HPE6-A73 Training Course

Aruba Certified Switching Professional Exam

Structured Learning & Certification Preparation

Table of Contents

Introduction

The HPE6-A73 Aruba Certified Switching Professional certification represents advanced-level knowledge in enterprise switching technologies within modern network infrastructures. It validates a candidate’s ability to design, implement, optimize, and troubleshoot switching solutions that support reliable, scalable, and secure connectivity across campus and branch environments. In today’s IT landscape, where network performance and resilience are essential for digital operations, this certification is relevant for professionals responsible for maintaining efficient data communication within organizational networks.

About This Training / Certification

This certification assesses competencies related to professional-level switching deployment and management in enterprise environments. Candidates are expected to demonstrate practical understanding of Layer 2 and Layer 3 switching concepts, VLAN implementation, routing integration, redundancy protocols, quality of service, network segmentation, security policies, and high-availability design. Positioned at an advanced stage in the networking learning journey, it typically builds on foundational networking knowledge and intermediate switching experience. It supports progression toward specialized expertise in enterprise infrastructure architecture, operational troubleshooting, and performance optimization.

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

Area 1: Plan the Wired Network Solution
This area focuses on the ability to interpret business and technical requirements and translate them into a structured wired network design. Candidates are expected to understand how to evaluate existing environments, define scalability and resiliency needs, align switching architecture with operational goals, and make sound design decisions around topology, segmentation, redundancy, and service readiness. Conceptually, this area is not only about selecting features, but also about understanding why a particular design approach supports performance, manageability, and long-term maintainability.

Area 2: Install and Configure the Wired Network Solution
This area covers the implementation of a planned wired infrastructure in a controlled and technically consistent way. Candidates should understand how switching solutions are deployed, how baseline configurations are established, and how core services and features are enabled to support secure and reliable network operation. The emphasis is on knowing how configuration elements work together, including VLANs, trunking, Layer 2 and Layer 3 behavior, access policies, resiliency mechanisms, and device roles within the broader network design. A strong conceptual foundation in this area helps ensure that deployment choices are accurate, interoperable, and aligned with the intended architecture.

Area 3: Troubleshoot the Wired Network Solution
This area emphasizes structured problem analysis within enterprise wired environments. Candidates are expected to understand how to isolate faults, validate assumptions, interpret device and network behavior, and determine the most likely causes of service disruption or degraded performance. This includes reasoning across multiple layers of the network, recognizing issues related to configuration consistency, forwarding behavior, segmentation, redundancy, routing interaction, and policy enforcement. The deeper objective is not memorizing isolated fixes, but developing the judgment required to move from symptoms to root cause in a methodical and technically defensible way.

Area 4: Manage, Maintain, Optimize, and Monitor the Wired Network Solution
This area addresses the ongoing operational lifecycle of a wired network after deployment. Candidates should understand how to sustain network health through monitoring, maintenance planning, performance analysis, change control, and continuous optimization. This includes interpreting operational data, identifying trends, improving efficiency, preserving service stability, and maintaining alignment between business requirements and network behavior over time. Conceptually, this area reflects the transition from implementation to operational excellence, where reliability, visibility, and incremental improvement become central responsibilities.

Detailed Knowledge Explanation

HPE6-A73 Plan the Wired Network Solution

The strategic necessity of a robust planning phase cannot be overstated; it serves as the foundational blueprint for organizational scalability and long-term risk mitigation. A thorough pre-implementation analysis allows architects to transform abstract business objectives into a tangible technical roadmap, ensuring that the infrastructure remains resilient under evolving traffic demands. By evaluating environmental constraints and technical dependencies early, the organization avoids the high costs associated with mid-cycle hardware refreshes and security retrofitting. This phase effectively balances performance requirements with budgetary limits, providing a stable platform for high-availability services. A meticulous transition from high-level planning to granular execution begins with a comprehensive needs analysis.

1. Needs Analysis and Evaluation

A successful deployment relies on a synthesized evaluation of user, business, and technical data. Architects must reconcile the relationship between diverse user categories and the subsequent allocation of network resources. Guest users, for instance, are typically sequestered with limited bandwidth to preserve resources for internal operations, while High-Priority users—such as executives or IT staff—require enhanced access speeds and dedicated resource reservation. Failure to accurately translate these user-specific profiles into technical requirements for bandwidth and redundancy often results in severe bottlenecks at the Aggregation layer, where traffic converges. This technical translation is critical for business continuity, as it ensures mission-critical flows, such as ERP data and VoIP, are protected by low-latency pathways and fault-tolerant architectures comprising link aggregation and dual-core redundancy.

1.1 User Requirements

Synthesizing data regarding user types—Guests, Employees, and High-Priority users—is the first step in calculating network capacity. Architects must estimate user volume and application profiles (e.g., standard web browsing versus high-definition video conferencing) to determine the necessary throughput at the Access and Aggregation layers. An accurate user requirement profile ensures the physical infrastructure is sized correctly to prevent saturation during peak operational hours.

1.2 Business Requirements

The operational success of an organization is often tied to the performance of mission-critical applications like VoIP and video conferencing. These applications are highly sensitive to latency and jitter, requiring a network design that prioritizes reliability over raw throughput for specific flows. Evaluating the impact of application sensitivity allows architects to design a backbone that guarantees business-critical data delivery even during periods of high congestion.

