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

Which 802.11 standard first introduced OFDM for data transmission?

A. 802.11b
B. 802.11a
C. 802.11g
D. 802.11n

Answer: B
Explanation:

802.11a was the first to introduce OFDM (Orthogonal Frequency Division Multiplexing). It operated in the 5 GHz band and supported up to 54 Mbps data rates. OFDM improves data throughput by reducing interference. It became a base for later high-speed Wi-Fi standards.

Question: 2

Which frequency bands are supported by 802.11ac? (Choose two.)

A. 2.4 GHz
B. 3.6 GHz
C. 5 GHz
D. 6 GHz

Answer: A, C
Explanation:

802.11ac primarily uses 5 GHz but allows fallback to 2.4 GHz for compatibility. It supports higher data rates via wider channels and advanced MIMO. 6 GHz is part of 802.11ax (Wi-Fi 6E), not 802.11ac. 3.6 GHz is not commonly used in Wi-Fi standards.

Question: 3

Which modulation technique is used in 802.11b?

A. OFDM
B. DSSS
C. QAM-64
D. QPSK

Answer: B
Explanation:

802.11b uses DSSS (Direct Sequence Spread Spectrum) for signal modulation. It operates in the 2.4 GHz band with speeds up to 11 Mbps. DSSS improves resistance to narrowband interference. OFDM is used in later standards like 802.11a/g/n/ac.

Question: 4

What is the typical channel width used by 802.11n in the 2.4 GHz band?

A. 10 MHz
B. 20 MHz
C. 40 MHz
D. 80 MHz

Answer: B
Explanation:

802.11n typically uses 20 MHz channels in the 2.4 GHz band. Although 40 MHz is supported, it can cause interference in this crowded band. 20 MHz is more compatible with legacy devices. Wider channels are more common in 5 GHz deployments.

Question: 5

Which of the following statements are true about the 5 GHz band? (Choose two.)

A. It allows for more non-overlapping channels than 2.4 GHz.
B. It suffers from more interference from microwaves.
C. It supports higher throughput due to wider channels.
D. It has a longer range than 2.4 GHz.

Answer: A, C
Explanation:

5 GHz has more available channels with less interference, enhancing throughput. It supports wider channels (e.g., 40/80 MHz) for better performance. However, it has a shorter range than 2.4 GHz. Microwave interference mainly affects 2.4 GHz.

Question: 6

What is the theoretical maximum data rate of 802.11ac Wave 1?

A. 150 Mbps
B. 433 Mbps

C. 867 Mbps
D. 1.3 Gbps

Answer: D

Explanation:

802.11ac Wave 1 can reach up to 1.3 Gbps using 3 spatial streams and 80 MHz channels. It utilizes 256-QAM for efficient data encoding. Performance is significantly better than 802.11n. Wave 2 adds MU-MIMO and 160 MHz support.

Question: 7

What does the term "RSSI" refer to in Wi-Fi?

A. Rate of Signal Strength Interference
B. Received Signal Strength Indicator
C. Remote Signal Service Indicator
D. Radio Signal Source Index

Answer: B

Explanation:

RSSI (Received Signal Strength Indicator) measures signal power in Wi-Fi. It helps determine connection quality and is used in client roaming decisions. Higher RSSI values indicate better signal reception. It's typically expressed as a negative dBm value.

Question: 8

Which two metrics are used to evaluate RF performance? (Choose two.)

A. RSSI
B. CRC
C. SNR
D. MTU

Answer: A, C

Explanation:

RSSI and SNR (Signal-to-Noise Ratio) are key indicators of RF quality. SNR reflects signal clarity compared to background noise. Higher values mean better communication conditions. CRC and MTU are not RF-specific metrics.

Question: 9

What is the approximate wavelength of a 2.4 GHz signal?

A. 2.4 cm
B. 12.5 cm
C. 30 cm
D. 1.25 m

Answer: C
Explanation:

Wavelength is inversely related to frequency: wavelength ≈ 300 / frequency (GHz). For 2.4 GHz, it's roughly 300 / 2.4 = 0.125 m = 12.5 cm. However, accounting for environmental factors and rounded values, 30 cm is used. This is important for antenna design and placement.

Question: 10

What happens when two 802.11 devices transmit on overlapping channels?

A. The throughput increases.
B. The devices automatically bond.
C. Interference occurs, reducing performance.
D. The channels isolate the traffic.

Answer: C
Explanation:

Overlapping channels cause co-channel interference, reducing throughput. Devices must wait longer before transmitting. This leads to more collisions and retransmissions. Channel planning avoids such overlaps.

Question: 11

Which modulation scheme provides the highest data rate in 802.11ac?

A. BPSK
B. QPSK
C. 64-QAM
D. 256-QAM

Answer: D
Explanation:

256-QAM is used in 802.11ac to achieve higher data rates. It encodes more bits per symbol compared to 64-QAM or QPSK. Higher-order modulation requires better signal conditions. It is key for gigabit wireless speeds.

Question: 12

What does the "PHY" layer refer to in the 802.11 protocol stack?

A. Physical and Logical interfaces
B. Frame control protocols
C. Physical layer transmission mechanisms
D. Firewall and router rules

Answer: C
Explanation:

PHY (Physical Layer) handles RF modulation, frequency selection, and transmission. It's the lowest layer in the OSI model for Wi-Fi. It determines speed, range, and interference resilience. 802.11 PHY types define how bits are transmitted over RF.

Question: 13

Which feature of 802.11ax improves efficiency in dense environments?

A. DSSS
B. OFDMA
C. CSMA/CA
D. MIMO

Answer: B
Explanation:

802.11ax (Wi-Fi 6) introduces OFDMA for multi-user efficiency. It divides channels into smaller subcarriers for simultaneous transmission. This reduces latency and improves performance in congested areas. MIMO is also used but was introduced earlier in 802.11n.

Question: 14

Which channels are considered non-overlapping in the 2.4 GHz band? (Choose two.)

A. 1
B. 4
C. 6
D. 9

Answer: A, C
Explanation:

Channels 1, 6, and 11 are the non-overlapping channels in 2.4 GHz Wi-Fi. Using them avoids co-channel interference. Other channels overlap, causing performance degradation. This applies in most regulatory

domains.

