HPE6-A72 Training Course

Aruba Certified Switching Associate Exam

Structured Learning & Certification Preparation

Table of Contents

Introduction

The Aruba Certified Switching Associate certification validates foundational knowledge and practical understanding of enterprise switching technologies within modern network environments. It represents an entry-level credential that confirms a candidate's ability to support, configure, and manage switching solutions in campus and small-to-medium enterprise infrastructures. In today's IT landscape, where stable and secure connectivity underpins business operations, foundational switching knowledge remains essential for network reliability and scalability.

About This Training / Certification

This certification assesses foundational competencies in configuring and managing Layer 2 and basic Layer 3 switching features using Aruba solutions. It is positioned at an associate level and is suitable for individuals beginning their professional journey in networking or transitioning into roles involving infrastructure support. The certification forms part of a broader networking learning pathway, typically following general networking fundamentals and serving as a stepping stone toward more advanced switching, routing, or network design certifications.

What We Offer (AAAdemy)

AAAdemy provides structured training resources designed to support certification preparation and skill development across a wide range of IT domains. Our learning materials are built around clear knowledge structures, practical study guidance, and exam-oriented practice to help learners progress with confidence.

We offer well-organized knowledge explanations that break down complex topics into clear, understandable sections aligned with official exam objectives and real-world skill requirements. Each topic is designed to support both conceptual understanding and practical application.

Our study plans and learning guidance help learners follow a logical progression, focusing on key concepts, common pitfalls, and effective preparation strategies. This approach enables learners to study efficiently while maintaining a clear view of their learning goals.

To reinforce understanding, AAAdemy also provides practice questions and exam-focused insights that reflect typical certification scenarios. These resources are intended to help learners evaluate their readiness and strengthen their confidence before taking an exam.

All content is designed for flexible, self-paced learning, allowing individuals to study independently or alongside their existing professional or academic commitments.

Knowledge Overview

Domain: Identify, describe, and apply foundational networking architectures and technologies
Candidates are expected to understand core networking architectures and technologies that underpin enterprise environments. This includes applying foundational switching and routing concepts, recognizing infrastructure components, and interpreting how these technologies interact within structured network designs.

Domain: Identify, describe, and differentiate the functions and features of Aruba products and solutions
This area focuses on understanding the functional characteristics of Aruba solutions. Candidates should be able to describe product capabilities, differentiate features across solution types, and explain how specific functions support operational and design requirements in enterprise networks.

Domain: Install, configure, set up, and validate Aruba solutions
Candidates are expected to understand the processes involved in installing and configuring Aruba switching solutions. This includes initial setup concepts, applying configuration settings, and validating that the deployed solution operates according to defined requirements.

Domain: Tune, optimize, and upgrade Aruba solutions
This domain covers performance tuning, optimization practices, and solution upgrades. Candidates should understand how to maintain operational efficiency, apply configuration adjustments, and manage solution updates within a controlled environment.

Domain: Troubleshoot, repair, and replace Aruba solutions
Candidates are expected to apply structured troubleshooting methodologies to identify and resolve issues. This includes diagnosing configuration problems, understanding repair procedures, and recognizing when component replacement is necessary.

Domain: Manage, monitor, administer and operate Aruba solutions
This area focuses on ongoing operational management. Candidates should understand how to monitor network performance, administer configuration settings, and perform routine operational tasks to maintain stable and reliable Aruba switching environments.

Detailed Knowledge Explanation

HPE6-A72 Identify, describe, and apply foundational networking architectures and technologies

1. Networking Models and Architectures

The Open Systems Interconnection (OSI) and TCP/IP models provide the architectural framework required for interoperability within multi-vendor enterprise environments. The OSI model serves as a seven-layer reference for modularizing network functions, from Layer 1 (Physical) electrical signaling to Layer 7 (Application) software interfacing. Aruba switches facilitate high-performance operations primarily at Layer 2 (Data Link), managing frame delivery via MAC addresses and Virtual Local Area Networks (VLANs), and Layer 3 (Network), handling packet routing and IP addressing. Advanced filtering and Quality of Service (QoS) mechanisms further leverage Layer 4 (Transport) segment headers for port-based traffic control. While the OSI model remains an essential diagnostic reference, the functional reality of modern internetworking is the four-layer TCP/IP model: Network Interface, Internet, Transport, and Application.

Enterprise network design typically adheres to a Three-Tier Architecture to ensure deterministic traffic flow and modular scalability. The Access Layer serves as the entry point for end-user devices, utilizing switches such as the Aruba 2930F or CX 6200. The Distribution Layer aggregates access traffic and enforces routing policies using high-capacity hardware like the CX 6300. The Core Layer acts as the high-speed switching backbone, requiring maximum availability and throughput; here, modular chassis systems like the CX 8400 or 5400R reside, offering redundant supervisor engines and 100Gbps connectivity. These physical hierarchies are unified by logical addressing schemes to facilitate end-to-end communication.

2. Addressing and Subnetting

A structured IP addressing scheme is mandatory for optimizing broadcast domains and enforcing security boundaries. IPv4 addresses utilize a 32-bit dotted-decimal format, partitioned into four 8-bit octets. Historically categorized into Classes A through E, modern networks rely on private IP ranges—specifically 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16—to conserve public IPv4 space. Subnetting enables architects to divide large network blocks into smaller, logical subnets, enhancing performance by limiting the scope of broadcast traffic. Classless Inter-Domain Routing (CIDR) notation (e.g., /24) defines the network/host boundary, while wildcard masks facilitate granular matching within Access Control Lists (ACLs). When calculating usable host addresses, the formula 2^n - 2 must be applied, as the first address (Network ID) and last address (Broadcast Address) are reserved.

IPv6 addresses utilize a 128-bit hexadecimal structure to resolve IPv4 exhaustion. Key address types include Link-local (fe80::), Global Unicast (routable), and Multicast (ff00::). IPv6 replaces the broadcast-heavy Address Resolution Protocol (ARP) with the Neighbor Discovery Protocol (NDP). NDP is critical for five primary functions: Router Discovery, Prefix Discovery, Stateless Address Autoconfiguration (SLAAC), Neighbor Unreachability Detection, and Duplicate Address Detection. These addressing fundamentals ensure devices have unique identities for local and remote communication.