1.3 Technical Requirements

Technical requirements involve the strategic analysis of data flow and fault tolerance across the three-tier hierarchy. Link aggregation is deployed to increase logical bandwidth while providing redundancy, and dual-core

devices ensure high availability at the network's most critical juncture. This technical framework establishes the necessary "skeleton" to support advanced security and traffic management policies.

2. Network Architecture Design

The strategic implementation of the three-layer model (Core, Aggregation, and Access) organizes data movement and security enforcement into a manageable hierarchy. This structure simplifies troubleshooting and allows for modular scaling without disrupting the existing environment.

2.1 Layered Model Design

The Core layer is designed for high-speed forwarding, minimizing complexity to maximize throughput. The Aggregation layer serves as the site for policy enforcement and traffic control, acting as the bridge between the high-speed backbone and the end-user environment. The Access layer provides the initial connection point, where basic security measures and port-level protections are first applied.

2.2 VLAN Planning

Role-based VLANs are essential for reducing broadcast traffic and improving security segmentation. By isolating departments—such as HR, IT, and Finance—into separate logical segments, architects minimize the "blast radius" of potential network issues and ensure that sensitive data is only accessible to authorized personnel.

2.3 IP Address Scheme

An organized IP address scheme is vital for future-proofing. Utilizing planned IP blocks and DHCP for automated assignment facilitates efficient management and avoids subnet overlaps. This structured approach simplifies the integration of new devices and facilitates the implementation of consistent Access Control Lists (ACLs).

3. Device Selection and Budgeting

Architects must reconcile port density and Power over Ethernet (PoE) requirements against long-term maintenance costs. Choosing the Aruba 2930F/2930M series for the access layer provides a balance of cost-efficiency and performance, while the Aruba CX series is preferred for high-performance core requirements. A critical strategic trade-off exists between fixed-port switches, which offer lower initial costs, and modular switches, which provide superior long-term scalability through the addition of line cards. Budgeting must account for equipment, professional installation, and redundancy hardware to ensure the network meets the five-nines availability standard.

4. Network Documentation

Topology diagrams and configuration records are indispensable for long-term maintenance and rapid troubleshooting. Documentation must include device names, IP allocations, VLAN mappings, and interface connections across all layers. This record-keeping provides the baseline for advanced traffic planning and ensures that subsequent engineers can manage the environment effectively.

5. Network Traffic and Bandwidth Planning

Effective bandwidth planning utilizes tools such as NetFlow, sFlow, and Wireshark to gain granular visibility into traffic patterns. To prevent bulk data transfers from impacting latency-sensitive traffic, architects must implement Quality of Service (QoS) mechanisms. This includes 802.1p for Layer 2 and DSCP for Layer 3, supported by scheduling mechanisms such as Weighted Fair Queuing (WFQ), Weighted Round Robin (WRR), and Strict Priority (SP) to ensure critical traffic is prioritized.

6. High Availability and Redundancy Design

High availability is achieved through switch-level redundancy (VRRP/HSRP) and link-level redundancy (MLAG or LACP). Furthermore, physical power redundancy—including dual power supplies and Uninterruptible Power Supplies (UPS)—is mandatory to prevent localized hardware failures from cascading into a network-wide outage.

7. Security Planning

The security framework must adopt a Zero Trust model, necessitating the use of 802.1X and Network Access Control (NAC). Port-level security is hardened through DHCP Snooping to block rogue servers, Dynamic ARP Inspection (DAI) to prevent spoofing, and port security violation modes (Restrict or Shutdown). Architects should implement "MAC Address Sticky Learning" to simplify the management of authorized devices while maintaining a strict security posture.

8. Network Scalability and Future Growth

Architects should consider the transition from traditional three-tier models to Spine-Leaf architectures in data centers to achieve lower latency. Additionally, an IPv6 transition strategy must be defined, utilizing Dual Stack, Tunneling, or **NAT64** for backward compatibility. These forward-looking measures ensure the infrastructure remains viable as the organization grows.

9. Plan the wired network solution Practice Question

Q1: When planning a wired network solution, which of the following is the most important factor to consider when designing VLANs for an enterprise environment?
A. Assigning a unique VLAN for each individual user
B. Ensuring VLANs are configured only at the access layer
C. Creating VLANs based on organizational roles and functions
D. Using VLANs only to separate guest traffic from internal traffic

Q2: Which of the following is NOT a key consideration when analyzing business requirements for a wired network solution?
A. Mission-critical applications
B. Number of employees in the organization
C. Bandwidth and latency requirements
D. Preferred hardware vendor for network devices

Q3: An organization requires high availability for its core network switches. Which of the following designs provides the BEST redundancy solution?
A. Implementing Spanning Tree Protocol (STP) on a single core switch

B. Using a single core switch with multiple power supplies
C. Deploying dual core switches with VRRP or HSRP
D. Configuring VLANs to only allow traffic through a single core switch

Q4: In a typical three-layer network architecture (Core, Aggregation, Access), what is the primary function of the core layer?
A. Enforcing security policies and VLAN segmentation
B. Providing high-speed forwarding and backbone connectivity
C. Managing and monitoring network devices
D. Assigning IP addresses to client devices