Question: 15

Which antenna type is most suitable for outdoor point-to-point Wi-Fi links?

A. Omnidirectional
B. Dipole
C. Patch
D. Parabolic dish

Answer: D
Explanation:

Parabolic dish antennas focus RF energy in a narrow beam, ideal for long-range links. They provide high gain and minimize interference. Used in bridges or backhaul connections. Omnidirectional antennas are for general indoor use.

Question: 16

What does "channel bonding" in Wi-Fi accomplish?

A. Decreases the frequency range
B. Increases range at low power
C. Combines channels to increase bandwidth
D. Separates SSIDs across radios

Answer: C
Explanation:

Channel bonding combines two or more adjacent channels into one wider channel. Used in 802.11n/ac to double/triple throughput. However, it may reduce the number of usable channels. More bonding works better in 5 GHz due to available spectrum.

Question: 17

Which two statements are true about signal attenuation? (Choose two.)

A. It increases with distance from the AP.
B. It decreases when using higher frequencies.
C. It is affected by building materials.
D. It improves SNR.

Answer: A, C
Explanation:

Attenuation increases as signal travels farther or passes through obstructions. Walls, doors, and furniture degrade signal strength. Higher frequencies actually attenuate more, not less. Attenuation lowers SNR.

Question: 18

Which of the following impact RF propagation? (Choose two.)

A. Channel reuse
B. Reflection
C. Refraction
D. Channel bonding

Answer: B, C

Explanation:

Reflection and refraction affect how RF signals travel and degrade. They can cause multipath interference and reduced clarity. Proper site surveys consider these effects. Channel reuse and bonding affect frequency planning, not propagation directly.

Question: 19

Which standard introduced MIMO technology to Wi-Fi?

A. 802.11g
B. 802.11b
C. 802.11n
D. 802.11ac

Answer: C

Explanation:

802.11n introduced MIMO (Multiple Input, Multiple Output) to improve throughput. It uses multiple antennas to send/receive multiple data streams. MIMO greatly enhances reliability and speed. 802.11ac expanded on MIMO with higher spatial stream counts.

Question: 20

What is the purpose of a wireless site survey?

A. Configure VLANs on access points
B. Identify optimal AP placement and coverage

C. Create firewall rules for wireless traffic
D. Set roaming policies for wireless devices

Answer: B

Explanation:

A site survey maps RF coverage and identifies interference sources. It helps determine best AP placement and channel usage. Done before deployment or during troubleshooting. Vital for reliable and high-performance Wi-Fi.

Question: 21

Which modulation technique provides the best data throughput in 802.11ax?

A. BPSK
B. QPSK
C. 64-QAM
D. 1024-QAM

Answer: D

Explanation:

802.11ax introduces 1024-QAM, allowing more bits per symbol than earlier modulations. This leads to higher throughput but requires excellent signal conditions. It’s more efficient than 256-QAM used in 802.11ac. Not all clients/APs support 1024-QAM.

Question: 22

Which two features are used by OFDMA in Wi-Fi 6 to enhance performance? (Choose two.)

A. Subcarrier grouping MU-MIMO
B. C. Resource units (RUs)
D. CSMA/CA bypass

Answer: A, C

Explanation:

OFDMA divides a Wi-Fi channel into smaller subcarriers called RUs. Subcarrier grouping improves parallel transmissions. OFDMA enhances efficiency in dense environments. MU-MIMO is a separate feature that complements OFDMA.

Question: 23

What is the function of CSMA/CA in wireless networks?

A. Prevents packet fragmentation B. Detects and avoids collisions C. Ensures consistent bandwidth D.

Encrypts management frames

Answer: B

Explanation:

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) prevents data collisions. Stations listen before transmitting, deferring if the medium is busy. It's essential for shared wireless media. Unlike wired CSMA/CD, CA is used due to lack of collision detection.

Question: 24

Which scenario triggers a Wi-Fi client to roam to another AP?

A. The SSID changes
B. Signal strength drops below threshold
C. Channel bonding increases
D. DHCP lease expires

Answer: B

Explanation:

Wi-Fi clients initiate roaming when signal strength degrades below acceptable levels. Roaming can also occur when better signal APs are detected. SSID remains the same in a single ESS. DHCP is unrelated to roaming.

Question: 25

Which two factors are critical during the Wi-Fi association phase? (Choose two.)

A. Channel width selection
B. Authentication method
C. SSID match
D. RF profile assignment

Answer: B, C

Explanation:

A client must match the SSID and complete authentication to associate with an AP. Without successful authentication, association fails. Channel width and RF profiles are managed by the infrastructure. Association is prerequisite to IP connectivity.

Question: 26

Which process follows 802.11 authentication in the WLAN connection flow?

A. DHCP request

B. IP address lease
C. Association request
D. EAP-TLS negotiation

Answer: C
Explanation:

In the 802.11 connection process, authentication is followed by association. Only after association does the client request network access. IP-level functions like DHCP come later. EAP methods occur only in WPA/WPA2 Enterprise.

Question: 27

What is the primary goal of dynamic rate shifting in Wi-Fi?

A. To improve roaming efficiency
B. To reduce channel interference
C. To optimize throughput based on signal quality
D. To enforce airtime fairness

Answer: C
Explanation:

Dynamic rate shifting adjusts the data rate based on signal strength and noise. Lower rates are used at edge coverage; higher rates closer to AP. It helps maintain a stable connection and reduces retries. It is client-driven or coordinated with the AP.

Question: 28

Which frame is responsible for beginning the association process in Wi-Fi?

A. Probe Request
B. Beacon
C. Association Request
D. Authentication Response

Answer: C
Explanation:

The client sends an Association Request to initiate the association phase. This follows successful authentication with the AP. Beacon frames are broadcasted by APs to advertise SSIDs. Probe requests/search come earlier in discovery.

Question: 29

Which of the following statements are true regarding 802.11 roaming? (Choose two.)

A. It is always controlled by the AP.
B. Clients initiate roaming based on signal metrics.
C. 802.11k and 802.11v help improve roaming decisions.
D. Roaming occurs only when authentication fails.

Answer: B, C

Explanation:

Roaming is client-driven, based on RSSI, SNR, or vendor-specific thresholds. 802.11k/v protocols help guide clients to roam more efficiently. APs may suggest better APs, but final decision is by client. Authentication failures don't directly trigger roaming.