3. Switching and Layer 2 Concepts

Layer 2 switching optimizes local area network efficiency by forwarding data based on hardware identity. Switches maintain a Content Addressable Memory (CAM) or MAC address table to map specific physical ports to device MAC addresses, significantly reducing collision domains. Virtual Local Area Networks (VLANs) extend this by logically partitioning a single physical switch into multiple isolated domains, improving security and performance. Port membership is defined as Untagged (for end-host devices), Tagged (using 802.1Q headers for inter-switch trunks), or Native (for handling untagged traffic on a trunk).

Redundancy in Layer 2 topologies can lead to catastrophic broadcast storms. The Spanning Tree Protocol (STP) and Rapid STP (RSTP) prevent these loops by electing a Root Bridge and systematically blocking redundant paths. In Aruba environments, administrators can influence this election using the command `spanning-tree priority 4096`. For increased throughput and resilience, Link Aggregation (LAG) using the Link Aggregation Control Protocol (LACP) bundles multiple physical links into a single logical interface. This architectural stability at Layer 2 provides the fabric upon which inter-subnet routing is constructed.

4. Routing and Layer 3 Concepts

Layer 3 routing is the mechanism that enables communication between isolated VLANs and provides path determination to external networks. Routers and Layer 3 switches utilize routing tables to evaluate the best path for data delivery, with the Default Gateway acting as the egress point for non-local traffic. Routing strategies involve either Static routes—manually defined and suitable for small stubs—or Dynamic routing protocols. The Open Shortest Path First (OSPF) protocol is a prevalent link-state protocol that builds a complete topology map. OSPF neighbors must progress through a specific sequence of states to reach full adjacency: DOWN, INIT, 2-WAY, EXSTART, EXCHANGE, LOADING, and finally FULL.

The Address Resolution Protocol (ARP) acts as the fundamental bridge between Layer 3 and Layer 2, resolving a known IP address to a physical MAC address. On ArubaOS-CX switches, Layer 3 functionality must be explicitly enabled using the `ip routing` command. The precision of the routing table, verifiable via `show ip route`, determines the efficiency of the network fabric as it passes data to the Transport Layer for end-to-end delivery.

5. Transport Layer Concepts

The Transport Layer manages end-to-end data delivery and manages multiplexing through port numbers. The two primary protocols are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). TCP is connection-oriented and provides reliable, ordered delivery through a 3-way handshake (SYN, SYN-ACK, ACK), making it essential for services like HTTPS (443), SSH (22), and HTTP (80). Conversely, UDP is connectionless and prioritizes low-latency speed over reliability, commonly used for DNS (53), VoIP, and streaming.

Transport Layer multiplexing allows a single IP address to maintain multiple simultaneous sessions by assigning unique source and destination port numbers. For example, a switch management session uses TCP port 22 for SSH, while its monitoring agent might use UDP port 161 for SNMP. These protocols ensure that data encapsulated in Layer 3 packets is accurately delivered to the correct application-layer process. When traffic must reach multiple destinations simultaneously, the network employs multicast and broadcast mechanisms.

6. Multicast and Broadcast

Efficient one-to-many communication is achieved through broadcast and multicast traffic. Broadcast traffic (MAC: FF:FF:FF:FF:FF:FF) is forwarded to every device within a VLAN, which is necessary for ARP and DHCP but can impact performance if excessive. Multicast traffic utilizes the Class D IP range (224.0.0.0 to 239.255.255.255) to target specific groups of interested recipients.

Aruba switches utilize the Internet Group Management Protocol (IGMP) and IGMP Snooping to optimize multicast delivery. By snooping on IGMP Join and Leave messages, the switch maintains a map of which ports require specific multicast streams, preventing unnecessary traffic flooding across the VLAN. This ensures that bandwidth-intensive streams, such as high-definition video, only consume resources where required. These efficiency mechanisms are supported by various common network protocols that automate configuration.

7. Common Network Protocols

Automated network operations rely on standardized protocols for configuration, translation, and monitoring. The Dynamic Host Configuration Protocol (DHCP) utilizes the DORA process (Discover, Offer, Request, Acknowledge) for automated IP assignment. The Domain Name System (DNS) provides human-to-machine translation between FQDNs and IP addresses. Diagnostic reachability is verified via the Internet Control Message Protocol (ICMP), which facilitates tools such as Ping and Traceroute.

Network management is conducted via the Simple Network Management Protocol (SNMP), with SNMPv3 providing necessary encryption and authentication for secure monitoring. The Network Time Protocol (NTP) is vital for synchronizing system clocks to ensure log accuracy and certificate validity. For secure administrative access, Secure Shell (SSH) is the standard, replacing the insecure plaintext Telnet protocol. These services provide the foundation for managing diverse network topologies.

8. Network Topologies

The physical and logical layout of a network dictates its resilience and management overhead. The Star topology is the standard for the Access Layer, where each endpoint connects to a central switch, isolating failures to a single device. In the network Core and Distribution layers, a Mesh topology (full or partial) is preferred to provide redundant paths and high availability. While Ring and Bus topologies are largely legacy in modern Ethernet LANs, their principles inform specialized redundancy protocols. Selecting the appropriate topology is the prerequisite for determining the required physical media and cabling infrastructure.

9. Cabling and Media Types

Physical media selection is determined by bandwidth requirements and transmission distance. Copper cabling (Cat5e, Cat6, Cat6a) is limited to 100 meters, with Cat6a supporting 10Gbps throughput. For longer distances or high-speed backbones, fiber optic cabling is utilized. Single-Mode Fiber (SMF) supports long-distance spans (up to 40km), while Multi-Mode Fiber (MMF) is suitable for intra-building links (300m-500m).

Aruba switches leverage modular Small Form-factor Pluggable (SFP/SFP+) transceivers to support these media types. Common modules include:

- **SFP-1G-SX**: Multi-mode, ~550m.
- **SFP-1G-LX**: Single-mode, ~10km.
- **SFP-10G-SR**: Multi-mode, ~300m.
- **SFP-10G-LR**: Single-mode, 10–20km. For high-density, short-range (≤7m) data center connections, Direct Attach Cables (DAC) provide a cost-effective, integrated transceiver solution. These physical links must be secured by foundational access control concepts.

10. Foundational Security Concepts (Networking Level)

Security at the network edge is enforced through traffic filtering and port-level constraints. Access Control Lists (ACLs) permit or deny traffic based on IP, port, and protocol. Port Security restricts access by limiting the number of MAC addresses on a port or binding the port to a specific hardware ID. When a violation occurs, the switch can be configured to take one of three actions: Protect (drop frames), Restrict (drop and log), or Shutdown (disable the interface).

