Aruba Certified Switching Professional (ACSP) OFFICIAL CERTIFICATION STUDY GUIDE (EXAM HPE6-A73)

First Edition

Richard Deal and Peter Debruyne
About the Authors

Richard Deal is an independent consultant who designs wireless and wired networks and provides network management services for small companies. He has created and developed many networking courses and instructs IT professionals on the best ways to design and implement Aruba’s wired and wireless network solutions. Richard has authored countless books on various networking topics.

Peter Debruyne was co-developer of the Implementing ArubaOS-CX Switching course. He is an Aruba Certified Edge Expert (ACCX, ACMX, and ACDX) and ACSP certified. Peter is an Aruba Certified Instructor and resides in Belgium.

Introduction

This book guides you through Aruba wired network solutions involving ArubaOS-CX switching products and features and helps you prepare for the Aruba Certified Switching Professional exam (HPE6-A73). You will learn the following:

- Implementing ArubaOS-CX switches, redundancy technologies, NetEdit switch management, link aggregation techniques, network analytics, and switch virtualization with HPE’s Virtual Switching Extension (VSX)

- Configuring dynamic routing with Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Virtual Routing Forwarding (VRF), and policy-based routing (PBR)

- Implementing IP multicast routing involving IGMP and PIM

- Optimizing networks by incorporating Quality of Service (QoS) priorities and device groups

- Protecting the network using access control lists (ACLs) and traffic classifier policies

- Securing access with 802.1X, MAC authentication, captive portal, dynamic segmentation with user-based tunneling (UBT), and local and downloadable user roles

Aruba Education Services

Aruba Education Services offers comprehensive training and certification programs from fundamental to advanced levels across the Aruba product line.

To learn more about Aruba certifications and training, please visit: https://www.arubanetworks.com/support-services/training-services/

Audience

This book is designed for individuals wanting to continue their journey in understanding the various Aruba products and using best practice design guidelines to implement campus wired solutions.
involving ArubaOS-CX switches and CX features. The audience includes network technicians, network engineers, network architects, and network presales individuals.

**Assumed Knowledge**

This is an intermediate-level guide that will leverage ArubaOS-CX switches and features to implement a campus-sized wired solution. It is assumed that you have a knowledge of basic switching technologies that is covered in the Configuring ArubaOS-CX Fundamentals (CXF) course.

**Minimum Qualifications**

Typical candidates for this certification are IT associates who want to learn about the ArubaOS-CX switching products and the features and protocols used to help implement a campus-switched network. It is assumed that you have the equivalent networking and switching knowledge covered in the Configuring ArubaOS-CX Fundamentals (CXF) course.

**Relevant Certifications**

The Aruba Certified Switching Professional (ACSP) certification validates that you have the intermediate knowledge and skills required to implement Aruba campus wired solutions involving ArubaOS-CX switches, CX switching features, and various standards-based protocols.

**Preparing for Exam HPE6-A73**

This self-study guide does not guarantee that you will have all the knowledge you need to pass the exam. It is expected that you will also draw on real-world experience and would benefit from completing the hands-on lab activities provided in the instructor-led training. However, the labs taught in the official course are provided for you here in this book assuming you have the correct hardware and software to perform the labs. This book covers the same material as the actual course. Therefore, to pass the certification exam, you should be intimately familiar with the material presented here. Aruba recommends reading the book and performing the labs three times before attempting the exam. Please note that successful completion of this book, corresponding course, or additional study materials alone does not ensure you will pass the HPE6-A73 exam.

**Recommended Training**

Recommended training to prepare for each exam is accessible from the ACDA exam page. For more information, please visit: http://www.arubanetworks.com/support-services/training-services/certified-switching-professional/.
Obtain Hands-on Experience

You are not required to take the recommended, supported courses, and completion of training does not guarantee that you will pass the exam. Aruba strongly recommends a combination of training, thorough review of courseware and additional study references, and sufficient on-the-job experience prior to taking an exam.