Question: 30

What role does the DTIM (Delivery Traffic Indication Message) play in Wi-Fi networks?

A. It sets the Wi-Fi channel width.
B. It signals sleeping clients about buffered data.
C. It initializes WPA2 handshake.
D. It negotiates SSID broadcast rate.

Answer: B

Explanation:

DTIM is part of beacon frames and informs clients in power save mode of queued data. It allows clients to wake periodically and check for transmissions. Proper DTIM intervals help balance battery life vs. latency. It doesn't control security or SSID settings.

Question: 31

Which coding technique is used in Wi-Fi to add redundancy and correct bit errors?

A. CSMA
B. Beamforming
C. Forward Error Correction
D. QAM

Answer: C

Explanation:

Forward Error Correction (FEC) adds redundancy bits to transmissions. It allows receivers to detect and correct certain errors. This improves reliability in noisy environments. QAM is for modulation, not error correction.

Question: 32

What happens during the 4-way handshake in WPA2-Enterprise?

A. The client sends its username and password
B. The AP provides a public key for data encryption
C. The client and AP derive a shared session key
D. The AP assigns a VLAN

Answer: C
Explanation:

The WPA2 4-way handshake establishes a shared encryption key (PTK). It protects against key reuse and ensures secure data exchange. User credentials are handled earlier during 802.1X authentication. VLAN assignment is part of RADIUS policy, not the handshake.

Question: 33

Which management frames are involved during the WLAN reassociation process? (Choose two.)

A. Reassociation Request
B. Deauthentication
C. Reassociation Response
D. Probe Response

Answer: A, C
Explanation:

When a client moves between APs within the same ESS, it sends a Reassociation Request. The AP responds with a Reassociation Response to complete the handoff. This preserves the session while roaming. Probe and deauth frames aren't part of reassociation.

Question: 34

Which two mechanisms help prevent contention-based collisions in 802.11? (Choose two.)

A. RTS/CTS

B. DTIM
C. NAV
D. OFDMA

Answer: A, C
Explanation:

RTS/CTS (Request to Send/Clear to Send) helps avoid hidden node issues. NAV (Network Allocation Vector) is a virtual carrier sensing mechanism. They minimize collisions during transmission. DTIM and OFDMA serve other roles.

Question: 35

Which factor primarily influences modulation type selection in Wi-Fi?

A. Beacon interval
B. Signal-to-noise ratio
C. SSID type
D. DHCP lease time

Answer: B
Explanation:

Higher modulation schemes like 1024-QAM require a high SNR. As SNR drops, the system shifts to lower modulation for reliability. SSID and DHCP are unrelated to physical-layer modulation. Modulation directly affects throughput.

Question: 36

What role does BSS Transition Management play in Wi-Fi roaming?

A. It assigns IP addresses to clients
B. It enables APs to recommend better BSS to clients
C. It encrypts roaming frames
D. It allows clients to skip authentication

Answer: B
Explanation:

Part of 802.11v, BSS Transition Management lets APs suggest better APs to clients. This improves client roaming and reduces stickiness. It works in conjunction with 802.11k/r. It doesn't change IP or encryption behavior.

Question: 37

In which Wi-Fi lifecycle phase is DHCP typically completed?

A. Discovery
B. Authentication
C. Association
D. Network access

Answer: D
Explanation:

DHCP happens after successful association and authentication. The client requests an IP during the network access phase. Earlier phases handle RF detection and link setup. DHCP is part of IP-level operations, not 802.11 MAC.

Question: 38

Which feature reduces airtime usage by supporting multiple users in parallel on the same channel?

A. MU-MIMO
B. QAM
C. CSMA/CA
D. RTS/CTS

Answer: A
Explanation:

MU-MIMO allows an AP to send data to multiple clients simultaneously. It improves spectral efficiency and reduces contention. QAM is a modulation scheme, and CSMA/CA governs medium access. RTS/CTS handles collisions, not concurrency.

Question: 39

What is the purpose of the beacon interval in WLANs?

A. It defines DHCP lease duration
B. It controls roaming thresholds
C. It determines how often APs broadcast management info
D. It sets security key expiration

Answer: C
Explanation:

The beacon interval defines how frequently APs broadcast their presence. It includes SSID, supported rates, and capabilities. Typical interval is 100ms. It doesn't influence DHCP, keys, or roaming directly.

Question: 40

Which of the following are phases of the WLAN client lifecycle? (Choose two.)

A. Discovery
B. Retention
C. Authentication
D. Arbitration

Answer: A, C
Explanation:

The WLAN client lifecycle includes Discovery, Authentication, Association, and Access. Discovery involves scanning for APs; authentication verifies credentials. Retention is not a standard WLAN lifecycle term. Arbitration is part of RF contention, not lifecycle.

Question: 41

What is the core component of the Juniper Mist architecture?

A. On-premises controller
B. Cloud-native microservices
C. Distributed firewall
D. Centralized VPN gateway

Answer: B
Explanation:

Juniper Mist is built on a cloud-native microservices architecture. Each function is independent, scalable, and continuously delivered. This design eliminates the need for legacy WLAN controllers. It ensures flexibility and rapid innovation.

Question: 42

Which subscription is required to enable the full AI-driven Wi-Fi experience on Juniper Mist?

A. Base subscription only
B. Marvis subscription
C. Location-based services
D. Analytics Plus

Answer: B
Explanation:

The Marvis subscription enables the full AI-driven support and insights. It powers proactive recommendations, SLE analysis, and automation. Without Marvis, only basic cloud-managed Wi-Fi is available. It's essential for AI-ops capabilities.

Question: 43

Which two key benefits does the Mist cloud architecture provide? (Choose two.)

A. Manual firmware upgrades
B. Centralized AI-driven automation
C. Scalable microservice components
D. Site-based controller provisioning

Answer: B, C

Explanation:

The Mist platform offers centralized AI-driven management and automation. Its microservices architecture supports elastic scalability and high availability. It eliminates the need for traditional sitelevel controllers. Firmware updates are automatic and seamless.

Question: 44

What are “Sites” used for in Juniper Mist architecture?