To mitigate rogue infrastructure threats, DHCP Snooping distinguishes between trusted ports (uplinks to legitimate servers) and untrusted ports (user access). This feature builds a binding table that lists authorized IP-to-MAC pairings, providing the database required for Dynamic ARP Inspection (protecting against ARP spoofing) and IP Source Guard (preventing IP spoofing). These foundational measures integrate deeply into the specialized Aruba product ecosystem.

11. Identify, describe, and apply foundational networking architectures and technologies Practice Question

Q1: In the OSI model, which layer is responsible for routing packets across different networks?
A. Data Link
B. Transport
C. Session
D. Network

Q2: What is the main purpose of the Spanning Tree Protocol (STP) in a Layer 2 network?
A. Preventing network loops
B. Encrypting broadcast traffic
C. Assigning MAC addresses
D. Increasing bandwidth between switches

Q3: Which of the following Aruba switch features enables traffic from multiple VLANs to traverse a single physical link?
A. Loop guard
B. Untagged ports
C. Tagged ports
D. Native VLAN

Q4: A user is assigned an IP address of 192.168.10.25 with a subnet mask of 255.255.255.0. What is the default gateway likely to be?
A. 255.255.255.0
B. 192.168.0.1
C. 192.168.10.1
D. 192.168.10.0

Q5: What is the role of the MAC address table on a Layer 2 switch?
A. To store port-to-MAC address mappings for forwarding decisions

B. To determine the shortest path to a destination network
C. To filter traffic by VLAN IDs
D. To resolve IP addresses into MAC addresses

Q6: Which protocol is used to dynamically form Link Aggregation Groups (LAGs) between two switches?
A. TCP
B. DHCP
C. OSPF
D. LACP

Q7: Which layer in the OSI model handles port numbers and ensures data is sent to the correct application?
A. Network
B. Transport
C. Data Link
D. Presentation

Q8: Which command would you use on an Aruba switch to verify the current IP routing table?
A. show ip route
B. show vlan
C. show arp
D. show spanning-tree

Q9: What does the CIDR notation /24 represent in IPv4 addressing?
A. 24 bits used for the network portion
B. 32 hosts in the network
C. Subnet mask of 255.0.0.0
D. 16 bits for host addresses

Q10: Which multicast IP address range is used for organization-defined multicast groups?
A. 224.0.0.1 – 224.0.0.255
B. 239.0.0.0 – 239.255.255.255
C. 225.0.0.0 – 229.255.255.255
D. 240.0.0.0 – 255.255.255.255

HPE6-A72 Identify, describe, and differentiate the functions and features of Aruba products and solutions

1. Aruba Product Families (Switching)

The Aruba portfolio provides a tiered range of hardware optimized for various network roles. The 2530 and 2540 series offer budget-friendly Layer 2 and Layer 3 Lite capabilities for SMBs. The 2930F and 2930M series serve as campus access workhorses, supporting VSF stacking and full Layer 3 routing. The modern CX 6200 and 6300 series bring the ArubaOS-CX operating system to the access and distribution layers, offering enhanced telemetry and modularity. At the high end, the CX 8320 and modular CX 8400 chassis provide 100Gbps density and VSX

redundancy for data center and campus cores. The portfolio is currently transitioning toward the modular, database-driven ArubaOS-CX operating system.

2. ArubaOS vs. ArubaOS-CX

The shift from legacy ArubaOS to ArubaOS-CX represents a transition from monolithic code to a modular, Linux-based architecture. Legacy ArubaOS utilizes a traditional CLI and offers limited historical telemetry. Conversely, ArubaOS-CX is built around a real-time state database that captures all configuration and operational data. This architecture enables the Network Analytics Engine (NAE), which utilizes the hardware-level Network Analytics Processor (NAP) to provide deep, historical telemetry. ArubaOS-CX natively supports REST APIs and Python scripting, facilitating advanced automation and self-healing capabilities that are not possible on legacy monolithic platforms.

3. Aruba Switching Features and Technologies

Aruba switches utilize distinct stacking and redundancy technologies. The Virtual Switching Framework (VSF) allows multiple switches to be managed via a Single Management Plane, ideal for access layer scaling. For core environments, the Virtual Switching Extension (VSX) creates an Active-Active Control Plane between two switches, enabling hitless firmware upgrades and synchronized state via an Inter-Switch Link (ISL). Beyond redundancy, features like ACLs and QoS (e.g., DSCP 46 for voice) ensure traffic integrity, while LACP and IGMP Snooping optimize link utilization and multicast distribution.

4. Aruba Network Management Platforms

Centralized management is achieved through three primary platforms. Aruba Central is a cloud-native solution providing AI-powered insights, Zero-Touch Provisioning (ZTP), and unified management for switches and APs. Aruba NetEdit is an on-premises tool specifically designed for ArubaOS-CX, offering multi-device configuration validation and automated auditing. For legacy environments, Aruba AirWave provides on-premises management for existing wired and wireless footprints. These platforms allow administrators to coordinate complex feature sets across the entire infrastructure.

5. Key Aruba Features

Aruba switches incorporate "Smart Network" features that automate deployment and visibility. The Network Analytics Processor (NAP) facilitates NAE by processing telemetry locally on the switch. Dynamic Segmentation and Colorless Ports automate access control by assigning VLANs and ACLs based on device identity rather than physical port location. Rapid deployment is achieved through Zero Touch Provisioning (ZTP), where switches automatically download firmware and configuration files from a ZTP server or Aruba Central upon initial boot.

6. Security and Access Features

Aruba integrates security into the switching fabric using 802.1X and MAC Authentication, typically coordinated through Aruba ClearPass (RADIUS). ClearPass enforces role-based access policies that follow the user regardless of their connection point. Local hardware defenses, including Port Security (Protect, Restrict, Shutdown actions), DHCP Snooping, and ARP Inspection, provide the first line of defense against internal threats. These security features are applied across all enterprise use cases.

7. Aruba Switching Use Cases

Optimal switch selection depends on the layer and performance requirements. SMBs typically utilize the 2530/2540 series for cost efficiency. Campus access layers benefit from the CX 6200 or 2930F. Distribution and Core layers requiring high availability utilize the CX 6300 (with VSF) or CX 8400 (with VSX). The CX 6300 is increasingly preferred over the 2930F for modern enterprises due to its modular architecture, full Layer 3 capabilities, and advanced NAP telemetry.

