation based on intent
C. Traditional DCs use only wireless switches
D. Apstra relies on manual provisioning

Answer: B

Explanation:

Unlike traditional systems that require manual provisioning and auditing, Apstra automates configuration, monitoring, and correction based on intent-defined policies and state validation.

Question: 57

Which Juniper solution supports AI-based SD-WAN routing and integrates with Marvis?

A. Apstra vMX
B. WAN Edge + Mist Cloud
C. Contrail Service Orchestration
D. Sky ATP

Answer: B

Explanation:

Juniper’s WAN Edge appliances work with Mist Cloud and Marvis to support AI-driven SD-WAN with intelligent path decisions, WAN visibility, and security integration.

Question: 58

What type of assurance does Marvis VNA offer in the data center environment?

A. App-layer DPI
B. Behavioral anomaly detection and recommendation
C. Physical cabling fault detection
D. VLAN loop prevention

Answer: B

Explanation:

Marvis VNA in the data center uses AI to detect behavioral anomalies (e.g., sudden topology changes) and recommends corrective actions. It does not inspect app payloads or cabling directly.

Question: 59

What is the main goal of Secure Vector Routing in Juniper SD-WAN?

A. Encrypt email headers
B. Prevent SD-WAN path loops
C. Provide secure and scalable control plane
D. Force VLAN translations

Answer: C

Explanation:

Secure Vector Routing (SVR) provides a secure, efficient, and scalable control and data plane mechanism between WAN Edge devices. It replaces legacy MPLS or static VPN methods.

Question: 60

Which two operations are automated by Apstra in the data center? (Choose two.)

A. Auto firmware updates of access points
B. Underlay and overlay configuration
C. Intent rollback
D. NAT traversal

Answer: B, C

Explanation:

Apstra automates both the configuration of underlay/overlay networking and rollback in case of a policy violation. It does not manage AP firmware or NAT-specific functions.