Q5: Which of the following is the best strategy for implementing IP address allocation in a large enterprise network?
A. Assigning static IP addresses to all client devices
B. Using DHCP for dynamic address assignment and reserving static addresses for critical infrastructure
C. Allocating a single large subnet to cover the entire network
D. Using overlapping IP subnets to maximize address space usage

Q6: When designing network security policies, which of the following strategies provides the MOST effective protection against unauthorized access?
A. Relying only on MAC address filtering
B. Implementing 802.1X authentication and role-based access control
C. Using static VLAN assignments without authentication
D. Disabling all unused switch ports without additional security measures

Q7: A network administrator is planning to implement Power over Ethernet (PoE) in a new office. Which of the following factors should be considered when selecting PoE switches?
A. The color of the network cables used
B. The maximum power budget available on the switch
C. The network topology (Spine-Leaf vs. Three-Layer)
D. The number of VLANs configured on the switch

HPE6-A73 Install and Configure the Wired Network Solution

The transition from design to physical execution requires precise installation and logical configuration to minimize future maintenance overhead. A correct initial setup ensures that security policies are enforceable and that the infrastructure functions as a synchronized, high-performance system.

1. Physical Device Installation

Physical installation begins with secure rack mounting and rigorous cable management. Architects must ensure optimal airflow to prevent overheating and maintain stability. It is critical to separate power and data cables to minimize electromagnetic interference (EMI). Finally, proper grounding and surge protection are mandatory to protect hardware from electrical anomalies.

2. Basic Configuration

Initialization involves setting unique hostnames, management IPs, and configuring the Network Time Protocol (NTP). Synchronized timing is essential for accurate audit logs and troubleshooting event correlation. Once the management baseline is established, VLANs are created and trunk ports are configured to enable inter-switch communication.

3. Security and Access Control Configuration

The first line of defense is established through ACLs and Port Security. Port security must be configured with specific violation modes: **Shutdown** (disabling the port) or **Restrict** (blocking unauthorized traffic while keeping the port active). These measures are managed via a AAA framework utilizing RADIUS for user authentication and TACACS+ for administrative access, ensuring all modifications are verified and audited.

4. Advanced Configuration

Efficiency is improved through QoS prioritization and Multicast management (IGMP Snooping and PIM). These protocols prevent bandwidth saturation by ensuring that high-priority applications—like VoIP—receive guaranteed bandwidth while limiting the propagation of unnecessary multicast data.

5. Device Initialization Optimization

Secure remote access must be prioritized by enabling SSH and disabling unencrypted protocols like Telnet. Furthermore, architects must configure centralized log management via a Syslog server to provide immediate visibility into system health and security events from the moment the device is brought online.

6. VLAN Configuration Optimization

Following 802.1Q standards ensures consistency across the enterprise. Optimization includes implementing dynamic VLAN assignment via 802.1X, which allows users to maintain their security policies and network access levels regardless of their physical connection point.

7. Link Aggregation Optimization

While static aggregation is possible, architects should mandate **LACP Active Mode** for all trunk links. Active Mode ensures dynamic negotiation between switches, allowing the system to automatically detect link failures or configuration mismatches, thereby providing a more resilient logical connection than passive or static modes.

8. Spanning Tree Protocol (STP) Optimization

The STP environment is hardened through the interplay of PortFast, BPDU Guard, and Root Guard. PortFast allows edge devices to transition to a forwarding state immediately; however, this creates a potential loop vulnerability if a switch is connected to that port. Enabling **BPDU Guard** on these edge ports mitigates this risk by shutting down the port if a BPDU is detected. Root Guard is applied to designated ports to prevent rogue devices from usurping the root bridge role, ensuring a stable and predictable topology.

9. Install and configure the wired network solution Practice Question

Q1: When installing a new rack-mounted switch, which of the following is the MOST important consideration to ensure proper operation?
A. The color of the Ethernet cables used
B. The brand of the rack being used
C. Ensuring proper airflow and cable management
D. Using fiber optic cables instead of copper cables

Q2: During the initial configuration of a managed switch, what is the purpose of assigning a management IP address?
A. To allow end users to access the internet
B. To enable remote administration and monitoring of the switch
C. To allow devices to communicate on different VLANs
D. To configure Quality of Service (QoS) settings

Q3: A network engineer wants to configure VLAN 20 on a switch and assign ports 5-10 to it. Which of the following commands should be used?
A. `vlan 20; name VLAN20; interface range gigabitethernet1/1/5-10; switchport access vlan 20`
B. `interface gigabitethernet1/1/5-10; vlan 20`
C. `interface vlan 20; switchport access vlan 20; exit`
D. `switchport mode trunk; vlan 20; exit`

Q4: What is the primary purpose of enabling Spanning Tree Protocol (STP) on a network switch?
A. To increase network bandwidth
B. To prevent switching loops in redundant network topologies
C. To prioritize traffic for VoIP applications
D. To assign static MAC addresses to switch ports

Q5: Which of the following BEST describes the function of Link Aggregation Control Protocol (LACP)?
A. It combines multiple physical links into a single logical link to increase bandwidth and redundancy
B. It ensures that only authorized users can access the switch
C. It assigns IP addresses to VLANs dynamically
D. It detects and blocks unauthorized devices on a network