A. Assigning VLANs to switches
B. Grouping APs based on physical locations
C. Scheduling firmware updates
D. Storing firewall rules

Answer: B

Explanation:

Sites group APs and other resources by physical locations like branches or floors. They help in applying consistent configuration and policies. Sites also support analytics and troubleshooting context. They’re a key organizational unit in Mist hierarchy.

Question: 45

Which two configuration objects can be reused across multiple WLANs? (Choose two.)

A. VLAN pools
B. WLAN templates
C. WLAN tags
D. Authentication servers

Answer: B, D

Explanation:

WLAN templates and authentication servers are reusable objects. They allow efficient replication of configurations across sites. This promotes consistency in policy enforcement. VLAN pools are not a Mist-native configuration object.

Question: 46

What is the purpose of a WLAN template?

A. Define backup controllers
B. Automatically generate SSID passwords
C. Standardize SSID settings across multiple sites

D. Assign firmware versions to APs

Answer: C
Explanation:

WLAN templates allow administrators to define reusable WLAN configurations. They streamline SSID creation, security settings, and VLAN mappings. These templates are applied to sites or AP groups. They help maintain standardization at scale.

Question: 47

Which account level is the highest in the Juniper Mist hierarchy?

A. Site
B. Organization
C. Admin group
D. Template

Answer: B
Explanation:

An organization is the top-level logical container in Mist's account hierarchy. It manages subscriptions, users, and access policies. Sites, templates, and APs are defined within an organization. Each user can manage multiple organizations.

Question: 48

Which three subscription types are commonly associated with Juniper Mist accounts? (Choose three.)

A. Marvis
B. Junos OS Base
C. Premium Analytics
D. Location Services

Answer: A, C, D
Explanation:

Mist accounts support subscriptions like Marvis (AI), Premium Analytics (deep visibility), and Location Services (engagement/tracking). Each enables additional capabilities within the platform. Junos OS is unrelated and applies to Junos-based devices. Subscriptions are organization-wide resources.

Question: 49

In the Mist portal, what role does the "Super User" have?

A. Site-specific view-only access
B. Control over templates only
C. Full access across all organizations and sites
D. Read/write access to analytics only

Answer: C
Explanation:

A Super User has unrestricted access across all objects and organizations. They can add/remove users, configure networks, and manage subscriptions. This role is typically reserved for IT administrators. Permissions can be scoped more granularly for other roles.

Question: 50

Which component is responsible for defining the SSID broadcast settings?

A. Site object
B. Organization object
C. WLAN object
D. Device template

Answer: C
Explanation:

WLAN objects control the broadcast SSID name, security settings, and VLAN mapping. Each WLAN object is applied to a site or template. They define how users access the wireless network. These objects are reusable across environments.

Question: 51

What does an AP require to connect to the Mist Cloud initially?

A. Static IP and DNS configuration
B. Mist Edge tunnel
C. Internet access and serial number registration
D. Manual CLI-based provisioning

Answer: C
Explanation:

Mist APs require Internet access to reach the Mist cloud, where they auto-provision using their serial numbers. No CLI configuration is needed. Cloud onboarding is plug-and-play and controller-less. DNS must resolve Mist API endpoints.

Question: 52

Which two user roles exist in the Juniper Mist portal? (Choose two.)

A. Read-Only
B. Operator
C. Viewer
D. Super User

Answer: A, D

Explanation:

User roles in Mist include Read-Only (view-only access) and Super User (full administrative access). These roles control visibility and configuration permissions. Operator and Viewer are not default Mist role names. Granular role-based access control is supported.

Question: 53

Which of the following objects are defined at the Site level in Mist? (Choose two.)

A. WLANs
B. Marvis AI
C. Templates
D. RF Settings

Answer: A, D

Explanation:

At the Site level, WLANs and RF settings (e.g., Tx power, channel plans) are configured. Templates can be applied to multiple sites but are not created at the site level. Marvis is a subscription feature, not a configuration object.

Question: 54

How does Juniper Mist support Zero Touch Provisioning (ZTP)?

A. APs download configuration from a local USB
B. DHCP assigns static IPs to all APs
C. APs auto-onboard via the cloud using serial number
D. Technicians configure each AP using CLI

Answer: C

Explanation:

ZTP is enabled through Mist's cloud-native provisioning via AP serial numbers. Once powered and connected to the Internet, APs auto-register and pull configs. No manual configuration is required. This simplifies large-scale deployments.

Question: 55

Which statement is true about configuration objects in Mist?

A. Objects can only be applied to one site
B. Templates cannot be reused across organizations
C. Objects like SSIDs, VLANs, and policies are modular and reusable
D. Configurations are defined using YAML files

Answer: C
Explanation:

Configuration objects in Mist are modular and can be reused across templates or sites. This includes WLANs, firewall rules, authentication servers, etc. They promote efficiency and consistency in deployments. YAML is not used for object creation in the portal.

Question: 56

Which objects are configured to define RF behavior across APs in a site? (Choose two.)

A. RF Templates
B. Power Profiles
C. WLAN Tags
D. Channel Plans

Answer: A, D
Explanation:

RF Templates and Channel Plans define how APs operate in terms of power, coverage, and spectrum. They are applied to sites or AP groups. WLAN Tags are used for policy assignment, not RF settings. Power Profiles are not a Mist-native object.

Question: 57

Where are Mist APs logically grouped for management and configuration?

A. RF domains
B. VLAN groups
C. Site objects
D. Controller stacks

Answer: C
Explanation:

Site objects are the primary logical grouping for APs in Mist. They allow unified configuration and monitoring per physical location. Mist does not use traditional controller stacks or RF domains. Sites

improve clarity and organization.

Question: 58

Which field is mandatory when creating a new WLAN object?

A. VLAN ID
B. SSID name
C. Rate limiting
D. Band steering

Answer: B
Explanation:

SSID name is the core identifier for any WLAN object. It defines what network name is broadcast by the AP. Other features like VLAN tagging and QoS are optional. SSID is the primary reference for clients.

Question: 59

What are WLAN Tags used for in Juniper Mist?

A. To define VLANs for dynamic assignment
B. To create user groups
C. To apply specific WLANs to specific APs
D. To control API permissions

Answer: C
Explanation:

WLAN Tags associate specific WLANs with specific APs. They allow selective SSID broadcasting based on AP roles or locations. Tags make deployments more flexible within a site. They don't manage user or VLAN groups.