Exam Registration

To register for an exam, please follow the links provided at: http://www.arubanetworks.com/support-services/training-services/certified-switching-professional/.
**CONTENTS**

1  **Introduction to Aruba Switching** .......................................................... 1
   Overview ........................................................................................................ 1
   AOS-CX Switch Overview ............................................................................. 2
      AOS-CX: Heart of Aruba’s Core, Aggregation, and Access ...................... 2
      What Does AOS-CX Mean to Customers? ............................................... 3
      End-to-End AOS-CX Architecture ............................................................ 4
      8400: Highly Available and Resilient Aggregation and Core ............ 5
      8325 Overview ....................................................................................... 6
      8320 Overview ....................................................................................... 7
      6400 Series ............................................................................................ 8
      6300 Platforms ....................................................................................... 9
      AOS-CX Switch Capabilities ................................................................... 10
   Features .......................................................................................................... 12
      Fully Open and Programmatic Software Architecture ....................... 12
      AOS-CX Switch Virtualization Solutions: VSX ................................... 13
      VSF and Backplane Stacking ................................................................. 14
      NetEdit ..................................................................................................... 15
      Network Analysis Engine (NAE) and the Time-Series Database .......... 16
      Dynamic Segmentation ........................................................................... 17
      Always-on PoE and Quick PoE for the 6300/6400 ........................... 18
      Virtual Output Queuing (VOQ) .............................................................. 19
      VOQ in the 6400 Switches ................................................................. 20
      Virtual Output Queuing – Use Cases .................................................... 22
   Lab 1: Base Configuration ........................................................................... 23
      Lab Course Topology ............................................................................. 23
      Lab 1 Diagram ....................................................................................... 24
      Overview .................................................................................................... 24
      Objectives .................................................................................................. 24
      Task 1: Factory Reset of Devices ......................................................... 24
      Task 2: Configure the OOBM for Access1 ........................................... 26
      Task 3: Configure the OOBM for Access2/Core1/Core2 ................... 30
   Learning Check .............................................................................................. 34
   Summary ........................................................................................................ 34
Traffic Forwarding..................................................................................212
  VSX LAG...................................................................................213
  Active-Gateway ........................................................................214
  Active-Gateway: South-North Unicast Traffic...........................216
  VSX LAG and Upstream Unicast Routing....................................217
  Upstream Connectivity: Routed Only Port (ROP) .........................218
  VSX and Upstream Routing...........................................................218

Split-Brain Condition .............................................................................219
  Split-Brain Scenario .................................................................219
  ISL Failure: SVI Impact...............................................................220

Lab 4: Configuring VSX ........................................................................221
  Overview ....................................................................................221
  Objectives ....................................................................................221
  Task 1: VSX Basic Setup ............................................................222
  Task 2: VSX Configuration Synchronization ..................................231
  Task 3: VSX Layer 2—VSX Link Aggregation (VSX LAG) ..........237
  Task 4: VSX Layer 3—Active-Gateway ........................................242
  Task 5: VSX Split-Brain Handling ................................................250
  Task 6: Finalize Configuration for Future Labs .................................259

Learning Check ....................................................................................261

Summary............................................................................................262

5 ACLs ................................................................................................263
  Overview ....................................................................................263
  ACL Overview .............................................................................263
    What is an ACL? ........................................................................264
    Reasons to Implement ACLs ....................................................265
    ACL IDs and Types ....................................................................266
    ACL Rule Components ............................................................268
    Example IP ACL Rules ............................................................269
    Example MAC ACL Rules ........................................................273
    Processing Order and Implicit Deny ............................................274
    Applying ACLs ........................................................................276
    Example ACL Configuration ....................................................278