Q6: A network administrator configures the following ACL on a switch:

access-list 101 deny tcp any any eq 23

access-list 101 permit ip any any

What effect will this ACL have?
A. It blocks all traffic on the network
B. It allows only Telnet traffic
C. It denies Telnet traffic but allows all other IP traffic
D. It blocks all TCP traffic

Q7: Which of the following security features prevents unauthorized devices from connecting to a switch port?
A. Quality of Service (QoS)
B. MAC Address Filtering (Port Security)
C. Link Aggregation Control Protocol (LACP)
D. Dynamic Host Configuration Protocol (DHCP) Snooping

Q8: A network engineer needs to implement AAA authentication for switch access. Which of the following protocols should be used?
A. DNS
B. RADIUS or TACACS+
C. SNMP
D. IGMP

Q9: A company uses VoIP phones for communication. Which of the following configurations should be applied to optimize network performance for these devices?
A. Disable Quality of Service (QoS)
B. Use VLANs and apply QoS policies to prioritize VoIP traffic
C. Configure STP to block VoIP traffic from crossing the network
D. Assign all VoIP traffic the lowest priority

HPE6-A73 Manage, Maintain, Optimize, and Monitor the Wired Network Solution

Network management is a continuous lifecycle where proactive monitoring prevents catastrophic failures. Proactive maintenance ensures that the network remains secure, efficient, and aligned with evolving organizational requirements.

1. Network Monitoring

Real-time visibility is achieved through Aruba AirWave and Aruba Central, supplemented by industry-standard tools like **PRTG, SolarWinds, and Wireshark**. These platforms provide a live view of traffic levels, device health,

and interface performance. Automated alerts for port failures or high-traffic thresholds allow administrators to intervene before user productivity is impacted.

2. Device Maintenance

Routine maintenance includes firmware version control and scheduled configuration backups. To minimize risk, architects should utilize hardware with **dual firmware storage**, which enables a rapid rollback to the previous version if a new update causes instability. Physical inspections of fans and power modules further protect against environmental failures.

3. Performance Optimization

Optimization involves refining QoS policies to match changing traffic patterns and utilizing load balancing across redundant links. VLAN optimization—including broadcast storm prevention and trunk pruning—reduces unnecessary traffic propagation, preserving bandwidth for critical applications.

4. Security Management

Security management requires the regular auditing of ACLs and AAA permissions. Routine vulnerability scanning and log auditing are essential for detecting anomalies, such as repeated login failures, which may indicate unauthorized access attempts. ARP protection (DAI) and DHCP Snooping should be audited frequently to ensure they continue to block rogue activity effectively.

5. Expanded Network Monitoring

SNMP is utilized for real-time status queries, while NetFlow and sFlow provide deep insights into traffic patterns. Analyzing these flows allows administrators to identify the root causes of congestion and detect unusual spikes that may indicate a security breach or a misconfigured application.

6. Increased Network Automation

The use of Aruba NetEdit, Ansible, and Python scripts reduces human error and ensures configuration compliance across the enterprise. Automation can be extended via the Aruba Central API to trigger automated fault responses, such as shutting down a compromised port or dynamically adjusting QoS during a congestion event.

7. Quality of Service (QoS) Optimization

Advanced QoS involves assigning DSCP **Expedited Forwarding (EF)** to VoIP packets to guarantee low-latency handling. Conversely, administrators should rate-limit low-priority traffic, such as P2P file sharing, to ensure that mission-critical business applications always have the required bandwidth.

8. VLAN and STP Optimization

In large-scale environments, Multiple Spanning Tree Protocol (MSTP) is implemented to reduce computation overhead by grouping VLANs into instances. Combined with VLAN trunk pruning, these optimizations streamline the topology and improve convergence times, ensuring high availability.

9. Manage, maintain, optimize, and monitor the wired network solution Practice Question

Q1: Which of the following tools can be used for real-time network monitoring in an Aruba-based environment?
A. SNMP
B. Aruba AirWave
C. Aruba Central
D. All of the above

Q2: A network administrator notices that a switch's CPU usage is consistently high. Which of the following is the MOST likely cause?
A. Excessive spanning tree recalculations
B. Low bandwidth utilization
C. Misconfigured VLANs
D. A disconnected trunk port

Q3: Which of the following statements about configuration backups is TRUE?
A. Backups should only be performed after major changes
B. Scheduled automatic backups help ensure quick recovery from failures
C. Configuration backups are not necessary if firmware updates are applied
D. Configuration files cannot be restored once a switch fails

Q4: A network administrator wants to enable Quality of Service (QoS) to prioritize VoIP traffic. Which of the following should be used?
A. DSCP markings
B. VLAN tagging
C. Port mirroring
D. Spanning Tree Protocol

Q5: A switch is experiencing high interface congestion. What is the BEST method to resolve this issue?
A. Enabling SNMP
B. Implementing load balancing
C. Configuring DHCP snooping
D. Increasing the STP priority

Q6: Which command is used to verify if QoS policies are applied to an interface?
A. `show policy-map interface`
B. `show spanning-tree`
C. `show ip route`
D. `show vlan`

Q7: An administrator wants to prevent unauthorized access to a switch by restricting management access to a specific IP subnet. What should be configured?