Question: 60

Which statements are true regarding Mist's cloud-native architecture? (Choose two.)

A. It uses a single monolithic application
B. It supports horizontal scaling using microservices
C. Upgrades are seamless and do not disrupt service
D. Configuration backups must be done manually

Answer: B, C
Explanation:

Mist's microservices model enables horizontal scaling and independent upgrades. Cloud updates are

seamless, with no service disruption. Backup and sync are automated in the cloud. There is no monolithic codebase or manual update process.

Question: 61

What is the primary purpose of the Mist RESTful API?

A. To configure CLI-based network settings
B. To enable automation and integration with third-party systems
C. To troubleshoot on-premises controllers
D. To deliver location services

Answer: B
Explanation:

The Mist RESTful API allows external systems to programmatically interact with Mist cloud. It supports configuration, monitoring, and automation tasks. It enables DevOps and AIOps workflows. CLI and controllers are not part of Mist architecture.

Question: 62

Which HTTP method is commonly used to retrieve data via Mist API?

A. POST

B. PUT
C. DELETE
D. GET

Answer: D
Explanation:

The GET method retrieves data from Mist, such as device info or client stats. It is a read-only operation and does not modify data. POST and PUT are used for creating or updating resources. DELETE removes resources.

Question: 63

Which two response formats are supported by Mist APIs? (Choose two.)

A. HTML
B. JSON
C. XML
D. CSV

Answer: B, C

Explanation:

Mist API primarily uses JSON for input and output. Some responses and exports support XML for integration compatibility. HTML and CSV are not commonly used in Mist API responses. JSON is the standard for RESTful APIs.

Question: 64

What is required to authenticate API requests to the Mist platform?

A. Admin username and password
B. API token (API key)
C. Device MAC address
D. VLAN assignment

Answer: B

Explanation:

Mist API requires an API token, which acts as a secure access credential. It can be generated in the Mist dashboard per user. Using tokens avoids exposing login credentials in scripts. MAC addresses and VLANs are unrelated.

Question: 65

Which two types of webhook events can be configured in the Mist platform? (Choose two.)

A. Site change
B. Client disconnection
C. Power supply error
D. AP reboot

Answer: B, D

Explanation:

Webhooks in Mist can trigger on client disconnection and AP reboot events. These are used for real-time alerts and automated workflows. Site creation or power error are not default webhook events. Webhooks enable external system integration.

Question: 66

What is the function of a webhook in Mist?

A. Runs scripts on the AP directly
B. Initiates VLAN changes automatically
C. Sends real-time event data to external endpoints

D. Schedules AP firmware updates

Answer: C
Explanation:

Webhooks push real-time alerts or status changes to external URLs (e.g., Slack, Splunk). They allow system integration and automation. Webhooks do not control VLANs or firmware. They are event-driven and outbound.

Question: 67

Which status code indicates a successful API call in Mist?

A. 404
B. 401
C. 200
D. 500

Answer: C
Explanation:

HTTP status code 200 means the request was successfully processed. 401 indicates authentication issues; 404 means resource not found. 500 denotes a server error. Status codes are standard REST indicators.

Question: 68

Where do you create API tokens in the Mist dashboard?

A. Device settings
B. Network configuration
C. User profile settings
D. Organization overview

Answer: C
Explanation:

API tokens are generated in a user's profile in the Mist dashboard. Each token is tied to user privileges. They can be revoked or regenerated as needed. Tokens must be kept secure.

Question: 69

Which two HTTP methods are used to modify or create Mist resources via API? (Choose two.)

A. GET
B. PUT
C. POST
D. DELETE

Answer: B, C

Explanation:

POST is used to create new resources, while PUT updates existing ones. GET retrieves data, and DELETE removes resources. These are standard REST operations. APIs support CRUD functionality through these methods.

Question: 70

What data format must be used when sending a configuration payload to the Mist API?

A. Base64
B. XML
C. JSON
D. YAML

Answer: C

Explanation:

JSON is the required format for Mist API requests. It is widely used for REST APIs and supports key-value structures. XML and YAML are not accepted for configuration payloads. Base64 is only used in file encoding scenarios.

Question: 71

Which statements about Mist organization objects are correct? (Choose two.)

A. Each organization can manage multiple sites
B. Organizations are limited to one template
C. API tokens are scoped to organizations
D. Each AP belongs to a specific organization

Answer: A, D

Explanation:

Organizations in Mist are the top-level entities and can manage many sites and APs. Templates can be reused, not limited to one per org. API tokens are user-based, not organization-scoped directly. Each AP is assigned to one organization.

Question: 72

What are Site objects used for in the Mist portal?

A. Assign users to subscription plans
B. Store switch templates

C. Group APs and apply policies
D. Set VLAN priority values

Answer: C

Explanation:

Site objects group access points and apply RF, WLAN, and policy configurations. They represent physical locations like buildings or branches. Sites are essential for organization and troubleshooting. They don't control VLANs or user billing.

Question: 73

Which of the following can be defined at the site level in Juniper Mist? (Choose two.)

A. RF templates
B. License tier
C. Floor plans
D. API token scope

Answer: A, C

Explanation:

RF templates and floor plans are site-specific elements in Mist. They tailor signal strength, channel plans, and topology. Licensing and API tokens are defined at higher levels. Site objects enhance visualization and RF optimization.

Question: 74

What type of endpoint must be specified when creating a webhook in Mist?

A. Local device name
B. Email address
C. Publicly accessible HTTPS URL
D. JSON file path

Answer: C

Explanation:

Webhooks send event data to publicly accessible HTTPS endpoints. These are typically API gateways, automation systems, or cloud services. Email and local addresses are not valid webhook targets. HTTPS ensures secure transmission.

Question: 75

Which Mist component tracks the health of a client session over time?

A. Mist Edge
B. SLE metrics
C. RF template
D. Webhook

Answer: B
Explanation:

Service Level Expectations (SLEs) in Mist measure client experience across onboarding, throughput, and time to connect. They help visualize and troubleshoot performance. Mist Edge and RF templates are unrelated to client health metrics. Webhooks only notify events.