8. Differentiators vs. Competitors

Aruba’s competitive advantage lies in its "Unified Infrastructure" and the modularity of ArubaOS-CX. Built-in analytics via NAP and AI-driven root-cause analysis in Aruba Central reduce the need for external probes and manual troubleshooting. The vendor-agnostic nature of ClearPass allows Aruba to secure heterogeneous environments. Features like Colorless Ports and VSX hitless upgrades provide a level of agility and uptime that differentiates Aruba from traditional, monolithic networking vendors.

9. Identify, describe, and differentiate the functions and features of Aruba products and solutions Practice Question

Q1: Which Aruba switch feature allows two switches to operate in an active-active high availability mode, typically used at the core layer?
A. VSX
B. Link Aggregation
C. ACL
D. VSF

Q2: Which ArubaOS-CX capability allows administrators to query historical data such as link flaps or CPU usage?
A. Python scripting
B. State database
C. NetEdit
D. ZTP

Q3: Which Aruba switch series supports VSX and is optimized for core or data center deployments?
A. Aruba 2930M
B. Aruba CX 6300
C. Aruba 3810
D. Aruba CX 8400

Q4: Which Aruba management solution is cloud-native and includes AI-powered insights, firmware management, and network-wide visibility?
A. NetEdit
B. Aruba Central
C. AirWave
D. ClearPass

Q5: Which Aruba feature allows real-time and historical analytics directly on the switch without external tools?
A. IGMP Snooping
B. AirWave
C. ZTP
D. Network Analytics Processor (NAP)

Q6: Which Aruba security feature automatically enforces port-based access control using RADIUS authentication?
A. Port security
B. 802.1X
C. DHCP Snooping
D. IGMP Snooping

Q7: What is a primary benefit of Aruba's "colorless ports" capability?
A. Each port supports up to four VLANs simultaneously
B. Ports automatically assign access policies based on the connected device
C. Only Aruba APs can connect to these ports
D. They require no physical cabling

Q8: What is the purpose of Aruba's Dynamic Segmentation?
A. To assign QoS tags to outgoing packets
B. To prevent DHCP spoofing
C. To automatically assign VLANs and policies based on user identity
D. To aggregate switch ports for higher bandwidth

Q9: Which Aruba switch model is best suited for small office networks with only basic Layer 2 functionality?
A. Aruba 2530
B. Aruba CX 6200
C. Aruba 3810
D. Aruba 2930M

Q10: What is the main function of Aruba NetEdit?
A. Secure Wi-Fi user onboarding
B. AI-driven troubleshooting and reporting
C. Multi-device configuration editing and validation
D. Dynamic VLAN assignment

HPE6-A72 Install, configure, set up, and validate Aruba solutions

1. Initial Setup and Access

Initial deployment requires secure console access, typically via a serial connection (9600 baud, 8-N-1). Administrators should configure the hostname, management IP, and default gateway immediately. Out-of-band (OOB) management ports provide a separate control path, while in-band management occurs via a designated

VLAN. SSH must be enabled, and Telnet disabled, to ensure encrypted administrative sessions. The command `crypto key generate ssh` is required on many models to initialize secure access.

2. VLAN and Interface Configuration

Layer 2 segmentation begins with VLAN creation and port assignment. Interfaces are defined as `untagged` for end-user devices or `tagged` for trunk links. For high-bandwidth uplinks, Link Aggregation Groups (LAGs) are configured with LACP using the `mode active` command. These configurations ensure a stable Layer 2 fabric before routing is implemented.

3. Routing Configuration

On ArubaOS-CX, inter-VLAN routing requires the `ip routing` command. Architects must configure Switch Virtual Interfaces (SVIs) with IP addresses to act as gateways for each VLAN. Static routes are configured using `ip route 0.0.0.0/0 [next-hop]`. For OSPF, a Router ID must be defined, and interfaces must be assigned to Area 0 to facilitate dynamic neighbor discovery and adjacency.

4. DHCP Configuration

Aruba switches support three DHCP roles:

1. **DHCP Client**: The switch obtains its management IP via `ip address dhcp-bootp`.
2. **DHCP Relay**: The `ip helper-address` command forwards client broadcasts to a centralized server.
3. **DHCP Server**: This role is primarily supported on ArubaOS (legacy) platforms and is not available on all CX platforms; it is best reserved for isolated or small-scale subnets.

5. AAA and Access Control

Administrative and port-level security is enforced via the AAA framework. Local authentication defines `manager` and `operator` roles. For port-based access, 802.1X is configured to authenticate supplicants against a RADIUS server (ClearPass). Command sets include `aaa port-access authenticator` to initialize the 802.1X state machine on specific interfaces.

6. Monitoring and Validation

Post-install validation is performed using essential `show` commands. `show interface brief` confirms physical link status, `show vlan` verifies port memberships, and `show ip route` confirms the presence of the default gateway and learned routes. `ping` and `traceroute` are used to verify end-to-end reachability across the fabric.

7. Firmware and File Management

Firmware is managed via dual-image slots (primary and secondary). New images are uploaded to the inactive slot to allow for rollback if a failure occurs. Configuration files are saved using `write memory` or `copy`

`running-config startup-config`. ZTP can be utilized for large-scale deployments to automate the download of these files upon first boot.

8. Best Practices for Setup and Validation

Professional deployments prioritize structured naming (e.g., SW-ACC-FL1), unique management IPs, and the use of secure protocols. All configurations should be validated in a staging environment. Before production go-live, architects must verify STP Root Bridge placement and ensure that ACLs are not inadvertently blocking critical management traffic.

9. Install, configure, set up, and validate Aruba solutions Practice Question

Q1: Which command is used on ArubaOS-CX to activate routing functionality between VLANs?
A. `ip routing`
B. `enable vlan-routing`
C. `routing enable`
D. `enable inter-vlan`

Q2: When setting up an Aruba switch for the first time, which access method is typically used if the switch has no IP address assigned?
A. Telnet over VLAN 1
B. Console port with a terminal emulator
C. HTTPS via management port
D. Aruba Central onboarding

Q3: Which command configures a switch to act as a DHCP relay for VLAN 10?
A. `ip dhcp-relay 10.1.1.1` on VLAN 10
B. `ip helper-address 10.1.1.1` on interface VLAN 1
C. `interface vlan 10` then `ip helper-address 10.1.1.1`
D. `dhcp forward 10.1.1.1` under VLAN 10

Q4: Which show command provides a summary of all VLANs and their assigned interfaces?
A. `show interface brief`
B. `show lag`
C. `show spanning-tree`
D. `show vlan`

