Implementing AOS-CX Switching (AR-ICX)

Course Description

This 5-day course prepares you for the updated AOS-CX switching based ACP - Switching certification exam (Exam Code: HPE7-A08). Attending this course will teach you the advanced skills necessary to implement and operate enterprise-level HPE Aruba Networking switching solutions. You will build on the skills you learned at the Associate level to configure and manage modern, open standardsbased networking solutions using HPE Aruba Networking AOS-CX routing and switching technologies. In this course, you will learn about AOS-CX switch technologies:

- Securing port access with HPE Aruba Networking Dynamic Segmentation
- Redundancy technologies such as Multiple Spanning Tree Protocol (MSTP)
- Link aggregation techniques, including Link Aggregation Protocol (LACP)
- Switch virtualization with HPE Aruba Networking Virtual Switching eXtension (VSX) and HPE Aruba Networking Virtual Switching Framework

This course is approximately 50% lecture and 50% hands-on lab exercises.

Course Duration:

5 days

Prerequisites:

It is highly recommended that candidates already have some advanced knowledge of networking (routing, switching, and security). Candidates are encouraged to have taken the AOS-CX Switching Fundamentals, Rev 24.31 course and achieved the ACA - Switching certification.

Objectives:

After you successfully complete this course, expect to be able to:

- Compare AOS-CX switching models and describe features
- Use NAE and scripts to ease monitoring, troubleshooting of operational issues as well as sFlow traffic flows and port mirroring
- Describe VSX use cases, operation, and best practices for resiliency and scalability
- Describe and configure access control lists for improved security, protecting management traffic and ease troubleshooting
- Describe and deploy multiarea OSPF networks, virtual links and improved convergence times as well as security
- Establish, monitor, manipulate, and filter BGP route relationships, path selection and advertisements
- Describe multicast addressing, IGMP, and IGMP snooping
- Describe and implement Protocol Independent Multicast (PIM)- Dense mode (PIM-DM) and Sparse mode (PIM-SM)
- Describe the components of 802.1x authentication, implementing it on AOS-CX switch ports, and integrate it with HPE Aruba Networking ClearPass

- Implement RADIUS-based MAC authentication and device profiles
- Understand user-based tunneling and configure Dynamic Segmentation and PAPI
- Describe and implement various Quality of Service (QoS) mechanisms, including classifications, marking, queues and schedules
- Implement VRF to isolate routed traffic and manipulate traffic routing with Policy-Based Routing (PBR)
- Understand and configure captive portal configuration with ClearPass Guest and BYOD solutions

Course Outline:

- Intro to AOS-CX Switching
    - AOS-CX switch overview
    - Legacy management systems
    - Modern management approach
    - The REST API and URIs
    - NAE and the Time-series database
    - Dynamic Segmentation
    - Always on POE
    - Virtual Output Queuing
- Virtual Switching eXtension
    - Virtual switching technologies
    - VSX components
    - VSX synchronization
    - Split brain scenarios
- Layer 2 Optimization
    - UDLD
    - Private VLAN
    - Basics of Spanning Tree Protocol
    - RPVST+
- Advanced OSPF
    - OSPF overview
    - Multi-area OSPF
    - Route redistribution using ASBRs
    - OSPF area types
    - OSPF redundancy
    - Additional OSPF features
- Border Gateway Protocol
    - BGP overview
    - BGP neighborconnections
    - BGP route advertisements
    - BPG route selection metrics and tuning
    - Controlling eBGP routes

- Additional Layer 3 Features
    - Virtual routing and forwarding (VRF)
    - Policy-based routing
    - ARP protection
    - DHCP snooping
    - IPsec and NAT
- IGMP
    - Multicast introduction
    - IGMP overview
    - Multicast Routing
    - PIM introduction
    - PIM-DM
    - PIM-SM
    - PIM-SM build-up process
    - BSR mechanism
    - VSX and PIM
- Access Control Lists
    - ACL introduction and creation
    - ACL application scenarios
    - Applying ACLs
    - Object groups
    - Classification policies
    - Restrictions and resource utilization
- 802.1X Authentication
    - Authentication overview
    - 802.1X authentication overview
    - Configuring 802.1X on switch ports
    - RADIUS attributes for the dynamic settings
    - User roles overview
    - Device fingerprinting overview
- MAC Authentication
    - MAC authentication overview
    - MAC-auth with multiple clients
    - MACsec overview
- Dynamic Segmentation
    - Dynamic Segmentation overview
    - overv
    - User-based tunneling
    - Configuring UBT
    - UBT with MC cluster
    - Troubleshooting

- REST API
    - REST API introduction
    - REST basic concepts
    - Enabling the REST interface on an AOS-CX switch
    - Sending requests to the REST API
    - Accessing the REST API reference interface
    - Use cases and resources
- Quality of Service
    - QoS overview
    - Classifying traffic and applying policies
    - LLDP-MED and device profiles
- Network Analytics Engine (NAE)
    - NAE overview
    - NAE agents
    - Agent actions
- Troubleshooting
    - Troubleshooting overview
    - Troubleshooting principles
    - Components of effective troubleshooting
    - Need for a methodical approach
    - Problem-solving methodology
    - Network troubleshooting tools

Who Should Attend

Typical candidates for this course have experience in advanced level implementation and maintenance of wired solutions. They possess experience assessing and interpreting existing networks and network design documentation. They regularly troubleshoot, resolve issues, and perform ongoing support of large network environments. They have familiarity with wired network security best practices and perform duties independently with at least two years of experience working as a member of the team that supports maintaining multiple campus topologies, edge branches, and data center networks.