Creating Rules (ACEs)........................................................................279
  Detailed Look at Source/Destination IP Addresses in ACLs ............279
  Specifying IP Address Ranges with a Prefix Length .......................280
  Specifying MAC Address Ranges ...............................................283
  Managing ACL Rule Sequence ....................................................284
  Logging and Counting ACL Matches ............................................285
  Review Activity: Analyzing an ACL ..............................................288
Options for External Route Metrics .................................................417
External Type 2 .............................................................................418
External Type 1 .............................................................................421
External Type 1 versus External Type 2: Which Would You Use? ......425
OSPF Area Types ................................................................................425
Need for Eliminating Excessive External Routes ...............................425
Using Stub Areas to Eliminate External Routes .................................427
Need for Eliminating All Inter-Area and External Routes .................428
Using Totally Stubby Areas ............................................................428
Need for Advertising External Routes into a Stub Area.....................430
Using Not-So-Stubby Areas .............................................................430
Totally Not-So-Stubby Areas (NSSAs) .............................................432
Review: Factors that Affect OSPF Route Selection .............................432
Implementing OSPF Redundancy ........................................................434
OSPF Failover and Convergence ....................................................434
OSPF and Bidirectional Forwarding Detection (BFD) .......................437
Using BFD to Speed OSPF Failed Neighbor Detection ....................438
Using OSPF with VSX .................................................................441
Implementing Additional OSPF Features ...........................................442
The Need for Graceful Restart .........................................................442
Implementing OSPF and VRRP .......................................................448
Example Situations that Require Virtual Links ................................449
OSPF Authentication .....................................................................453
Lab 6.3 ..............................................................................................455
Lab 6.3 Diagram ..........................................................................455
Overview .....................................................................................455
Objectives ....................................................................................456
Task 1: Configure Link to RouterA ...................................................456
Task 2: Redistribute Static Routes into OSPF .....................................458
Task 3: Control Route Redistribution and Metric Types ......................464
Task 4: Filter Routes with Stub and Totally Stubby Areas ...................468
Task 5: Filter Routes with a Not So Stubby Area (NSSA) ..................475
Learning Check ................................................................................481
Summary ............................................................................................482

7 BGP ......................................................................................... 483
Overview ...........................................................................................483
Introduction to BGP ........................................................................483
BGP Use Case: Multi-Homed ISP Connections .................................484
Other BGP Use Cases .....................................................................485
BGP AS ........................................................................................486
Establishing BGP Connections ..............................................................488
  BGP TCP Sessions ........................................................................489
  BGP Neighbor Addresses: eBGP ....................................................489
  BGP Neighbor Addresses: iBGP .....................................................491
  MD5 Authentication ......................................................................494
  BGP Connection States ..................................................................494
BGP Routing Metrics ............................................................................496
  More Criteria in BGP Best Route Selection .......................................496
  BGP AS Path Length Metric ............................................................498
  Weight .........................................................................................500
  Local Preference ............................................................................501
  Multiple Exit Discriminator (MED) ...................................................502
Receiving and Advertising Routes .........................................................503
  BGP Routing Table ........................................................................504
  Next-Hop Reachability ..................................................................505
  Next-Hop Reachability: Next-Hop-Self ..........................................505
  Receiving Routes from BGP Neighbors ............................................506
  Advertising Routes to BGP Peers .....................................................508
  Preferred Solution: Inject Routes .....................................................511
  Inject Routes Example .....................................................................511
Route Control ......................................................................................512
  Reasons to Control eBGP Routes .....................................................513
  Route Control Implementation .......................................................513
  Avoid Becoming a Transit AS ...........................................................519
  Control Inbound Routes ..................................................................521
  Advertising External Routes into OSPF ............................................522
Lab 7 .................................................................................................523
  Lab 7 Diagram .............................................................................523
  Overview ......................................................................................524
  Objectives ......................................................................................524
  Task 1: Prepare the Lab Setup ........................................................524
  Task 2: Core1 eBGP Peering to ISP1 ..............................................525
  Task 3: Core1 and Core2 iBGP Peering ..........................................531
  Task 4: Core2 eBGP Peering to ISP2 ..............................................538
  Task 5: Announce Routes to eBGP Peers ........................................544
Learning Check ..................................................................................550
Summary ............................................................................................550

8 IGMP ...............................................................................................551
  Overview ......................................................................................551
  Multicast Introduction .....................................................................551
Configuring 802.1X .................................................................661
  Specifying the RADIUS Server ..............................................661
  Need for Changing Authorization Information for Devices Dynamically ......................................................662
  Dynamic Authorization Configuration ...................................663
  Enabling 802.1X .....................................................................665
  Managing Multiple RADIUS Servers using RADIUS Groups .................................................................667

