Configuring Aruba OS Switching Level 2 (AR-CASL2)

Course Description

This course teaches you how to implement and operate enterprise-level Aruba campus switching solutions. Hand-on labs give you experience with ArubaOS-Switches, including securing access, redundancy technologies such as Multiple Spanning Tree Protocol (MSTP), link aggregation techniques including Link Aggregation Protocol (LACP) and switch virtualization with HPE's Virtual Switching Framework (VSF).

You will also learn to configure dynamic routing with Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP), network optimization via Quality of Service (QoS), IP multicast routing leveraging Protocol Independent Multicast (PIM), and protecting the network using Access Control Lists (ACLs).

This course is approximately 30% lecture and 70% hands on lab exercises

Course Duration:

5 days

Prerequisites:

Aruba Switching Fundamentals

Objectives:

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

- Implement spanning tree protocol and loop protections
- Ensure redundancy for a network's default gateway by configuring VRRP on Aruba switches
- Implement and manage an VSF fabric
- Deploy ArubaOS switches in single-area and multi-area OSPF systems
- Use Internet Group Management Protocol (IGMP) to optimize forwarding of multicasts within VLANs
- Implement PIM-DM to route multicast traffic
- Establish and monitor BGP sessions between your routers and ISP routers
- Define ACLs and identify the criteria by which ACLs select traffic
- Configure ACLs on ArubaOS switches to select given traffic
- Implement 802.1X on ArubaOS switch ports
- Configure captive portal authentication on ArubaOS switches to integrate them with an Aruba ClearPass solution
- Configure tunneled-node on ArubaOS switches
- Configure ArubaOS switches to select traffic, apply the appropriate QoS marking, and place the traffic in the proper priority queues
- Implement DHCP snooping and ARP protection to defend networks against DHCP exploits, ARP snooping, and ARP poisoning attacks
- Implement the proper port security measures for various use cases
- Implement connection rate filtering to provide a first layer of protection against viruses and worms

Course Outline:

- Introduction to Aruba Solutions
    - Describe market trends that are leading companies to implement a digital workplace
    - Describe how the Mobile First Network from Aruba, a Hewlett Packard Enterprise company, delivers the digital workplace
- Data Link Layer Redundancy Technologies
    - Compare RPVST+ with RSTP and MSTP
    - Implement spanning tree protocol and loop protections
    - Describe how Unidirectional Link Detection (UDLD) and Device Link Detection
    - Protocol (DLDP) detect and handle unidirectional links
- Virtual Router Redundancy Protocol (VRRP)
    - Ensure redundancy for a network’s default gateway by configuring VRRP onAruba switches
    - Establish load-balancing of active routing in several different ways
    - Use best practices for implementing VRRP with MSTP
- Aruba Backplane Stacking and Advanced Virtual Switch Framework (VSF)
    - Describe the three topologies supported with backplane stacking and the roles
    - members play in the stack
    - Explain how backplane stacking handles stack fragments
    - Implement and manage an VSF fabric
    - Describe what a split VSF stack is and configure the mechanisms designed to detect and remedy this problem
- Advanced Open Shortest Path First (OSPF)
    - Deploy ArubaOS products in single-area and multi-area OSPF systems
    - Use area definitions and summaries to create efficient and scalable multiple area designs
    - Advertise routes to external networks in a variety of OSPF environments
    - Promote fast, effective convergence during a variety of failover situations
    - Use virtual links as required to establish non-direct connections to the backbone
    - Implement OSFP authentication
- Internet Group Management Protocol (IGMP)
    - Use Internet Group Management Protocol (IGMP) to optimize forwarding of multicasts within VLANs
    - Describe the differences between IGMP and IGMP snooping
- Protocol Independent Multicast–Dense Mode (PIM-DM)
    - Distinguish between PIM-DM and PIM-SM
    - Implement PIM-DM to route multicast traffic
- Border Gateway Protocol (BGP)
    - Establish and monitor BGP sessions between your routers and ISP routers
    - Advertise an IP block to multiple ISP routers
    - Configure a BGP router to advertise a default route in OSPF
- Access Control Lists (ACL)
    - Define ACLs and identify the criteria by which ACLs select traffic
    - Configure ACLs on ArubaOS switches to select given traffic

- Apply static ACLs to interfaces to meet the needs of a particular scenario
    - Examine an ACL configuration and determine the action taken on specific packets
- 802.1XAuthentication
    - Implement 802.1X on ArubaOS switch ports
    - Integrate ArubaOS switches with an Aruba ClearPass solution, which might apply dynamic VLAN assignments, ACLs, QoS priorities, and rate Limits
- MAC Authentication
    - Implement RADIUS-based MAC Authentication (MAC-Auth) on ArubaOS switch ports
    - Implement local MAC Authentication (LMA) on ArubaOS switch ports
- Captive Portal and Other Guest Options
    - Configure captive portal authentication on ArubaOS switches to integrate them with an Aruba ClearPass solution
    - Implement Web Authentication (Web-Auth) on Aruba switch ports
    - Combine multiple forms of authentication on a switch port that supports one or more simultaneous users
    - Use the Unauthenticated VLAN on ArubaOS switches to provide guest access
- Integrating with an Aruba Mobility Solution
    - Configure tunneled-node on ArubaOS switches
    - Describe when and how to configure PAPI enhanced security, high availability, and fallback switching for tunneled-node
- Secure Device Management
    - Set up RADIUS authentication and authorization for managers
    - Describe the differences between SNMPv2c and v3 and configure SNMPv3 settings on ArubaOS switches
    - Explain how technologies such as RMON, sFlow, and traffic mirroring allow you to monitor network traffic
    - Explain best practices for managing configurations and monitoring network traffic using a solution such as Aruba AirWave
- Quality of Service
    - Describe how ArubaOS switches prioritize traffic based on its queue
    - Configure ArubaOS switches to honor the appropriate QoS marks applied by other devices
    - Configure ArubaOS switches to select traffic, apply the appropriate QoS marking, and place the traffic in the proper priority queues
    - Implement rate limiting
    - Configure a voice VLAN and LLDP-MED
- Additional Security Features
    - Implement DHCP snooping and ARP protection to defend networks against DHCP exploits, ARP snooping, and ARP poisoning attacks
    - Implement the proper port security measures for various use cases
    - Explain how MAC lockdown differs from port security and use the proper solution for each use case
    - Implement connection rate filtering to provide a first layer of protection against viruses and worms

Who Should Attend

- Typical candidates for this course are IT Professionals who will deploy and manage networks based on HPE’s ArubaOS-Switches.