A. VLAN pruning
B. Access Control Lists (ACLs)
C. Port security
D. Link Aggregation Control Protocol (LACP)

Q8: A network administrator is reviewing system logs and notices multiple failed SSH login attempts. Which security measure should be implemented to mitigate this risk?
A. Enabling DHCP snooping
B. Implementing AAA with TACACS+ or RADIUS
C. Configuring port mirroring
D. Using VLAN tagging

Q9: A network administrator wants to optimize VLAN configurations to prevent broadcast storms. Which of the following methods should be used?
A. Enabling BPDU Guard
B. Configuring VLAN pruning
C. Disabling STP
D. Increasing the switch MTU

HPE6-A73 Troubleshoot the Wired Network Solution

Troubleshooting is a structured discipline that ensures network stability through systematic diagnostic methodologies. A combination of real-time monitoring and historical log analysis allows engineers to isolate and remediate failures efficiently.

1. Diagnostic Tools and Methods

Engineers rely on a suite of commands: Ping for reachability, Traceroute for hop-by-hop analysis, and "Show" commands for interface and routing status. These tools, integrated with Syslog and event logs, allow for the correlation of errors with specific configuration changes or environmental events.

2. Common Issue Resolution

Remediation often focuses on VLAN connectivity (resolving trunk mismatches), LACP failures (aligning configuration modes), and STP loops. Resolving loops requires verifying port states and tuning switch priorities to ensure the intended primary path is maintained.

3. Performance Troubleshooting

Performance degradation is addressed by reviewing CPU and memory usage, as well as monitoring port bandwidth. If a port consistently operates at over 90% capacity, hardware upgrades or QoS adjustments are required. Packet loss is often a result of physical layer issues, speed mismatches, or MTU settings.

4. Expanding Diagnostic Tools

Advanced troubleshooting may involve real-time **debug** commands for STP or LACP analysis. However, because debugging is CPU-intensive, it must be used cautiously and disabled immediately after use. Historical log reviews remain the primary method for analyzing intermittent failures without impacting device performance.

5. Advanced VLAN Troubleshooting

Connectivity failures often stem from Native VLAN mismatches on trunk ports or restrictive VLAN Access Control Lists (VACLs). Verifying that trunk configurations are identical on both ends of a link is a standard troubleshooting step.

6. Enhanced STP Troubleshooting

BPDU Guard and Root Guard act as defensive mechanisms. If an interface is found in a **Blocking state**, engineers must determine if this is a legitimate loop prevention measure or if a rogue device has triggered a protection mechanism like Root Guard to prevent root bridge manipulation.

7. LACP and QoS Troubleshooting

LACP troubleshooting involves using the "EtherChannel summary" command to identify ports stuck in a "standalone" state due to configuration mismatches. QoS issues are verified by auditing policies on specific interfaces and ensuring Low-Latency Queuing (LLQ) is functioning correctly for real-time traffic.

8. Deep Packet Loss Analysis

Persistent packet loss requires an analysis of MTU settings. While the standard Ethernet MTU is 1500 bytes, architects must ensure consistency across the path, particularly when using **9000-byte Jumbo Frames**, as mismatches cause drops due to fragmentation. Interface error counters should be checked for CRC errors, which typically point to faulty physical cabling. This holistic approach ensures that the wired network remains stable, secure, and performant.

9. Troubleshoot the wired network solution Practice Question

Q1: A network administrator is troubleshooting a connectivity issue. The administrator runs the command `ping 192.168.1.1` from a workstation and receives no response. Which of the following could be a possible reason?

A. The target device is powered off or disconnected
B. The target device does not have a valid IP address assigned
C. There is a VLAN misconfiguration preventing communication
D. All of the above

Q2: A user reports that they cannot access the internet. The network administrator runs `traceroute 8.8.8.8` and notices that the trace stops at the default gateway. What is the MOST likely issue?
A. The user's workstation is configured with an incorrect IP address
B. The DNS server is unreachable
C. The default gateway is misconfigured or down
D. The user's Ethernet cable is faulty

Q3: A network technician is troubleshooting a VLAN connectivity issue. Devices on VLAN 10 cannot communicate with devices on VLAN 20. Which command would help determine if VLANs are correctly configured on the switch?
A. `show vlan`
B. `show ip route`
C. `show interfaces trunk`
D. Both A and C

Q4: A network administrator suspects an issue with a link aggregation group (LACP). Which command should be used to verify the status of aggregated links?
A. `show etherchannel summary`
B. `show spanning-tree`
C. `show ip route`
D. `show vlan brief`

Q5: Which of the following is a likely cause of an STP loop in a network?
A. A switch has been incorrectly configured as the STP root bridge
B. A trunk port is configured as an access port
C. A switch port is blocking BPDU packets
D. A switch has a misconfigured ACL

Q6: A user complains of poor VoIP call quality. Which command can be used to check for interface congestion?
A. `show interfaces counters errors`
B. `show spanning-tree`
C. `show vlan`
D. `show ip route`

Q7: Which command should be used to verify if QoS settings are applied to an interface?
A. `show policy-map interface`
B. `show spanning-tree`
C. `show ip route`
D. `show etherchannel summary`