Q5: A network administrator wants to tag VLANs 10, 20, and 30 on a trunk port using ArubaOS-CX. What is the correct command syntax?
A. `vlan-tag 10,20,30`
B. `vlan add 10,20,30 trunk`
C. `vlan 10,20,30 tagged 1/1/48`
D. `switchport trunk vlan 10,20,30`

Q6: Which of the following is required to enable secure remote access to an Aruba switch?
A. Enable HTTP
B. Enable Telnet and SSH
C. Generate SSH keys and enable SSH
D. Configure SNMPv3

Q7: What is the function of the command `show ip route`?
A. Show the routing table and next-hop info
B. Show the ARP cache
C. Display SNMP traps
D. Display physical port states

Q8: During ZTP, which service typically provides the switch with its configuration file?
A. SNMP manager
B. Telnet client
C. NTP server
D. FTP or TFTP server

Q9: Which of the following best describes a use case for port security?
A. Prevent unauthorized devices from connecting to access ports
B. Enable multicast forwarding
C. Limit spanning-tree changes
D. Dynamically route between VLANs

Q10: What is the correct command to configure the switch's hostname to "Branch-Access-01"?
A. `set hostname Branch-Access-01`
B. `hostname Branch-Access-01`
C. `device-name Branch-Access-01`
D. `name Branch-Access-01`

HPE6-A72 Manage, monitor, administer and operate Aruba solutions

1. User and Role Management

Administrative accountability is maintained through role-based access. Local accounts should be assigned either the `manager` role for full configuration or the `operator` role for read-only status. All management must be conducted over SSH or HTTPS. Auditors should use the `show users` command to monitor active administrative sessions.

2. Remote Management and Automation Tools

Operations scale through centralized platforms. Aruba Central provides cloud-based monitoring and AI-driven troubleshooting. Aruba NetEdit allows for multi-device configuration validation and bulk changes on CX hardware. REST APIs enable external scripts to poll the switch state or push changes programmatically.

3. Configuration and File Management

Config lifecycle management involves maintaining the `running-config` and `startup-config`. ArubaOS-CX introduces `checkpoints`, which are snapshots of the system state. Administrators use the `checkpoint` command to create restore points before major changes, allowing for rapid comparison and rollback if instability occurs.

4. Monitoring and Health Checking

Proactive health monitoring uses `show system resource-utilization` to track CPU, memory, and buffer usage. Interface health is monitored for CRC errors and drops. SNMPv3 should be configured for secure polling by NMS platforms, while syslog forwards events to a centralized SIEM for long-term correlation.

5. Time and Event Synchronization

Accurate timekeeping via NTP is mandatory for log sequencing and security certificate validity. Multiple redundant NTP sources should be configured. ArubaOS-CX `event-handlers` can be programmed to trigger automated responses, such as sending a syslog alert or an SNMP trap when a critical interface changes state.

6. Port and Access Management

Daily tasks include port status control and authentication monitoring. The `show port-access clients` command provides visibility into currently authenticated 802.1X and MAC-auth devices. Administrators must regularly shut down unused ports to reduce the attack surface.

7. Software and Image Operations

Firmware management utilizes the primary/secondary slot system. Upgrades are staged in the inactive slot and verified via `show version` before the switch is reloaded. This dual-image approach ensures that the last-known-good software is always available for immediate recovery.

8. Daily Admin Best Practices

Operational excellence is defined by weekly configuration backups, daily log reviews, and the enforcement of change control. Upgrades must be restricted to maintenance windows. Consistent use of interface descriptions and structured naming ensures the network remains transparent and manageable for the entire engineering team.

9. Manage, monitor, administer and operate Aruba solutions Practice Question

Q1: An administrator needs to boot an Aruba switch using the firmware stored in the secondary image slot. Which command should be used?
A. reload firmware
B. boot system flash secondary
C. show image
D. copy tftp flash

Q2: Which command provides real-time statistics on CPU and memory usage in ArubaOS-CX?
A. show logging
B. show vlan
C. show system resource-utilization
D. show ip route

Q3: A network engineer needs to make batch configuration changes across multiple ArubaOS-CX switches and validate them before deployment. Which tool should be used?
A. REST API Explorer
B. Aruba NetEdit
C. Aruba Central
D. AirWave

Q4: What is the correct syntax to label an interface with a description for documentation purposes?
A. interface 1/1/10 description "Connected to Core"
B. name 1/1/10 "To Core"
C. interface 1/1/10 name "Finance Link"
D. description set "Core Uplink"

Q5: What is the benefit of creating a configuration checkpoint in ArubaOS-CX?
A. Enables rollback to a known good state
B. Automates VLAN tagging
C. Verifies SNMP traps
D. Clears unused VLANs

Q6: What is the correct command to back up the startup configuration file to a TFTP server?
A. tftp upload config startup 192.168.1.10
B. copy running-config usb backup.cfg
C. copy startup-config tftp 192.168.1.10 backup.cfg
D. backup running-config tftp 192.168.1.10

Q7: Which command disables insecure protocols on Aruba switches to harden management access?
A. no vlan access
B. no telnet
C. secure-mode enable
D. disable password-recovery

Q8: Which tool provides cloud-based management, topology mapping, and AI-powered insights for Aruba infrastructure?
A. Aruba Central
B. SNMP Manager
C. AirWave
D. NetEdit

Q9: What is a recommended best practice for user access on Aruba switches?
A. Create individual user accounts with appropriate roles
B. Use a shared admin account for convenience
C. Enable Telnet for all admin access
D. Disable all user authentication

Q10: What is the best practice for time synchronization on Aruba switches in secure enterprise networks?
A. Configure LLDP-MED time distribution
B. Use DHCP Option 82
C. Set a local firewall or domain controller as the NTP source
D. Enable SNTP via public internet

HPE6-A72 Troubleshoot, repair, and replace Aruba solutions

1. Troubleshooting Methodology

A logical, layered approach is required for rapid resolution:

1. **Identify**: Observe symptoms and alerts.
2. **Define Scope**: Determine if the issue is isolated or widespread.
3. **Gather Info**: Utilize CLI commands, packet captures, and logs.
4. **Hypothesize**: Formulate root causes.
5. **Implement/Test**: Apply a fix and validate results.
6. **Document**: Record the resolution in the knowledge base.

2. Common Network Issues and Fixes

Common failures occur at Layers 1-3. Interface flaps often require cable or transceiver replacement. VLAN mismatches or tagging errors on trunks break L2 connectivity. Routing failures are typically caused by missing SVIs or incorrect default gateways. LAG failures often result from LACP mode mismatches (Active vs. Passive) or mismatched hashing algorithms.