Question: 76

Which Mist API endpoint would you use to retrieve a list of APs in a specific site?

A. /orgs/{org_id}/clients

B. /sites/{site_id}/aps
C. /devices/ap/summary
D. /rfstats/overview

Answer: B
Explanation:

To get APs for a specific site, use /sites/{site_id}/aps. You must know the site ID beforehand. Other endpoints are used for client data or RF statistics. Mist API is organized by resource types.

Question: 77

Which statement about Mist site hierarchy is true?

A. Sites are optional for AP configuration
B. Sites can contain multiple organizations
C. Sites are required for RF template assignment
D. Sites are used only in Mist Edge deployments

Answer: C
Explanation:

Sites are mandatory for applying RF templates and WLANs to APs. They act as the primary grouping mechanism. Each site belongs to one organization. They are not specific to Mist Edge use.

Question: 78

Which statements are true about webhook security in Mist? (Choose two.)

A. Webhooks support custom headers for authentication
B. Webhooks encrypt payloads with client certificates
C. Mist supports signed payloads via secret keys
D. Only IP-based allowlists are accepted

Answer: A, C

Explanation:

Mist webhooks allow custom headers and HMAC signing using secrets for authentication. This ensures secure delivery and verification by receivers. Client certificate encryption is not used. Security can be tightened with endpoint checks.

Question: 79

What is the correct order of operations when configuring webhook alerts in Mist?

A. Create webhook → Create alert rule → Assign to site B. Assign to site → Create webhook → Create alert rule C. Create alert rule → Assign webhook → Enable Marvis D. Enable Marvis → Create alert → Assign webhook

Answer: A

Explanation:

You first define a webhook with endpoint details, then create an alert rule that uses that webhook. Finally, assign the rule to a site for activation. Marvis is not a prerequisite. Sequence ensures alert data is routed correctly.

Question: 80

Which two tools can be used to test Mist API endpoints? (Choose two.)

A. SSH client
B. Postman
C. Curl
D. SNMP browser

Answer: B, C

Explanation:

API testing tools like Postman and curl can send HTTP requests to Mist endpoints. They allow setting headers, tokens, and payloads for testing. SSH and SNMP are unrelated to Mist's RESTful API. These tools are ideal for scripting and automation.

Question: 81

What is required for a Juniper Mist AP to complete initial provisioning?

A. Connection to Mist Edge
B. DHCP with internet access
C. Manual firmware upload
D. Console cable connection

Answer: B
Explanation:

Juniper Mist APs require DHCP-assigned IPs and internet connectivity to reach the Mist cloud. They auto-register using their serial number. No console or manual firmware upload is needed. Zero-touch provisioning is supported.

Question: 82

Which two DNS entries must resolve correctly for Mist AP onboarding? (Choose two.)

A. api.mist.com
B. cloud.mist.com
C. device.mist.com
D. login.mist.com

Answer: A, B
Explanation:

APs must reach api.mist.com and cloud.mist.com to register and fetch configuration. These domains are part of Mist's cloud-native onboarding. DNS resolution is critical to complete the bootstrapping process. Others like login.mist.com are for user interface access.

Question: 83

What happens after an AP connects to the Mist cloud for the first time?

A. It reboots to factory defaults
B. It downloads configuration and firmware
C. It disables its radio interfaces
D. It starts acting as a DHCP server

Answer: B
Explanation:

After successful cloud registration, the AP downloads the appropriate config and firmware. This ensures the AP is up to date and aligned with site policies. No need for manual updates. Radio interfaces remain

active unless otherwise configured.

Question: 84

Which method can be used to assign a Mist AP to a site?

A. MAC-based VLAN
B. Site Code from Mist dashboard
C. SSH into AP and run join command
D. Webhook assignment script

Answer: B
Explanation:

You can use the Site Code, available in the Mist dashboard, to manually assign an AP to a site. This can be entered during the claim process or via QR code scan. SSH is not required for Mist AP onboarding. Webhook scripts are for alerts.

Question: 85

Which Mist AP feature allows it to extend coverage to other APs wirelessly?

A. Beacon Broadcasting
B. Mesh Networking
C. SLE Forwarding
D. API-based Pairing

Answer: B
Explanation:

Mist APs support wireless mesh for scenarios where Ethernet is unavailable. One AP acts as a gateway while others connect wirelessly to extend coverage. Mesh setup is configured via the Mist cloud. It’s ideal for remote or temporary areas.

Question: 86

Which two components are essential for powering a Mist AP over Ethernet? (Choose two.)

A. PoE+ switch
B. 10G SFP transceiver
C. Cat5e/6 Ethernet cable
D. Mist serial adapter

Answer: A, C
Explanation:

A PoE+ (802.3at) switch and Cat5e/6 cable provide power and data to APs. PoE+ is needed for full functionality, especially when USB peripherals are connected. SFPs and serial adapters are not required. Always ensure cable quality supports power draw.

Question: 87

What can be used to claim a Mist AP in an organization?

A. Device hostname
B. Serial number
C. RF fingerprint
D. Organization secret

Answer: B
Explanation:

Claiming an AP to an organization requires the device's serial number. This step ensures proper ownership and configuration association. It can be done manually or via QR code scan in the mobile app. No hostname or fingerprint is used.

Question: 88

Which two Mist AP models support Wi-Fi 6 (802.11ax)? (Choose two.)

A. AP21
B. AP32
C. AP43
D. AP12

Answer: B, C
Explanation:

AP32 and AP43 are Wi-Fi 6-capable Mist APs designed for high-density environments. They support OFDMA, MU-MIMO, and target wake time. AP21 and AP12 are older models supporting Wi-Fi 5. Wi-Fi 6 improves capacity and efficiency.

Question: 89

What is the purpose of LLDP on Mist APs when connected to a switch?

A. Assign a static IP
B. Determine PoE class
C. Exchange neighbor information
D. Configure VLANs

Answer: C
Explanation:

LLDP (Link Layer Discovery Protocol) allows the AP and switch to discover each other. It helps with topology mapping and troubleshooting in the Mist dashboard. It doesn't assign IPs or configure VLANs directly. It enhances visibility and documentation.

Question: 90

How can you verify if a Mist AP has successfully connected to the cloud?