RADIUS Attributes ......................................................................670
  Customizing Authenticated Users’ Access ..............................671
  How the RADIUS Server Sends Dynamic Settings ................672
  Device-Based Mode ..............................................................675
  Device-Based Mode Use Case ...............................................676
  Issues with Device-Based Mode ................................ ..........677
  Client-Based Mode ...............................................................678
  Example of How Client-Based Mode Operates ....................679

User Roles ...................................................................................680
  Colorless Ports .......................................................................680
  User Roles Overview ............................................................681
  Role Assignment: LUR ...........................................................682
  Role Assignment: DUR ..........................................................685
  User Role-Based Authorization .............................................686
  Local Authorization Role Options .........................................687

Lab 10 .......................................................................................691
  Lab 10 Diagram .......................................................................691
  Overview ................................................................................691
  Objectives ..............................................................................691
  Task 1: Prepare the Lab Start Configuration .........................692
  Steps (Required) .....................................................................692
  Task 2: RADIUS Server Setup ..............................................692
  Task 3: Basic 802.1X Authentication with a Single User ..........702
  Task 4: Change of Authorization Verification ........................711
  Task 5: Aruba User Role-Based Access .................................716
  Task 6: Unknown Role Assignment .......................................725

Learning Check ..........................................................................727

Summary ....................................................................................727