3. Monitoring Tools and Commands

Diagnostic commands provide real-time status. `show spanning-tree` identifies blocked ports; `show lacp` verifies aggregated link health. ArubaOS-CX supports `monitor capture`, allowing engineers to export PCAP

files for Wireshark analysis. Historical patterns are reviewed via the CX state database to identify intermittent issues.

4. Log Analysis

Syslog analysis isolates root causes. Log levels range from `debug` (verbose) to `critical` (emergencies). Engineers should filter logs using `show logging | include [keyword]` to find link changes or authentication failures. Remote syslog ensures that event data survives a switch reboot.

5. Recovery and Repair Operations

Service restoration involves password recovery via the boot menu or factory resets using the `erase startup-config` command. If a configuration is corrupted, it is restored from a TFTP/SFTP backup. Firmware rollbacks are executed by booting from the secondary flash partition using `boot system flash secondary`.

6. Hardware Replacement

Failed modular components, such as power supplies or fans, can be hot-swapped on supported chassis. When a full switch RMA occurs, ZTP can be used to automatically configure the replacement unit by matching its MAC address to a pre-staged template in Aruba Central or a local ZTP server.

7. Best Practices for Troubleshooting

Effective troubleshooting begins at Layer 1. Engineers must verify physical connectivity before analyzing complex routing protocols. Baseline configurations should be maintained for comparison. Only one change should be implemented at a time to ensure the root cause is accurately identified without compounding the issue.

8. Troubleshoot, repair, and replace Aruba solutions Practice Question

Q1: A network technician observes that a switch port is up but users report no connectivity. Which command should be used first to assess port-level issues?
A. show interfaces
B. show vlan
C. show ip route
D. show logging

Q2: A user connected to VLAN 20 cannot access the DHCP server in VLAN 100. Which of the following is most likely misconfigured?
A. Spanning tree priority
B. IP helper address on VLAN 20
C. ACL direction
D. DHCP lease time

Q3: What command enables real-time monitoring of CPU and memory usage on an ArubaOS-CX switch?
A. show spanning-tree
B. show logging
C. show system resource-utilization
D. show access-list

Q4: Which issue would most likely be caused by a mismatch in native VLAN configuration on a trunk link?
A. Interface CRC errors
B. DHCP IP conflicts
C. STP root bridge flapping
D. Intermittent connectivity between switches

Q5: A switch is unable to communicate with Aruba Central after a firmware upgrade. What is the best command to verify whether the upgrade was successful?
A. show version
B. show lag
C. show vlan
D. show boot-history

Q6: After configuring an ACL to block HTTP traffic from guest VLAN to internal servers, users still access the servers. What is the likely issue?
A. STP is blocking the port
B. Incorrect SNMP trap configuration
C. ACL was applied outbound on SVI
D. Route to the VLAN is missing

Q7: What feature allows an Aruba switch to automatically retrieve configuration and firmware when booted for the first time?
A. LLDP auto-detect
B. Zero Touch Provisioning (ZTP)
C. SNMPv3 integration
D. Dynamic segmentation

Q8: You replaced a failed Aruba CX 6300 switch in a stack with a new unit. What step ensures full synchronization with the rest of the stack?
A. Configure IP routing
B. Enable DHCP snooping
C. Enable LLDP
D. Assign the correct VSF member ID and priority

Q9: What is the function of the `monitor capture` command on ArubaOS-CX?
A. Collects interface packet captures for export
B. Enables SNMP traps
C. Captures CLI configuration changes
D. Enables switch memory diagnostics

Q10: An engineer needs to reset an Aruba switch that is completely misconfigured and unreachable. Which command should they use from the console?
A. clear boot-image
B. enable vlan reset
C. reload boot-system
D. erase startup-config

HPE6-A72 Tune, optimize, and upgrade Aruba solutions

1. Performance Optimization

Optimization maximizes existing resource efficiency. QoS prioritizes time-sensitive traffic (e.g., DSCP 46 for VoIP) using strict priority queuing. Storm control limits broadcast/multicast traffic to a percentage of link bandwidth (e.g., `storm-control broadcast level 5`). Jumbo frames (up to 9000 bytes) are enabled to improve throughput for storage and data center backbones.

2. High Availability and Redundancy

Resilience is built through redundant links and control planes. LACP bundles links for bandwidth and failover. RSTP ensures fast convergence (<2 seconds) with prioritized root bridge placement. VSF provides a Single Management Plane for access stacks, while VSX provides Active-Active core redundancy with hitless upgrades.

3. Software and Firmware Upgrade Procedures

Maintaining current software is a strategic necessity. Upgrades are staged via the inactive firmware slot. Validation includes checking version numbers and routing neighbor status. Using Aruba Central or NetEdit allows for scheduled, automated upgrades across the entire enterprise with minimal manual oversight.

4. Configuration Optimization

Refining configurations involves removing orphaned VLANs, unused ACL rules, and disabling insecure protocols (Telnet/HTTP). Shutting down unused ports prevents unauthorized access. Standardized templates ensure consistency, making the environment more predictable and easier to monitor.

5. Monitoring and Analytics

Data-driven tuning leverages the Network Analytics Processor (NAP) on CX switches to identify "top talkers" and congestion points. Aruba Central AI Insights provides automated root-cause analysis for anomalies. Threshold alerts should be set for CPU and memory usage to proactively address bottlenecks.

6. Time Synchronization

Precise timekeeping is the foundation of log correlation and secure authentication. Redundant NTP sources must be configured to prevent clock drift. Proper time synchronization ensures that NAE scripts and Central analytics accurately sequence events across the distributed fabric.

7. Logging and Debugging

Visibility is optimized by tuning syslog and SNMP. Secure SNMPv3 should be implemented for encrypted polling. Log levels must be balanced to provide sufficient detail without overwhelming system resources. These diagnostic logs are essential for auditing and performance tuning.

8. Upgrading Best Practices

Lifecycle management concludes with structured upgrade habits. All changes should be validated in a lab environment before production. Comprehensive backups and maintenance windows are mandatory. Post-upgrade, engineers must monitor the switch for anomalies in LAG status and OSPF adjacencies. Adherence to these protocols ensures a high-performance, automated, and secure Aruba networking environment.