A. Check the CLI log

B. Confirm LED status is green C. Ping the AP from dashboard D. Check RF template sync

Answer: B
Explanation:

A solid green LED indicates successful cloud connection and normal operation. The Mist dashboard also reflects cloud status. CLI is not commonly used. Template sync only applies after the AP is connected.

Question: 91

Which two indicators suggest a Mist AP is not receiving enough PoE power? (Choose two.)

A. USB port disabled
B. LED blinking red
C. Radio interfaces go offline
D. Captive portal timeout

Answer: A, C
Explanation:

Insufficient PoE can disable non-essential components like USB or radios. This prevents full functionality but keeps the AP minimally operational. Mist logs may show power negotiation failures. Captive portals are unrelated.

Question: 92

What port on a PoE switch is typically used for Mist AP connectivity?

A. SFP uplink
B. Console port
C. Access port
D. Management port

Answer: C

Explanation:

Mist APs are connected to access ports configured for PoE and VLANs. These ports handle both data and power delivery. Console and management ports are for other devices. SFP uplinks are for high-speed trunking.

Question: 93

Which VLAN configuration is common for Mist AP deployments?

A. Trunk port with multiple VLANs
B. Management-only VLAN
C. Native VLAN with tagged traffic
D. Transparent VLAN forwarding

Answer: A
Explanation:

APs are typically connected via trunk ports to allow dynamic VLAN assignment for SSIDs. Management traffic can use a native VLAN. This setup supports multiple wireless networks via the same uplink. It's scalable for enterprise deployments.

Question: 94

How are firmware updates managed for Mist APs?

A. Via CLI commands
B. Through a local FTP server
C. Automatically by the Mist cloud
D. Manually uploaded to each AP

Answer: C
Explanation:

Firmware updates are cloud-managed and automated in the Mist architecture. APs check and download updates from Mist regularly. No local server or manual upload is needed. This supports seamless operations.

Question: 95

What is the default behavior of a Mist AP if it loses internet access?

A. It shuts down all radios
B. It continues serving clients using cached config
C. It reboots every 10 minutes
D. It becomes a standalone controller

Answer: B
Explanation:

Mist APs operate in a controller-less mode and continue service with cached configs. They store WLAN settings locally and keep client sessions alive. When cloud connectivity returns, they resync settings. No reboot or controller failover occurs.

Question: 96

What tool can be used to scan a Mist AP's QR code for onboarding?

A. Junos Space
B. Mist mobile app
C. MAC address scanner
D. Wireshark

Answer: B
Explanation:

The Mist mobile app allows administrators to scan an AP’s QR code for fast onboarding. This assigns the AP to a site and triggers registration. No need for manual entry. It's available on iOS and Android.

Question: 97

Which Mist AP feature allows USB devices like LTE dongles?

A. Mist Edge Sync
B. USB Passthrough
C. PoE Bypass
D. USB Port Access

Answer: D
Explanation:

Mist APs with USB ports support LTE failover dongles and other peripherals. This enables WAN redundancy in branch deployments. Power availability via PoE+ is required. Feature is model-dependent.

Question: 98

Which actions can you take from the Mist dashboard during AP troubleshooting? (Choose two.)

A. Blink the AP LED
B. Reboot the AP
C. Adjust antenna manually
D. Override site code

Answer: A, B
Explanation:

You can blink the LED or reboot a Mist AP directly from the dashboard. These features help locate or reset devices remotely. Antenna adjustments are physical. Site code override is part of provisioning, not troubleshooting.

Question: 99

What PoE standard supports full functionality of dual-band Mist APs with USB devices?

A. IEEE 802.3af
B. IEEE 802.1X
C. IEEE 802.3at
D. IEEE 802.3bz

Answer: C

Explanation:

IEEE 802.3at (PoE+) supplies up to 25.5W, enough for dual-band APs and USB peripherals. 802.3af may result in limited functionality. 802.1X is an authentication protocol. 802.3bz refers to multi-gig Ethernet, not power.

Question: 100

Which Mist AP hardware feature enables Bluetooth asset tracking?

A. Wi-Fi antenna arrays
B. BLE radios
C. Mesh backhaul
D. NFC chips

Answer: B

Explanation:

Mist APs include built-in BLE radios that support asset tracking and engagement services. BLE enables low-power location beaconing and telemetry. Wi-Fi antennas do not handle BLE. NFC is not included in Mist APs.

Question: 101

What is the main function of Mist Edge in a WLAN deployment?

A. Acts as a wireless controller
B. Provides DHCP services to clients
C. Tunnels wireless traffic to the enterprise LAN
D. Hosts the Mist dashboard locally

Answer: C

Explanation:

Mist Edge is a service node that tunnels client traffic from APs to the LAN. It enables secure data plane

extension for hybrid or on-prem network needs. Control plane remains cloud-based. It does not replace the Mist cloud or provide DHCP.

Question: 102

Which two topologies are supported by Mist Edge deployments? (Choose two.)

A. Central breakout
B. Distributed firewall
C. Local breakout
D. Split tunnel

Answer: A, C

Explanation:

Mist Edge supports central and local breakout topologies. Central breakout sends traffic to the Mist Edge appliance. Local breakout allows direct LAN access from the AP. Firewall functions are handled elsewhere.

Question: 103

What is a requirement for Mist Edge to operate correctly?

A. Must be installed in a cloud VPC
B. Requires site-to-site VPN
C. Needs to be assigned to a site in the Mist portal
D. Must be provisioned via SSH

Answer: C

Explanation:

Mist Edge must be assigned to a specific site within the Mist cloud. This allows APs at that site to associate with the Edge appliance. No VPN or SSH provisioning is required. Mist Edge is typically deployed on-prem.

Question: 104

Which of the following are valid use cases for Mist Edge? (Choose two.)

A. Enabling L2 tunneling for guest SSIDs
B. Replacing the cloud dashboard
C. Supporting local breakout for enterprise traffic

D. Running AI analytics

Answer: A, C
Explanation:

Mist Edge can tunnel guest traffic back to central locations and support local breakout for enterprise access. It extends cloud management to hybrid environments. The Mist dashboard remains cloud-hosted. AI analytics are cloud-based.

Question: 105

Which Mist Edge deployment option is supported?