11 MAC Authentication .............................................................729
  Overview ................................................................................729
  RADIUS MAC-Auth ..............................................................729
    MAC-Auth Use Cases ...........................................................729
    RADIUS-Based MAC-Auth ..................................................731
<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS-Based MAC-Auth Options</td>
</tr>
<tr>
<td>MAC-Auth and Provisioning with ClearPass</td>
</tr>
<tr>
<td>RADIUS-Based MAC-Auth Configuration Process</td>
</tr>
<tr>
<td>Optional Configuration Steps</td>
</tr>
<tr>
<td>Multiple Client and Authentication Method Scenarios</td>
</tr>
<tr>
<td>Combining MAC-Auth and 802.1X</td>
</tr>
<tr>
<td>Implementing MAC-Auth on Ports with Multiple Clients</td>
</tr>
<tr>
<td>Combining MAC-Auth and 802.1X in Multiple Client Scenarios</td>
</tr>
<tr>
<td>Lab 11</td>
</tr>
<tr>
<td>Overview</td>
</tr>
<tr>
<td>Objectives</td>
</tr>
<tr>
<td>Task 1: MAC Authentication with a Single Device on a Port</td>
</tr>
<tr>
<td>Task 2: Verify Access with Two Devices Connected on the Same Port</td>
</tr>
<tr>
<td>Task 3: Aruba User Role-Based Access</td>
</tr>
<tr>
<td>Task 4: Client-Mode versus Device-Mode Port Authentication</td>
</tr>
<tr>
<td>Task 5: Authentication Priority Order with Combined MAC-Auth and 802.1X</td>
</tr>
<tr>
<td>Task 6: Device Profiles with LLDP</td>
</tr>
<tr>
<td>Task 7: Save checkpoint configuration</td>
</tr>
<tr>
<td>Learning Check</td>
</tr>
<tr>
<td>Summary</td>
</tr>
<tr>
<td>12 Dynamic Segmentation</td>
</tr>
<tr>
<td>Overview</td>
</tr>
<tr>
<td>Dynamic Segmentation Overview</td>
</tr>
<tr>
<td>Colorless Ports</td>
</tr>
<tr>
<td>Benefits of Tunneled-Node</td>
</tr>
<tr>
<td>Use Cases</td>
</tr>
<tr>
<td>Switch and Mobility Controller (MC) Communications</td>
</tr>
<tr>
<td>Enhanced PAPI Security</td>
</tr>
<tr>
<td>Tunneling User Traffic to an MC</td>
</tr>
<tr>
<td>How the MC Handles Tunneled-Node Traffic</td>
</tr>
<tr>
<td>Guidelines for the Path Between Switch and MC</td>
</tr>
<tr>
<td>What is User-Based Tunneling (UBT)?</td>
</tr>
<tr>
<td>Local Switching versus UBT</td>
</tr>
<tr>
<td>Local Switching or UBT Process</td>
</tr>
<tr>
<td>Policy Source and Enforcement for Different Scenarios</td>
</tr>
<tr>
<td>License Requirements</td>
</tr>
<tr>
<td>UBT Scalability</td>
</tr>
<tr>
<td>Section</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Lab 13</td>
</tr>
<tr>
<td>Lab 13 Diagram</td>
</tr>
<tr>
<td>Overview</td>
</tr>
<tr>
<td>Objectives</td>
</tr>
<tr>
<td>Task 1: Prepare the Lab Start Configuration</td>
</tr>
<tr>
<td>Task 2: Port Classification—Trust Configuration</td>
</tr>
<tr>
<td>Task 3: LLDP Device Profile for QOS Trust</td>
</tr>
<tr>
<td>Task 4: QOS Classification</td>
</tr>
<tr>
<td>Task 5: Queue configuration</td>
</tr>
<tr>
<td>Task 6: LLDP-MED and Voice VLAN configuration</td>
</tr>
<tr>
<td>Learning Check</td>
</tr>
<tr>
<td>Summary</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 Additional Routing Technologies</td>
<td>939</td>
</tr>
<tr>
<td>Overview</td>
<td>939</td>
</tr>
<tr>
<td>Virtual Routing and Forwarding (VRF)</td>
<td>939</td>
</tr>
<tr>
<td>Introduction to VRF</td>
<td>939</td>
</tr>
<tr>
<td>VRF Management Example</td>
<td>941</td>
</tr>
<tr>
<td>VRF Service Provider Example</td>
<td>941</td>
</tr>
<tr>
<td>Creating VRFs</td>
<td>942</td>
</tr>
<tr>
<td>Implementing Routing with VRFs</td>
<td>943</td>
</tr>
<tr>
<td>Policy-Based Routing (PBR)</td>
<td>944</td>
</tr>
<tr>
<td>Introduction to PBR</td>
<td>944</td>
</tr>
<tr>
<td>Policy Actions</td>
<td>946</td>
</tr>
<tr>
<td>Guest Example</td>
<td>950</td>
</tr>
<tr>
<td>Implementing a PBR Policy</td>
<td>951</td>
</tr>
<tr>
<td>Lab 14</td>
<td>954</td>
</tr>
<tr>
<td>Lab 14 Diagram</td>
<td>954</td>
</tr>
<tr>
<td>Overview</td>
<td>954</td>
</tr>
<tr>
<td>Objectives</td>
<td>955</td>
</tr>
<tr>
<td>Task 1: Prepare the lab start configuration</td>
<td>955</td>
</tr>
<tr>
<td>Task 2: Add a New Routing VRF</td>
<td>955</td>
</tr>
<tr>
<td>Task 3: OSPF Routing Protocols Inside the VRF</td>
<td>965</td>
</tr>
<tr>
<td>Learning Check</td>
<td>969</td>
</tr>
<tr>
<td>Summary</td>
<td>970</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 Captive Portal Authentication</td>
<td>971</td>
</tr>
<tr>
<td>Overview</td>
<td>971</td>
</tr>
<tr>
<td>Guest Introduction</td>
<td>971</td>
</tr>
<tr>
<td>Guest Access Considerations</td>
<td>971</td>
</tr>
</tbody>
</table>
Chapter 6: Advanced OSPF ............................................................... 1024
Chapter 7: BGP ................................................................................ 1025
Chapter 8: IGMP .............................................................................. 1025
Chapter 9: Multicast Routing .............................................................. 1026
Chapter 10: 802.1X Authentication .................................................... 1026
Chapter 11: MAC Authentication ....................................................... 1026
Chapter 12: Dynamic Segmentation ................................................... 1026
Chapter 13: Quality of Service ........................................................... 1026
Chapter 14: Additional Routing Technologies ...................................... 1027
Chapter 15: Captive Portal Authentication .......................................... 1027
1 Introduction to Aruba Switching

OBJECTIVES

After completing this chapter, you should be able to:

✓ Compare and contrast the different AOS-CX switching models

✓ Describe the important features of the AOS-CX switching product line

Overview

This chapter introduces the AOS-CX products and features that are covered in this guide. AOS-CX switches and operating system was designed for both data center and campus networks. The AOS-CX switch hardware enhancements like HPE’s ASICs, with over 20 years of design and development experience, Virtual Output Queuing (VOQ) for dealing with head-of-line blocking, deep packet buffers, always-on POE on the 6300 and 6400 switches, and many other hardware features are needed for both campus and data center networks. The operating system was designed from scratch. It has all your typical features needed in campus and data center networks; however, it has a lot of enhanced features that lead the industry, including enhanced API functionality, network analytics that go beyond what is available with SNMP and sFlow, highly resilient virtual switching with VSX, dynamic segmentation for securely controlling access and forwarding of traffic, and many other features that you will see throughout this guide. The future of switching with HPE is AOS-CX and this guide will provide an intermediate-level coverage for implementing campus wired solutions.

Note

Data center designs and features are covered in other Aruba-related courses. This guide focuses on campus solutions.
AOS-CX Switch Overview

In this first section, you will be provided with a brief introduction of the AOS-CX switching product line.

AOS-CX: Heart of Aruba’s Core, Aggregation, and Access

The AOS-CX software forms the heart of Aruba’s strategy for campus core and aggregation switching, as shown in Figure 1-1. Its programmable nature rests on open REST APIs, which enable external applications to securely view and configure all components of the system. Developers can use Python, a familiar scripting language, to script interaction with the REST API as well as to create Network Analytics Engine (NAE) agents for system monitoring and troubleshooting. AOS-CX is extensible. It is built to support micro-services and, with its open API, to integrate with other workflow systems and services.

The AOS-CX takes an innovative approach to high availability and fault-tolerance. The software architecture supports resiliency; for example, a process that fails can roll back to a good state using the stateful database. AOS-CX has even been honored by the industry for its innovation. CRN awarded the 8400 switch ‘Product of the Year 2017’ in large part due to NAE. NAE takes the guesswork out of troubleshooting and optimization and will be a game-changer for many customers.

Finally, the AOS-CX is secure and forms the bedrock for a trusted infrastructure. In addition to standard security features such as access control lists (ACLs), the AOS-CX supports a trusted boot
process. The software will not boot unless every hardware component checks out as authentic and free from malware and rootkits.

**Note**
Configuration version roll back may cause issues when going between major AOS-CX software versions.

### What Does AOS-CX Mean to Customers?

**Hardware**
- 8400, 8300, 6400, and 6300 series
- Pedigree
- Credibility
- Future proofing & scale

**Software**
- AOS-CX
- Extending the message we started with the 8k
- This platform enables solutions!
- One OS access to DC

**Analytics**
- Network Analytics Engine
- Network is always working for you
- Saves time
- Saves people
- Saves money
- Keeps the network up

**Configuration Automation**
- CX Mobile App
- NetEdit
- Configuration powerhouse
- Remove complexity
- Simple, elegant, operator friendly and enterprise speed
- ZTP/1TP for the modern world

**Dynamic Segmentation**
- Role based enterprise
- Unified policy
- Speed, quality and security of service
- Makes your network smart, less touch, more dynamic. Plug in anywhere, wireless or wired and have the network know exactly what to do with you

**User-based tunneling**
- Pedigree
- Credibility
- Future proofing & scale

By deploying the AOS-CX switches in a campus or data center network, customers get all the benefits of an advanced operating system and the HPE Gen7 ASIC family (Figure 1-2). They get a combination of:

- Proven technologies including dynamic segmentation, which unifies wired and wireless access, enhances and simplifies policy enforcement, and protects IOT and other critical devices
- New hardware that brings together Gen 7 HPE ASICs with Virtual Output Queuing, Smart Rate ports, and up to Class 6 PoE
- The AOS-CX operating system with its modern architecture enables a seamless REST interface, with support for the exclusive Network Analytics Engine
- A set of advanced tools that cover:
  - Enhanced deployment (zero-touch or one-touch) via the CX mobile app
  - Advanced configuration management with NetEdit