9. Tune, optimize, and upgrade Aruba solutions Practice Question

Q1: Which command limits the broadcast traffic to 5% on an Aruba switch port?
A. `traffic-filter broadcast 5`
B. `qos dscp 46 local-priority 6`
C. `limit-broadcast 5 percent`
D. `storm-control broadcast level 5`

Q2: What is the primary benefit of using Jumbo Frames in a high-throughput network?
A. Prevents STP convergence
B. Increases data transfer efficiency for large payloads
C. Enhances wireless roaming
D. Reduces VLAN tag overhead

Q3: What protocol is used in a Link Aggregation Group to dynamically negotiate bundled links?
A. RIP
B. LACP
C. OSPF
D. STP

Q4: Which Aruba solution allows two core switches to operate in active-active mode with synchronized configurations?
A. VSX
B. VSF
C. LACP
D. RSTP

Q5: What is the correct command to synchronize time with an NTP server on an Aruba switch?
A. `ntp sync server <IP>`
B. `ntp server <IP>`
C. `set time ntp <IP>`
D. `sync time-server <IP>`

Q6: Which Aruba command disables an unused interface to improve security?
A. `shutdown`
B. `no enable`
C. `interface disable`
D. `disable port`

Q7: What tool does Aruba recommend for automating upgrades and validations across multiple ArubaOS-CX switches?
A. ClearPass
B. SolarWinds
C. NetEdit
D. AirWave

Q8: What does the `qos trust dscp` command do?
A. Converts DSCP values to VLAN tags
B. Assigns lowest priority to all traffic
C. Honors DSCP markings from upstream devices
D. Overrides DSCP with local policy

Q9: Which log level captures only critical errors on an Aruba switch?
A. warning
B. debug
C. critical
D. info

Q10: What is the function of Aruba Central AI Insights?
A. Automates port shut/no shut sequences
B. Provides anomaly detection and root cause analysis
C. Hosts DHCP relay policies
D. Monitors user credentials

Learning Path & Study Advice

Preparation should begin with strengthening networking fundamentals, including TCP/IP models, Ethernet operations, and IP addressing concepts. Building a clear conceptual understanding of how switches forward traffic and segment networks is critical before progressing to configuration tasks.

Candidates should reinforce theoretical knowledge with hands-on practice in lab or simulated environments. Emphasis should be placed on understanding why specific configurations are applied and how they affect traffic behavior and network stability. Structured troubleshooting practice, including identifying root causes and verifying solutions, will help develop practical competence aligned with real-world operational responsibilities.

Who This PDF Is For

This document is intended for entry-level network professionals, technical support engineers, and IT staff responsible for basic network configuration and maintenance tasks. It is suitable for individuals with foundational knowledge of networking concepts who are seeking to formalize and validate their skills in enterprise switching environments. Those preparing to advance toward more specialized networking roles will benefit from using this overview as a structured reference for foundational switching knowledge.

Call To Action

This document provides an overview of structured learning and certification preparation approaches. For learners seeking clear knowledge organization, guided study planning, and exam-focused practice resources, AAAdemy offers a comprehensive platform to support independent and effective learning.

Explore additional training materials, study guidance, and practice resources at:

https://www.aaademy.com/Aruba-Certified-Switching-Associate-ACSA-V1/HPE6-A72.html

Online Flashcards (Quizlet):

https://quizlet.com/user/AAAdemy/folders/hpe6-a72-aruba-certified-switching-associate-exam-flashcards?i=6zfa5t&x=1xqt

Attachment: Answers by Knowledge Point

Identify, describe, and apply foundational networking architectures and technologies Practice Question
A1: Answer: D
Explanation: The Network layer (Layer 3) handles logical addressing (IP) and determines the best path for data across networks. Routers operate at this layer.

A2: Answer: A
Explanation: STP prevents Layer 2 loops by selectively blocking redundant paths, ensuring a loop-free topology.

A3: Answer: C
Explanation: Tagged ports are used in trunk links and allow traffic from multiple VLANs to pass over a single link.

A4: Answer: C
Explanation: The default gateway is typically the first usable IP in the subnet, which is 192.168.10.1 for this address and subnet mask.

A5: Answer: A
Explanation: The MAC address table maps MAC addresses to specific switch ports, allowing the switch to forward frames only to the correct port.

A6: Answer: D
Explanation: LACP (Link Aggregation Control Protocol) is part of IEEE 802.3ad and allows switches to automatically create and manage aggregated links.

A7: Answer: B
Explanation: The Transport layer (Layer 4) uses TCP and UDP port numbers to deliver data to the correct application or service.

A8: Answer: A
Explanation: The command `show ip route` displays the device's current IP routing table, which includes all known routes.

A9: Answer: A
Explanation: /24 means 24 bits are used for the network portion, which corresponds to a subnet mask of 255.255.255.0.

A10: Answer: B
Explanation: The range 239.0.0.0 to 239.255.255.255 is reserved for local or private multicast scopes used within an organization.

Identify, describe, and differentiate the functions and features of Aruba products and solutions Practice Question
A1: Answer: A
Explanation: VSX (Virtual Switching Extension) enables two Aruba CX core switches to work in an active-active fashion, allowing hitless upgrades and enhanced resilience. It is designed for core or data center use.

A2: Answer: B
Explanation: ArubaOS-CX uses a state database architecture that enables the collection of both real-time and historical telemetry, helping in root cause analysis and trend tracking.

A3: Answer: D
Explanation: Aruba CX 8400 is a modular, high-end switch designed for core and data center networks. It supports VSX for high availability.

A4: Answer: B
Explanation: Aruba Central is a cloud-native management platform that offers unified visibility, AI-based troubleshooting, ZTP, and firmware control across the network.

A5: Answer: D
Explanation: NAP is an onboard analytics engine in ArubaOS-CX switches that collects and stores detailed operational data for analysis, without requiring additional software.

A6: Answer: B
Explanation: 802.1X is a standard for port-based access control that uses RADIUS servers like ClearPass to authenticate users or devices before granting network access.

A7: Answer: B
Explanation: Colorless ports dynamically apply VLAN, ACL, and QoS settings based on the identity or role of the connected device, enabling policy mobility across the network.

A8: Answer: C
Explanation: Dynamic Segmentation integrates with ClearPass to assign VLANs, ACLs, and QoS policies dynamically, based on user/device identity and role, enhancing access control and mobility.

A9: Answer: A
Explanation: Aruba 2530 is a basic Layer 2 switch using legacy ArubaOS. It is budget-friendly and ideal for simple, small-office environments.

A10: Answer: C
Explanation: Aruba NetEdit is an on-premises tool used for centralized configuration management, multi-switch editing, validation, and compliance tracking within ArubaOS-CX environments.