Q8: A network administrator notices high CPU usage on a switch. What is a likely cause?
A. Excessive STP recalculations due to topology changes
B. A misconfigured VLAN
C. A disconnected trunk port
D. A missing default route

Q9: A network technician finds that a switch port is discarding packets. Which of the following is the MOST likely cause?
A. The MTU setting is mismatched
B. The VLAN ID is incorrectly assigned
C. The switch's firmware is outdated
D. The interface speed is set to auto-negotiate

Learning Path & Study Advice

A productive study approach begins with reinforcing core networking principles such as Ethernet behavior, IP addressing, VLAN concepts, and switching fundamentals. From there, learners should progress toward advanced topics including redundancy mechanisms, routing interactions, policy enforcement, and traffic optimization. Emphasis should be placed on understanding why specific switching technologies are used, how they interact in enterprise designs, and what operational outcomes they support. Practical comprehension is strengthened by reviewing configuration logic, troubleshooting workflows, topology analysis, and scenario-based problem solving. Focusing on conceptual clarity alongside applied reasoning helps build durable professional knowledge.

Who This PDF Is For

This document is intended for network engineers, infrastructure specialists, enterprise administrators, technical consultants, and IT professionals responsible for managing switching environments in business networks. It is most suitable for individuals who already possess foundational networking knowledge and some hands-on experience with enterprise network operations. Learners preparing to deepen their expertise in switching design, resilience, security, and troubleshooting will benefit most from this overview.

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:

HPE6-A73 Aruba Certified Switching Professional Certification Training Courses - AAAdemy

Online Flashcards (Quizlet):

Attachment : Answers by Knowledge Point

Plan the wired network solution Practice Question
A1: Answer: C. Creating VLANs based on organizational roles and functions
Explanation: VLANs should be designed based on the roles and functions within an organization to ensure proper traffic segmentation, security, and efficiency. Assigning a unique VLAN for each user (Option A) is impractical due to scalability issues. VLANs should be configured at multiple network layers as needed (Option B). While separating guest traffic is important (Option D), VLANs serve broader purposes than just guest isolation.

A2: Answer: D. Preferred hardware vendor for network devices
Explanation: Business requirements should focus on how the network will support business operations, such as mission-critical applications (Option A), bandwidth and latency needs (Option C), and the number of users who will use the network (Option B). The choice of hardware vendor is important, but it is not a business requirement—it is a technical decision made later in the planning process.

A3: Answer: C. Deploying dual core switches with VRRP or HSRP
Explanation: The best redundancy solution for core network switches is to use dual core switches with Virtual Router Redundancy Protocol (VRRP) or Hot Standby Router Protocol (HSRP). This ensures failover capabilities and high availability.

- Option A: STP helps prevent loops but does not provide redundancy if the core switch fails.
- Option B: A single core switch with multiple power supplies improves uptime but does not prevent network failure if the switch itself fails.
- Option D: Restricting VLAN traffic to a single core switch reduces redundancy.

A4: Answer: B. Providing high-speed forwarding and backbone connectivity
Explanation: The core layer is designed for high-speed data forwarding and backbone connectivity within an enterprise network.

- Option A (Security policies and VLAN segmentation) are typically enforced at the aggregation layer.
- Option C (Managing and monitoring devices) is a function of the network management system, not the core layer.
- Option D (Assigning IP addresses) is handled by DHCP servers, usually located at the access or aggregation layer.

A5: Answer: B. Using DHCP for dynamic address assignment and reserving static addresses for critical infrastructure
Explanation: In a large enterprise network, DHCP is the best approach for assigning dynamic IP addresses to

clients, while critical devices (such as core switches, servers, and routers) should use static IP addresses for stability.

- Option A (Static IPs for all clients) is inefficient and difficult to manage.
- Option C (A single large subnet) lacks scalability and network segmentation.
- Option D (Overlapping subnets) causes routing conflicts and should be avoided.

A6: Answer: B. Implementing 802.1X authentication and role-based access control
Explanation: 802.1X authentication and role-based access control (RBAC) provide strong security by ensuring that only authorized users and devices can access the network.

- Option A (MAC filtering) is easy to bypass using MAC spoofing.
- Option C (Static VLANs without authentication) does not provide enough security.
- Option D (Disabling unused ports) is a good practice, but it is not sufficient on its own to prevent unauthorized access.

A7: Answer: B. The maximum power budget available on the switch
Explanation: When implementing PoE, it's important to consider the power budget of the switch, as each powered device (such as IP phones, access points, and cameras) requires a certain amount of power.

- Option A (Cable color) has no impact on PoE functionality.
- Option C (Network topology) is important but does not directly affect PoE implementation.
- Option D (VLAN count) does not influence PoE power delivery.

Install and configure the wired network solution Practice Question
A1: Answer: C. Ensuring proper airflow and cable management
Explanation: Proper airflow prevents overheating, which can damage network equipment, and proper cable management ensures easier troubleshooting and maintenance.

- Option A (Cable color) does not affect installation.
- Option B (Rack brand) is irrelevant as long as the rack meets standard specifications.
- Option D (Fiber vs. Copper) depends on network requirements, but does not directly impact physical installation.

A2: Answer: B. To enable remote administration and monitoring of the switch
Explanation: A management IP address allows network administrators to remotely access and configure the switch.