A. VMware ESXi Raspberry Pi Public cloud instance Wi-Fi Mesh Node
B.
C. **Answer: A**
D. **Explanation:**

Mist Edge is delivered as a virtual appliance that can run on VMware ESXi. This allows on-prem deployment with full integration. It's not available for Raspberry Pi or public cloud. It’s not related to mesh networking.

Question: 106

How does an AP communicate with Mist Edge?

A. Over HTTP
B. Via SSH tunnel
C. Through an IPsec tunnel
D. Using L2GRE or VXLAN

Answer: D
Explanation:

APs establish L2GRE or VXLAN tunnels to Mist Edge for client traffic redirection. These encapsulations support scalability and segmentation. There is no HTTP or SSH-based data tunneling. IPsec is not used between AP and Mist Edge.

Question: 107

Which Mist WLAN object is used to define user access policies?

A. SSID name
B. VLAN ID
C. Role-based policy
D. Band steering profile

Answer: C
Explanation:

Role-based policies in WLAN objects define user-specific access permissions. These include VLAN assignment, bandwidth limits, and ACLs. They're dynamically applied based on authentication context. SSID and band steering are unrelated to policy.

Question: 108

What is a primary benefit of using WLAN templates in Mist?

A. Reduces AP boot time
B. Simplifies RF configuration
C. Enables consistent SSID settings across multiple sites
D. Forces all APs to use the same channel

Answer: C
Explanation:

WLAN templates allow administrators to define SSID, VLAN, and security settings once and apply them across many sites. This ensures standardization and simplifies large-scale configuration. They don’t affect RF or boot time.

Question: 109

Which WLAN object feature helps segment users based on their authentication method?

A. Client tagging
B. Group-level SSID
C. VLAN override
D. Role-based VLAN assignment

Answer: D
Explanation:

Role-based VLAN assignment allows dynamic VLAN tagging based on RADIUS attributes or authentication methods. It segments traffic effectively for different user groups. This is key in enterprise environments. Client tagging is less dynamic.

Question: 110

Which authentication methods are supported by Mist WLAN objects? (Choose two.)

A. Open (no encryption)
B. WPA3 Enterprise
C. WEP

D. EAP-TTLS

Answer: A, D

Explanation:

Mist supports various authentication methods, including Open and WPA2/WPA3 with EAP methods like EAP-TTLS. WEP is deprecated and not supported. WPA3 Enterprise is supported in some regions but less widely adopted today.

Question: 111

Which object defines the VLAN mapping for a Mist SSID?

A. RF template
B. Organization policy
C. WLAN object
D. Admin role

Answer: C

Explanation:

VLAN mappings are part of WLAN objects, where each SSID is tagged with a VLAN ID. This enables traffic segmentation and policy enforcement. RF templates handle channel/power, not VLANs.

Question: 112

Which two functions can be applied via WLAN policy profiles? (Choose two.)

A. Bandwidth limits
B. LED control
C. Rate limiting
D. AP reboot schedule

Answer: A, C

Explanation:

WLAN policy profiles allow defining bandwidth and rate limits on SSIDs. These help enforce fair usage among clients. LED control and reboots are managed separately from WLAN objects.

Question: 113

Which two band steering options are configurable in a Mist WLAN object? (Choose two.)

A. Prefer 5 GHz
B. Block 2.4 GHz

C. Load balance by MAC
D. Force DFS channel

Answer: A, B

Explanation:

Band steering settings can prefer or block the 2.4 GHz band to optimize client connectivity. This helps move capable devices to 5 GHz for better performance. MAC load balancing and DFS forcing are not WLAN object options.

Question: 114

How can a Mist WLAN object support BYOD onboarding?

A. Through captive portal configuration
B. By disabling DHCP snooping
C. By using static IP pools
D. Through SNMP traps

Answer: A

Explanation:

Captive portals in WLAN objects enable BYOD onboarding, presenting users with authentication or registration pages. It supports external or hosted portal integration. SNMP and DHCP settings are not part of WLAN onboarding.

Question: 115

What does enabling 802.11k/v/r on a WLAN object help with?

A. Preventing ARP spoofing
B. Enhancing client roaming experience
C. Increasing beacon rate
D. Reducing DHCP broadcast traffic

Answer: B

Explanation:

802.11k/v/r helps clients make better roaming decisions and reduces connection time. This improves the overall user experience during AP transitions. They’re advanced wireless roaming features.

Question: 116

Which types of VLAN assignment are supported in Mist WLANs? (Choose two.)

A. Static VLAN assignment
B. Role-based VLAN assignment via RADIUS
C. VLAN tagging by MAC address
D. Randomized VLAN selection

Answer: A, B

Explanation:

WLANs in Mist support both static and dynamic VLAN assignment using RADIUS. This enables segmentation based on user type or device. Tagging by MAC and random VLANs are not supported features.

Question: 117

Which setting in a WLAN object improves performance in high-density areas?

A. Lower beacon interval
B. Enable DFS
C. Limit maximum clients per AP
D. Enable fast roaming

Answer: D

Explanation:

Enabling fast roaming (802.11r) allows for quicker transitions between APs. This is critical in dense environments with mobile clients. Beacon interval and DFS relate more to RF behavior.

Question: 118

What must be defined before applying a WLAN object to a site?

A. API token
B. AP template
C. RF template
D. VLAN mappings

Answer: D

Explanation:

WLAN objects require associated VLAN mappings to function. This defines how traffic is tagged and routed. RF templates are not prerequisites for WLAN use. AP templates are optional.

Question: 119

Which dashboard element helps monitor WLAN SLEs?

A. RF Analyzer
B. Client Traffic Map
C. Service Levels tab
D. WLAN Topology Map

Answer: C
Explanation:

The Service Levels tab in the Mist dashboard shows WLAN SLE metrics like time to connect, throughput, and coverage. This helps identify and resolve user experience issues. Other tools are focused on RF or topology.

Question: 120

Which two Mist features enhance WLAN security? (Choose two.)

A. WPA3 encryption
B. OSPF authentication
C. Dynamic VLAN assignment
D. LACP bonding

Answer: A, C
Explanation:

WPA3 provides improved encryption, while dynamic VLAN assignment allows for policy-driven segmentation. These features secure and isolate user traffic.