Install, configure, set up, and validate Aruba solutions Practice Question
A1: Answer: A
Explanation: The correct command on ArubaOS-CX to activate Layer 3 routing between VLANs is `ip routing`. It enables the switch to route between SVIs (Switch Virtual Interfaces).

A2: Answer: B
Explanation: Console access via a terminal emulator (e.g., PuTTY) is the default method used for first-time setup when no IP address has been assigned yet.

A3: Answer: C
Explanation: DHCP relay must be configured under the interface of the client VLAN (e.g., VLAN 10) using `ip helper-address <DHCP server IP>`.

A4: Answer: D
Explanation: `show vlan` provides a clear overview of all VLANs configured on the switch and the ports associated with each VLAN.

A5: Answer: C
Explanation: The correct syntax to tag VLANs on ArubaOS-CX is `vlan 10,20,30 tagged <interface>`, which configures the specified port as a trunk.

A6: Answer: C
Explanation: Secure access is enabled by generating SSH keys and turning on the SSH service. Telnet is insecure and should be disabled.

A7: Answer: A
Explanation: The `show ip route` command is used to verify both static and dynamic routing entries and confirm next-hop reachability.

A8: Answer: D
Explanation: In Zero Touch Provisioning, switches use TFTP, FTP, or HTTP/HTTPS to download initial configuration or firmware as instructed by DHCP options.

A9: Answer: A
Explanation: Port security is used to restrict network access to specific MAC addresses on a port, helping prevent unauthorized device connections.

A10: Answer: B
Explanation: The command `hostname Branch-Access-01` is used to set the hostname on Aruba switches. It is valid on both ArubaOS and ArubaOS-CX.

Tune, optimize, and upgrade Aruba solutions Practice Question
A1: Answer: D
Explanation: The correct command to limit broadcast traffic on an Aruba switch port is `storm-control broadcast level 5`, which sets the threshold to 5% of the port's bandwidth.

A2: Answer: B
Explanation: Jumbo frames allow the transmission of larger Ethernet frames (up to ~9000 bytes), which is more efficient for large data transfers, such as backups or storage replication.

A3: Answer: B
Explanation: LACP (Link Aggregation Control Protocol) is used to dynamically manage and negotiate link aggregation, ensuring both sides agree on port bundling.

A4: Answer: A
Explanation: VSX (Virtual Switching Extension) allows two Aruba core switches to run as active-active peers with high availability and state synchronization.

A5: Answer: B
Explanation: The `ntp server <IP>` command is used to configure an Aruba switch to synchronize time using Network Time Protocol (NTP).

A6: Answer: A
Explanation: The `shutdown` command disables an interface on Aruba switches, which is a best practice for security on unused ports.

A7: Answer: C
Explanation: NetEdit is Aruba's automation and validation tool for managing ArubaOS-CX switches, supporting upgrades, audits, and rollbacks.

A8: Answer: C
Explanation: `qos trust dscp` instructs the switch to honor existing DSCP markings received from upstream devices, enabling effective QoS handling.

A9: Answer: C
Explanation: The `critical` logging level records only severe errors or system failures, minimizing log volume while capturing essential faults.

A10: Answer: B
Explanation: Aruba Central AI Insights provides intelligent monitoring by detecting anomalies, analyzing trends, and suggesting root causes for network issues.

Troubleshoot, repair, and replace Aruba solutions Practice Question
A1: Answer: A
Explanation: The `show interfaces` command provides critical details like port status, errors, speed/duplex mismatches, and traffic counters, making it the first choice for diagnosing physical and link-layer issues.

A2: Answer: B
Explanation: Inter-VLAN DHCP requires a helper address on the interface of the client VLAN. Without `ip helper-address`, DHCP broadcast requests won't reach the remote server.

A3: Answer: C
Explanation: The `show system resource-utilization` command provides real-time performance metrics like CPU and memory usage, crucial for diagnosing system stress or overload.

A4: Answer: D
Explanation: Native VLAN mismatches lead to untagged traffic being misinterpreted on trunk links, causing intermittent or failed communication between devices in that VLAN.

A5: Answer: A
Explanation: `show version` confirms the current active firmware image and ensures the switch is running the intended OS version after an upgrade.

A6: Answer: C
Explanation: If the ACL is applied outbound and the traffic never exits the interface (e.g., stays within the VLAN), it may not be matched. ACLs should often be applied inbound on routed interfaces.

A7: Answer: B
Explanation: ZTP automates switch provisioning by using DHCP to fetch configuration and firmware from a predefined server, simplifying deployment.

A8: Answer: D
Explanation: In a VSF stack, new members must be manually assigned the correct VSF member ID and priority to match the logical stack configuration and participate correctly.

A9: Answer: A
Explanation: The `monitor capture` feature captures real packet traffic on a selected interface, which can be exported and analyzed using tools like Wireshark.

A10: Answer: D
Explanation: `erase startup-config` deletes the saved configuration. After rebooting, the switch loads with factory default settings, ideal for full recovery.

Manage, monitor, administer and operate Aruba solutions Practice Question
A1: Answer: B
Explanation: The command `boot system flash secondary` instructs the switch to load the secondary image on the next reboot, useful for rollback or testing alternate firmware.

A2: Answer: C
Explanation: The `show system resource-utilization` command displays key metrics like CPU usage, memory consumption, and buffer usage — essential for monitoring performance.

A3: Answer: B
Explanation: Aruba NetEdit provides centralized configuration management for CX switches, including batch edits, pre-deployment validation, and compliance enforcement.

A4: Answer: A
Explanation: In ArubaOS-CX, the `description` command is used under the interface context to add human-readable notes, improving manageability and clarity.

A5: Answer: A
Explanation: Checkpoints allow admins to save the current configuration state, which can later be restored (rolled back) if needed, ensuring safer changes in production.

A6: Answer: C
Explanation: The `copy startup-config tftp` command sends the saved configuration file to an external server, helping preserve configuration integrity across reboots or upgrades.

A7: Answer: B
Explanation: `no telnet` disables Telnet, which transmits credentials in plaintext. Disabling this and other insecure protocols strengthens the device's security posture.

A8: Answer: A
Explanation: Aruba Central is a cloud-native management platform offering switch/AP visibility, topology views, configuration push, and AI insights for troubleshooting.

A9: Answer: A
Explanation: Each admin should have a unique user account with role-based access to ensure accountability, ease of auditing, and better security controls.

A10: Answer: C
Explanation: Enterprise environments should avoid reliance on public NTP. Instead, configure Aruba switches to sync with trusted internal sources like firewalls or domain controllers.