- Option A (Internet access for users) is unrelated to management IPs.
- Option C (Inter-VLAN communication) is achieved using routing, not management IPs.
- Option D (QoS settings) can be configured but is not the purpose of a management IP.

A3: Answer: A. `vlan 20; name VLAN20; interface range gigabitethernet1/1/5-10; switchport access vlan 20`
Explanation: This command sequence correctly:

1. Creates VLAN 20
2. Names it VLAN20

3. Assigns ports 5-10 to VLAN 20

- Option B lacks the necessary VLAN creation step.
- Option C incorrectly applies VLAN settings to an interface VLAN instead of switch ports.
- Option D enables trunk mode instead of access mode.

A4: Answer: B. To prevent switching loops in redundant network topologies
Explanation: STP prevents network loops by detecting and disabling redundant paths in a network.

- Option A (Increase bandwidth) is incorrect since STP disables some paths.
- Option C (VoIP prioritization) is a function of QoS, not STP.
- Option D (Static MAC addresses) is unrelated to STP.

A5: Answer: A. It combines multiple physical links into a single logical link to increase bandwidth and redundancy
Explanation: LACP allows multiple physical connections between devices to function as a single logical connection, improving both bandwidth and redundancy.

- Option B (Access control) is managed by AAA or ACLs, not LACP.
- Option C (IP assignment) is done by DHCP, not LACP.
- Option D (Unauthorized device detection) is handled by port security or 802.1X.

A6: Answer: C. It denies Telnet traffic but allows all other IP traffic
Explanation:

- The ACL rule `deny tcp any any eq 23` blocks Telnet traffic (port 23).
- The rule `permit ip any any` allows all other IP-based traffic.
- Option A (Blocking all traffic) is incorrect because the second rule allows all other traffic.
- Option B (Allowing only Telnet) is incorrect because Telnet is explicitly denied.
- Option D (Blocking all TCP traffic) is incorrect because only Telnet (port 23) is blocked.

A7: Answer: B. MAC Address Filtering (Port Security)
Explanation: Port security restricts access to a switch port based on MAC addresses, preventing unauthorized devices from connecting.

- Option A (QoS) manages traffic priority but does not restrict access.
- Option C (LACP) is used for link aggregation, not security.
- Option D (DHCP Snooping) prevents DHCP-based attacks but does not block unauthorized devices from connecting.

A8: Answer: B. RADIUS or TACACS+
Explanation: RADIUS and TACACS+ are used for Authentication, Authorization, and Accounting (AAA), ensuring secure access to network devices.

- Option A (DNS) is used for domain name resolution.
- Option C (SNMP) is used for monitoring and management, not authentication.
- Option D (IGMP) is used for multicast traffic management.

A9: Answer: B. Use VLANs and apply QoS policies to prioritize VoIP traffic
Explanation:

- VLANs can isolate VoIP traffic from data traffic, reducing congestion.
- QoS prioritizes VoIP packets, ensuring low latency and jitter.
- Option A (Disabling QoS) would negatively impact VoIP quality.
- Option C (Blocking VoIP with STP) makes no sense as STP prevents loops, not traffic types.
- Option D (Assigning lowest priority) would degrade VoIP performance.

Troubleshoot the wired network solution Practice Question
A1: Answer: D. All of the above
Explanation: A failed ping response can result from various issues:

- Option A (Powered off/disconnected): If the target device is powered off or its cable is unplugged, it will not respond.
- Option B (No valid IP address): If the device is misconfigured or does not have an IP, it cannot communicate.
- Option C (VLAN misconfiguration): If the workstation and target device are on different VLANs without proper routing, they cannot communicate.

A2: Answer: C. The default gateway is misconfigured or down
Explanation:

- If `traceroute` stops at the default gateway, the problem is likely at that point.
- Option A (Incorrect IP address) would prevent local network access, but if the user reaches the gateway, this is not the issue.
- Option B (DNS issue) would prevent domain name resolution, but `traceroute` works with IPs.
- Option D (Ethernet cable issue) would prevent all network access.

A3: Answer: D. Both A and C
Explanation:

- Option A (`show vlan`) lists VLAN assignments and ensures that interfaces belong to the correct VLANs.
- Option C (`show interfaces trunk`) helps verify if VLANs are properly passed between switches.
- Option B (`show ip route`) is only useful if routing between VLANs is involved.

A4: Answer: A. `show etherchannel summary`
Explanation:

- Option A (`show etherchannel summary`) displays the status of link aggregation groups, showing active/inactive ports.
- Option B (`show spanning-tree`) is useful for STP issues but not LACP.
- Option C (`show ip route`) is for routing, not link aggregation.
- Option D (`show vlan brief`) shows VLANs but does not relate to LACP.

A5: Answer: C. A switch port is blocking BPDU packets
Explanation:

- Option C (Blocking BPDU packets) can prevent STP from functioning properly, causing loops.

- Option A (Incorrect root bridge) may cause suboptimal traffic flow but does not create a loop.
- Option B (Trunk as access port) may prevent VLAN traffic but does not cause a loop.
- Option D (Misconfigured ACL) can block traffic but does not impact STP.

A6: Answer: A. `show interfaces counters errors`
Explanation:

- Option A (`show interfaces counters errors`) helps identify packet drops or congestion.
- Option B (`show spanning-tree`) relates to STP but not congestion.
- Option C (`show vlan`) does not show bandwidth usage.
- Option D (`show ip route`) helps with routing but not congestion.

A7: Answer: A. `show policy-map interface`
Explanation:

- Option A (`show policy-map interface`) displays applied QoS settings.
- Option B (`show spanning-tree`) is unrelated to QoS.
- Option C (`show ip route`) does not show QoS policies.
- Option D (`show etherchannel summary`) is for link aggregation, not QoS.

A8: Answer: A. Excessive STP recalculations due to topology changes
Explanation:

- Option A (STP recalculations) can cause high CPU usage if the network experiences frequent topology changes.
- Option B (Misconfigured VLAN) does not directly affect CPU usage.
- Option C (Disconnected trunk port) would affect connectivity but not CPU usage.
- Option D (Missing default route) would cause routing issues but not high CPU load.

A9: Answer: A. The MTU setting is mismatched
Explanation:

- Option A (MTU mismatch) can cause packet fragmentation and loss.
- Option B (Incorrect VLAN ID) would prevent communication but not cause discards.
- Option C (Outdated firmware) may cause instability but not necessarily discards.
- Option D (Auto-negotiation) is unlikely to cause packet discards unless there's a speed mismatch.

Manage, maintain, optimize, and monitor the wired network solution Practice Question
A1: Answer: D. All of the above
Explanation:

- Option A (SNMP): SNMP (Simple Network Management Protocol) is widely used for real-time monitoring and gathering device statistics.
- Option B (Aruba AirWave): Aruba AirWave provides comprehensive network visibility and management for on-premises deployments.
- Option C (Aruba Central): Aruba Central is a cloud-based monitoring and management platform.

- Since all three tools are used for network monitoring, the correct answer is D (All of the above).

A2: Answer: A. Excessive spanning tree recalculations
Explanation:

- Option A (Excessive spanning tree recalculations): Frequent changes in the network topology can cause STP to recalculate constantly, leading to high CPU usage.
- Option B (Low bandwidth utilization): This would not impact CPU usage.
- Option C (Misconfigured VLANs): VLAN misconfigurations can cause connectivity issues but are unlikely to increase CPU usage.
- Option D (A disconnected trunk port): This might impact VLAN communication but does not directly lead to high CPU usage.

A3: Answer: B. Scheduled automatic backups help ensure quick recovery from failures
Explanation:

- Option A (Only after major changes): Backups should be regularly scheduled, not just after changes.
- Option B (Automatic backups ensure quick recovery): This is the best practice for disaster recovery and device restoration.
- Option C (Backups unnecessary with firmware updates): Firmware updates and configuration backups serve different purposes.
- Option D (Cannot restore after failure): Configurations can be restored from backups.

A4: Answer: A. DSCP markings
Explanation:

- Option A (DSCP markings): DSCP (Differentiated Services Code Point) is used to classify and prioritize traffic for QoS.
- Option B (VLAN tagging): VLANs segment traffic but do not provide prioritization.
- Option C (Port mirroring): Used for traffic analysis, not prioritization.
- Option D (STP): Prevents network loops but does not manage traffic priority.

A5: Answer: B. Implementing load balancing
Explanation:

- Option A (Enabling SNMP): SNMP is used for monitoring, not for resolving congestion.
- Option B (Implementing load balancing): Load balancing distributes traffic across multiple links, reducing congestion.
- Option C (Configuring DHCP snooping): Helps prevent rogue DHCP servers but does not address congestion.
- Option D (Increasing STP priority): Affects spanning-tree root selection but does not resolve congestion.

A6: Answer: A. `show policy-map interface`
Explanation:

- Option A (`show policy-map interface`): Displays the applied QoS policies on an interface.
- Option B (`show spanning-tree`): Displays STP status but is unrelated to QoS.

- Option C (`show ip route`): Displays routing table, not QoS policies.
- Option D (`show vlan`): Displays VLAN assignments, not QoS.

A7: Answer: B. Access Control Lists (ACLs)
Explanation:

- Option A (VLAN pruning): Reduces unnecessary VLAN traffic but does not restrict access.
- Option B (ACLs): Can be used to restrict management access to a specific subnet.
- Option C (Port security): Controls device access at the port level but not subnet-based management.
- Option D (LACP): Used for link aggregation, not access restriction.

A8: Answer: B. Implementing AAA with TACACS+ or RADIUS
Explanation:

- Option A (DHCP snooping): Prevents rogue DHCP servers but does not protect against unauthorized SSH logins.
- Option B (AAA with TACACS+ or RADIUS): Provides authentication, authorization, and accounting to secure switch access.
- Option C (Port mirroring): Used for traffic monitoring, not access control.
- Option D (VLAN tagging): Organizes traffic but does not enhance SSH security.

A9: Answer: B. Configuring VLAN pruning
Explanation:

- Option A (BPDU Guard): Prevents unauthorized switches from becoming part of the STP topology but does not reduce broadcast storms.
- Option B (VLAN pruning): Limits VLAN propagation to only necessary links, reducing unnecessary broadcast traffic.
- Option C (Disabling STP): Increases the risk of loops, worsening the problem.
- Option D (Increasing switch MTU): Affects frame size but does not reduce broadcast traffic.